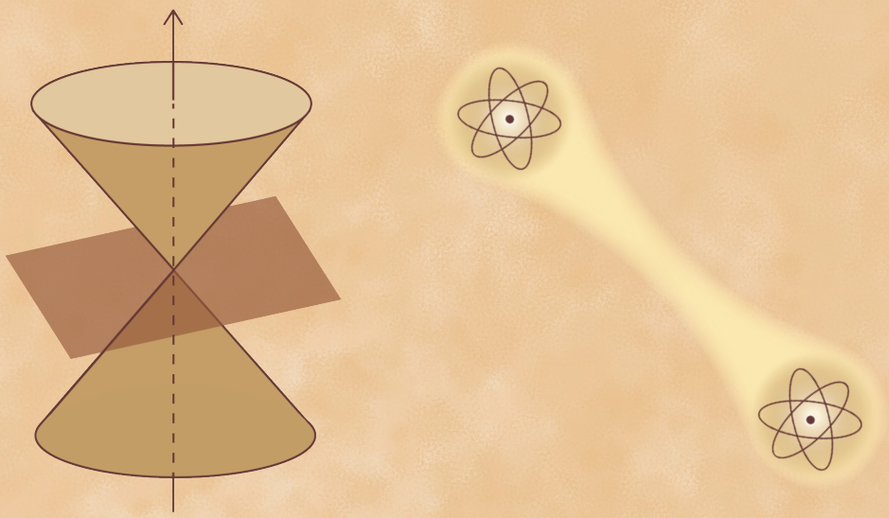
This doctoral thesis explores quantum position verification (QPV)—a cryptographic task where one attempts to confirm someone's geographical location. The core question that QPV aims to answer is: *Are you truly at the location you claim to be?* To achieve this, QPV combines two pillars of the fundamental laws of nature: (i) *special relativity*, which limits the speed at which information can travel to the speed of light in vacuum, and (ii) *quantum mechanics*, which governs the behavior of quantum particles in ways that defy intuition. QPV protocols rely on (i) timing communication between the entities involved in the protocol, and (ii) transmitting information encoded in quantum particles.

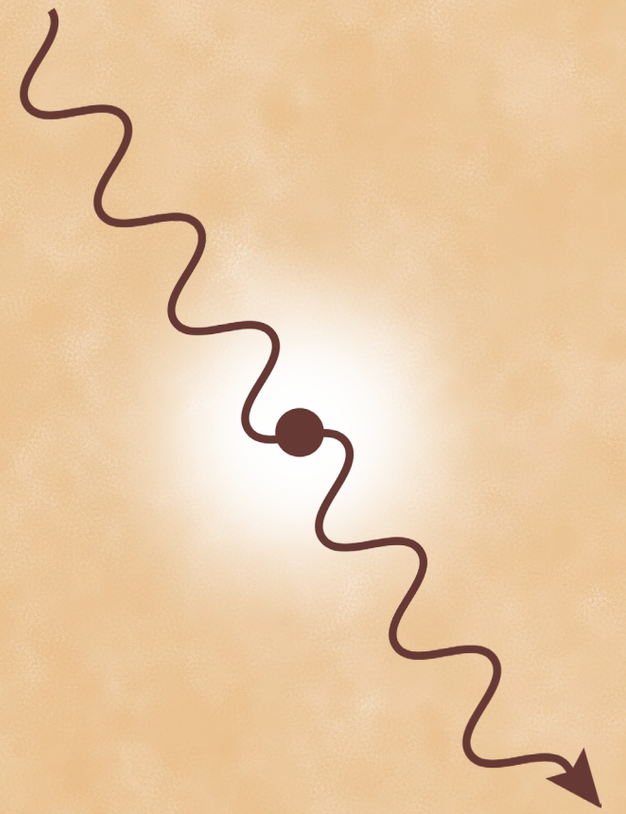
However, quantum hackers may attempt to pretend to be at the claimed location while actually being elsewhere. This raises the critical question: *Can one be certain that the claimed location is genuine and not forged by hackers?*

This thesis presents new advances toward a fundamental understanding of QPV, its security against powerful quantum hackers, and the feasibility of secure QPV protocols despite experimental challenges that, if exploited by hackers, can severely compromise their security. Furthermore, related to attacks on QPV protocols, this thesis analyzes quantum correlations that emerge in broader cryptographic primitives.



On Quantum Position Verification: Security and Experimental Constraints Llorenç Escolà Farràs

On Quantum Position Verification: Security and Experimental Constraints



Llorenç Escolà Farràs

On Quantum Position Verification: Security and Experimental Constraints

Llorenç Escolà Farràs

On Quantum Position Verification: Security and Experimental Constraints

This doctoral thesis received financial support from the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.

Cover design by Marta Crespí Campomar and Llorenç Escolà Farràs.
Printed and bound by Ipskamp Printing.

ISBN: 978-94-6473-880-3

On quantum position verification: security and experimental constraints

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. P.P.C.C. Verbeek
ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op vrijdag 12 september 2025, te 13.00 uur

door Llorenç Escolà Farràs
geboren te Sant Pere de Ribes

Promotiecommissie

Promotores:	prof. dr. P. Grosso	Universiteit van Amsterdam
	prof. dr. C. Schaffner	Universiteit van Amsterdam
Copromotores:	dr. F. Speelman	Universiteit van Amsterdam
Overige leden:	prof. dr. E. Diamanti	Lip6 Sorbonne
	dr. B. Škorić	Technische Universiteit Eindhoven
	dr. W. Löffler	Universiteit Leiden
	prof. dr. S.M. Jeffery	Universiteit van Amsterdam
	prof. dr. H.M. Buhrman	Universiteit van Amsterdam
	prof. dr. C.J.M. Schoutens	Universiteit van Amsterdam

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

To my father, Andreu; my mother, Carme; my siblings, Marçal, Roger, and Vinyet; and to the rest of my family and friends.

The results of this thesis are based on the following articles. For all articles, the authors are ordered alphabetically and co-authorship is shared equally.

1. [EFS23] Llorenç Escolà-Farràs, and Florian Speelman. "Single-Qubit Loss-Tolerant Quantum Position Verification Protocol Secure against Entangled Attackers," *Phys. Rev. Lett.* **131**, 140802 (2023). Contributed talk at *TQC 2023* and *QCrypt 2023*.

2. [EFS25a] Llorenç Escolà-Farràs, and Florian Speelman, "Lossy-and-Constrained Extended Non-Local Games with Applications to Quantum Cryptography", *Quantum* **9**, 1712 (2025).

3. [EFHO+25] Llorenç Escolà-Farràs, Jaròn Has, Maris Ozols, Christian Schaffner, and Mehrdad Tahmasbi, "Parallel repetition of local simultaneous state discrimination", *Quantum* **9**, 1706 (2025).

4. [EFPS24] Léo Colisson Palais, Llorenç Escolà-Farràs, and Florian Speelman, "A quantum cloning game with applications to quantum position verification", *arXiv:2410.22157* (2024). Accepted for publication in the proceedings of *TQC 2025*.

5. [EFS25b] Llorenç Escolà-Farràs, and Florian Speelman, "Quantum position verification in one shot: parallel repetition of the f-BB84 and f-routing protocols", *arXiv:2503.09544* (2025). Accepted contributed talk at *TQC 2025*.

6. [EFRA+24] Llorenç Escolà-Farràs, Arpan Akash Ray, Rene Allerstorfer, Boris Škorić, and Florian Speelman, "Continuous-variable quantum position verification secure against entangled attackers", *Phys. Rev. A* **110**, 062605 (2024).

Additionally, the author has co-authored the following articles, which are not covered in the present thesis:

7. [ABB+23] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel, "Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss", *arXiv:2312.12614* (2023). Contributed talk in *QIP 2024* and *QCrypt 2024*.

8. [AEFR+23] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, Florian Speelman, and Philip Verduyn Lunel, "Security of a Continuous-Variable based Quantum Position Verification Protocol", *arXiv:2308.04166* (2023).

9. [EFB22] Llorenç Escolà-Farràs, and Daniel Braun, "Quantifying Causal Influence in Quantum Mechanics", *Phys. Rev. A* **106**, 062415 (2022).

Contents

Acknowledgments

I would like to express some words of gratitude to the people that have supported, guided, and inspired me throughout the course of my PhD journey from both personal and professional points of view. I would like to begin by thanking my supervisor, Florian, who I spent a lot of my research time with during the PhD and who I bothered every time I felt like I needed his help, promising that I would take at most 30 minutes and always ended up being much longer. I also want to give thanks to my promotors Christian and Paola, who made possible that I completed my PhD and who were very supportive from the very beginning helping me face the thesis and keeping track of my progress during these 4 years, providing an atmosphere where I felt comfortable.

I want to express my gratitude to the members of my doctorate committee, Boris, Eleni, Harry, Kareljan, Stacey, and Wolfgang, for the time spent on this thesis and the valuable feedback.

I would like to deeply thank my family, who deserve a special treatment in these acknowledgments. First, I would like to thank my father, Andreu, who passed away during this journey, and was an exceptional person who always showed via his actions, that us, his children, were his priority in this world. For that, for all the years that you took care of us, provided us with love and support, and for your character that could not avoid being constantly worried about our wellbeing, thank you. I also want to express my gratitude to my mother, Carme, one of the most energetic persons I know, with constant new projects and new interests. She has always been present and helpful, and I owe it to her that our family has always been so close-knit and supportive of one another, thanks. And now, to my siblings, who, despite living far away from them, have remained very close: Marçal, for the constant voice messages we exchanged on WhatsApp, the times we called each other to update about our lives or ask for advice, and for spending a lot of time together whenever I was visiting my hometown; Roger, for always being someone I could count on when needed, for coming to Amsterdam twice in a row—those visits were a lot of fun—for finding time to make plans together, and I also want to take this chance to congratulate him on his new job and apartment; and Vinyet, for always checking in, for calling me very often,

for always being so thoughtful, making sure we could make plans together, and wishing me good luck whenever I had something new going on. I loved hanging out with them, having drinks, dinners and going for walks every time I came back to my hometown, Sant Pere de Ribes, and when they visited me in Amsterdam. They are not only siblings but also friends. I also want to thank their partners, Ariadna, Raquel, and Àngel, respectively, who have become part of our family and whom I've gotten to know over these past years—often, and very gladly, with me as the third wheel. I would also like to express my gratitude to my grandfather, Jaume, who I enjoy drinking a *Vichy* with every time I visit him. Worth to mention, he might potentially be one of the causes I was drawn to scientific research; he is an engineer and showed an extreme interest in physics and mathematics during all his life and I used some of his textbooks to study during my bachelor's. I also can't leave out my cousin Anna, with whom I share so many teenage memories, and with whom it always feels like no time has passed when we reunite, my uncle Carles, and his partner, Teresa, who I enjoy his "boomer" jokes and her passion for acting, I'm glad they live close to my parents so that is makes easier to see each other often. I also want to warmly acknowledge my cousin Jordi and his husband, David; Jordi holds the title of being one of the people who visited me most in Amsterdam, and remarkably, every time he came, he invited me to dinner at a Michelin-star restaurant. I shouldn't close the family section without mentioning Toni, the godfather of my brother Roger, who, although not a family member by law, has always been like one to us. I especially appreciate the effort he made to come to my hometown to visit whenever I was back.

I owe a huge thanks to my friends Fran and Bernat, with whom I decided to start a new adventure: living like a family in our flat. Fran is probably the person I spent most time with during the years of my PhD; I considered him a true friend. Over the last years, he's really honored this label, always being present and being someone who I felt comfortable sharing my joys and worries, and I admire his kindness to people and his commitment to political beliefs aiming the world to be a better place for everybody. Bernat became a great, close friend after he moved to Amsterdam a couple of years ago. I admire Bernat's funny character: he always brings great energy wherever he goes, cracking jokes and brightening the mood. Worth to mention, he often makes food for me and does not forget to bring ice cream for desert, which I really appreciate. I thank both for their valuable company, I consider myself lucky to live with them. I also want to express a great gratitude to my friends Eva and Milagros, who became very important, and, together with Bernat and Fran, we meet every week to update about our lives, have dinner, have drinks, watch movies, have coffee, go for a walk, etc. I want to thank them for making this journey nicer and making me feel like home.

I would like to turn my attention to the *Petxines i Cigales* group, who are the friends from my hometown, who I grew up with, and I am very lucky to still be close to them, and their partners, who became an essential part of the

group and who I could no longer see my friends without them, and I am happy that they became my friends as well. I feel very grateful that this group has remained so present in my life, despite the distance. I would like to mention each of them, in alphabetical order: Andreu, for having been partners in crime in high school, for having kept the friendship ever since, for having shared with me your present and future plans of life. Anna B., for bringing a spark of creativity to the group through thoughtful activities that turn ordinary moments into something memorable, and with whom I had a lot of fun making jokes about *La que se avecina*. Anna G., for always being so kind and asking me how my grandfather is doing, and how I am doing, and, of course, for always being late (some traditions never die). Arantza, for the interesting conversations whenever we hang out, and for teasing me in the funniest ways. I'm also grateful for the times she hosted me at her parents' place in her hometown, Yécora, for multiple occasions, they were memorable. Eva, for becoming closer over the last years and for enthusiastically listening to my anecdotes and chanting out loud in front of the group whenever I say that I am going to tell one. Guillem, for being the friend who is always ready to go out for a drink, catch a concert, and *per donar-ho tot sempre (fins que t'adorms el primer)*, not to mention being *el més culer del grup*. Huge congrats on being the first to get married—I'm really happy for you and all the adventures ahead! Julieta, for all these evenings of playing the board game *Catan* (although I don't remember myself winning ever against her), for the laughter during after-dinner conversations, and for *mantenir el Sergi a ratlla*. Maria, for bringing more calm and *seny* in the group, for always showing a smile and listening to my stories, and I would also like to congratulate you on your incoming marriage with Guillem and wish you all the best in this new adventure. Nil, for always being there and making sure that we caught up on a phone call if we hadn't talked for a while; I'm especially grateful for your patience listening to the same stories over and over—while I was meeting you and others, sharing the story anew each time, you were always there, hearing it again and again. Sergi, for being *el més cigalero del grup amb diferència*, which always brings a lively dynamic to our group, and for your hospitality whenever we spend time at your vineyard—those moments made our gatherings special. I would also like to thank Ballús, who I met when we were kids (playing basketball) and, after all these years, I am glad we managed to keep in touch and have a coffee while telling our lives. To all of them, I am really grateful that they will come to Amsterdam for my PhD defense, *amics i amigues, de tot cor, moltes gàcies*.

I would like to continue acknowledging my friends from the Autonomous University of Barcelona, who I studied with, and despite having finished 6 years ago and all of us living in different countries, we still make the effort of seeing each other a few times a year, highlighting our traditional Christmas dinner at *Ca l'Estevet*. Every time that we gather, it is full of laughter and complaints about the cuisine in the countries that we live. I would like to mention each of them, in alphabetical order: Andreu, for always being down to join improvised plans—

we know that if someone would say yes to a random trip, that's him—for the adventures we shared, and for the very interesting stories that could only ever happen to him. And beyond all the spontaneity, for the good laughs we've had that always make me feel happier. Biel, whose nickname we all know, for always bringing a fun and vibrant atmosphere to the group, and for being the kind of friend who can lift the energy of any room. While we joke about your legendary lateness—from running like there was no tomorrow to catch an 8h train (seeing it from inside) to missing a flight for no reason at all—I also appreciate the friendship behind all the fun and how easy it is to be around him. Gerard, for having spent essentially all the time together during our bachelor's: in lectures, at the library, at the cafeteria, in events, etc., while enjoying saying "hi" to everybody that we were crossing while eating a *xuxo de crema*, and for having kept this vibe, even from the distance. Joan, *l'home assenyat del group*, for all those times you were worried about us not planning things on trips, always trying to keep us out of trouble, for bringing more balance into the group, and for the evenings we spent with a drink, catching up and talking about everything, and always making time to meet if I was around Barcelona. Laura, for every time that she and Gerard hosted me at their place, always showing a big smile, whenever I was visiting them and was always looking forward to the next time, for all the great chats that we had and showing interest about my life, I always liked being the third wheel. Nicetu, who is always a couple of steps above in life despite being the youngest (the first one getting a PhD, the first one getting married, etc), for the great moments spent together and for still keeping in touch after all this time although he is living on the other side of the world. Marc, for having very successfully organized *les colònies de física* during all the years of our bachelor's, which were one of the best weekends of the year and we were very enthusiastic about them, and for having kept the effort of seeing each other a couple of times a year to catch up.

I would like to thank the people that I met at work. Marten, for our friendship since the beginning of the PhD, that started that day having Nachos and beers at Polder, and continued with trips (road trip in The Netherlands, California, Canary Islands, Barcelona, Morocco, and even other places!), watching "Wie is de Mol" with his girlfriend Renée—who I also want to thank for the good moments I spend with her and Marten—and many fun plans in Amsterdam. Sebastian and Chelsea, who got recently married (congratulations!), for all the evenings that we had Spanish omelette for dinner and drinking cava, for the trips that we shared (Maastricht, Paris, and Mumbai), and for all the times I asked Sebas about bureaucracy and logistics. Adam, for encouraging me to join calisthenics classes, which we weekly go together for the lasts two years, and for the good occasions where we spent time doing outdoor activities, which in particular, I want to mention the surf trip in Morocco. Randy, with whom I shared the office most of this journey, who was always down for a passionate game of foosball whenever we needed a break, and for the fantastic historical

poster he gifted for decoration when I moved to my current apartment. I'd like to thank the "CWI foosball community", for all these foosball games that we played: Nikhil (also for inviting me to his wedding in India), Dyon (also for the amazing trip in Hawaii and his little secret there), Léo (also for the time spent together doing research and inviting me to his wedding), Amira (also for the many times I asked you about future professional tips), Lynn (also for always inviting me to her celebrations), Davi (also for swearing in Portuguese during the games, that was a lot of fun), Yanlin (also for his crazy *snakes* while playing), Arjan (for sending a voice message every time he hears *Pepas*), Poojith (for his enthusiasm in the games), Daan (for being always fun to play with—or even better, against), Sebastian V. (also for the times that we shared pictures of our trips and families), Chris C. (for being there from the beginning), Harold (for the *gezellig* times). I'd to acknowledge Lorenzo, for having cappuccinos together in the mornings before to start working, Salvatore, for releasing the tension in my back; Simona, for her amazing birthday parties together with Lisa, who was always the last standing person in the celebrations; Vicky, for always being present despite not living in Amsterdam and always willing to make fun plans, catch up and express her joys and worries with me; Ido, for making the effort to keep on updating about our lives every now and then; Garazi, for sharing the first steps of the PhD together; Philip and Rene, who were always together, for all the QPV discussions and the amazing trip in Canada; Jordi, for our funny trip in San Francisco; Joran and Rosa, for keeping inviting each other for celebrations; Luca, Philippo, Franceso and Nunzia for bringing good (Italian) vibes during your stay at QuSoft, Subha, for always showing strength in life raising her kid. I am grateful to Remco, for the chats at the reception; Mohammed, for his generous food portions he gave me at the canteen; Paul, for the chats about football, Bikkie, for helping me to practice my Dutch; Minnie, for the pictures and the always funny vibe; Peter, who was present at all the PhD defenses of my colleagues and we shared good conversations; Susanne, for being always willing to help. A warm thank to Ailsa, Akshay, Ake, Aldo, Alicja, Alvaro, Anna, Arie, Carla, Doutzen, Emiel, Filippo, Freek, Galina, Gina, Hema, Ilaria, Jana, Jelena, Jeroen, John, Jonas, Jop, Joppe, KoenG, KoenL, Krystal, Laurens, Ludovico, Mani, Maris, Max, Maxim, Mehrdad, Mert, Niels, Nicolas, Ronald, Sarah, Seenivasan, Subha, Tony, Vania, VictorL, Vlad, Yanlin, Yaroslav, and Zongbo. I'd like to thank the people in the cryptography group: Ludo, Shane, Yu-Hsuan, Julia, Paola, and Michael. I would like to thank Andreas, Ángela, Arpan, and Vincent, who are coauthors and people I still collaborate with.

Of course, I can't forget the friends I met in Amsterdam—you've made life here more enjoyable, and I want to mention each of you: Àngel, Ana, Blanca, Cesc, Fede, Ferran, Gallo, Guillaume, Guillermo, Henny, Isabel, Joie, Jorn, Leon, Marina, Marion, Marta, Monroy, Núria, Olga, Pablo, Quique, Ramon, Ric, Robin, Sandra, Silvia, Simon, Stijn, and Yasan.

Chapter 1

Introduction

1.1 Historical background

Quantum physics emerged in the 1900s in response to natural phenomena that defied explanation by the prevailing physical theories. Puzzling observations such as blackbody radiation, the photoelectric effect, and the discrete spectral lines of atomic emission[1] could not be understood within existing frameworks. Theoretical breakthroughs addressing these three phenomena were proposed by Planck [Pla01], Einstein [Ein05a], and Bohr [Boh13], respectively. One of the earliest crises was the so-called "ultraviolet catastrophe": according to the prevailing theories of electromagnetism at the time, an ideal blackbody (a perfectly absorbing and radiating object) in thermal equilibrium would emit infinite energy at high frequencies. Planck resolved this paradox by proposing that electromagnetic energy is exchanged only in discrete packets—*quanta* (from Latin, meaning "amounts")—a revolutionary idea that laid the foundation for a new physical theory. The singular form, *quantum*, would soon come to name the emerging framework.

These early discoveries revealed that, at microscopic scales, nature behaves in ways that challenge our everyday intuitions. Concepts such as wave–particle duality emerged, showing that light can exhibit both wave-like and particle-like behavior [Ein05a], and that energy is delivered in discrete units [Pla01]. In the 1920s, the mathematical formalism of quantum mechanics was established, with major milestones including Heisenberg's matrix mechanics [Hei25]; Schrödinger's wave equation [Sch26], describing the dynamics of quantum particles; and Dirac's unification of quantum theory with special relativity [Dir30]. Alongside its predictive success, quantum theory introduced deeply novel principles: Heisenberg's uncertainty principle [Hei27], which imposes fundamental limits on the simultaneous precision of position and momentum; the superposition principle, where a

[1] For a broader overview of these and other foundational developments that led to quantum theory, we refer the reader to [Gas03].

quantum system can exist in multiple different states simultaneously [Dir30]; and entanglement [EPR35, Sch35], which describes correlations between distant systems that defy explanation within pre-quantum frameworks. All physical theories not encompassed by quantum mechanics came to be referred to by the quantum physics community as *classical* physics.

It was not until decades later that the use of quantum systems for processing and communicating information was explored, with early ideas including Wiesner's concept of *quantum money*, first formulated in 1969 and published in 1983 [Wie83]—widely regarded as the origin of quantum cryptography—and Feynman's 1982 proposal of *quantum computers* [Fey82]. In the 1980s, Bennett and Brassard introduced the first quantum key distribution (QKD) protocol, BB84 [BB84], which played a key role in the development of quantum cryptography. The 1990s saw the emergence of the first quantum algorithms that outperform their best-known classical counterparts, including the Deutsch–Jozsa algorithm [DJ92], Shor's algorithm for factoring [Sho94], and Grover's algorithm for database search [Gro96].

In this thesis, quantum cryptography plays a central role. While QKD has historically received the most attention in the field (see, e.g. [PAB+20]), numerous other quantum cryptographic primitives have been explored, such as position verification, unclonable encryption, bit commitment, oblivious transfer, and coin flipping. We refer to [BCWW24] for a recent survey of the state of the art.

1.2 Quantum position verification

Position-based cryptography (PBC) explores the use of a party's geographical location as a cryptographic credential. A central primitive in this field is position verification (PV), which seeks to determine whether an untrusted prover P is physically located at a claimed position *pos*. To this end, a coalition of trusted verifiers interacts with the prover in a structured protocol designed to establish that the prover is located at the claimed position. In the 1990s, the first approach to address this problem was proposed by Brands and Chaum in [BC94], where they introduced the *distance bounding* technique, based on combining communication of classical messages, and fundamental laws of nature—specifically, the relativistic constraint that no information can propagate faster than the speed of light, formalized by Einstein's theory of special relativity [Ein05b]. Upon this fundamental physical constraint, verifiers interacting with a prover, that is sending and receiving messages that can travel at (or close to) the speed of light, can establish an upper bound on their distance with P. Importantly, such high-speed communication is feasible with current technology—for example, radio waves travel at nearly the speed of light in vacuum.

In 2006, Kent, Munro, Spiller, and Beausoleil proposed using quantum information as a foundational tool for position verification, as documented in a

U.S. patent [KMSB06]. Their idea anticipated critical limitations of classical PV protocols, later demonstrated by Chandran, Goyal, Moriarty, and Ostrovsky [CGMO09], who showed that no classical protocol can securely verify position in the presence of colluding adversaries, due to a general attack based on copying classical information. This vulnerability does not carry over to the quantum setting, due to the no-cloning theorem [WZ82]. Consequently, growing attention shifted toward the development of quantum position verification (QPV) protocols, explored more thoroughly in subsequent academic work [KMS11, Mal10, BCF+14, LL11].

In this thesis, we will focus our attention on one-dimensional position verification protocol. This is the case that captured most of the attention in literature. Ideas generalize to multiple dimensions, however, some care has to be taken when introducing nonnegligible timing uncertainty in the three-dimensional case. The general setting for a one-dimensional QPV protocol is described by two trusted verifiers V_0 and V_1 located in a straight line at the left and at the right of P, respectively, who is supposed to be at the position *pos*. The two verifiers are assumed to have synchronized clocks. Then, a protocol proceeds as follows:

1. The verifiers privately agree on classical bits or quantum states to be used in the protocol,

2. V_0 and V_1 send quantum or classical messages at the speed of light so that they arrive at *pos* at the same time.

3. Upon receiving the messages, P must, in a negligible time, perform a publicly known operation (e.g. a quantum measurement or classical computation) on the received information and immediately reply to the verifiers, also at the speed of light.

4. Upon receiving the information back, the verifiers *accept* the location if they received correct answers, given the publicly known challenge, according to the time that the speed of light would take to reach *pos* and return, otherwise, they *reject*.

Throughout this thesis, we will use the expressions "*immediately*" and "within a *negligible* time" interchangeably. Moreover, because QPV relies on relativistic speed-of-light constraints, we model fast quantum signals as photons—the natural carrier of light-speed communication.

In order to illustrate QPV, we describe a concrete protocol: the BB84-QPV protocol, denoted by $\mathrm{QPV}_{\mathrm{BB84}}$, that was originally introduced in [KMS11], and will take a central role in this thesis. In $\mathrm{QPV}_{\mathrm{BB84}}$,

1. V_0 and V_1 secretly agree on random bits $v, z \in \{0,1\}$. Then, V_0 prepares the qubit state $|\phi\rangle = H^z|v\rangle \in \{|0\rangle, |1\rangle, |+\rangle\,|-\rangle\}$, where H is the Hadamard transformation.

2. V_0 sends the qubit $|\phi\rangle$ to P, and V_1 sends z to P, both at the speed of light in vacuum, coordinating their times so that they arrive at *pos* at the same time.

3. Immediately, P measures the received qubit in the computational basis if $z = 0$ or the Hadamard basis if $z = 1$, and broadcasts her outcome, either 0 or 1, to V_0 and V_1.

4. If V_0 and V_1 receive their respective answers at the time corresponding with *pos* and both are equal to v, the verifiers *accept* the location. Otherwise, they *reject*.

The idea behind QPV_{BB84} is that in order to decode v, both z and $H^z|v\rangle$ are needed, since measuring this qubit in a basis that is not the correct one yields to a probabilistic outcome. Then, due to relativistic constraints, any party who is not located at position *pos* would necessarily receive both z and the quantum state $H^z|v\rangle$ strictly *after* a party who is. Consequently, while a party away from *pos* might be able to compute the correct response, at least one of the verifiers would receive it too late. The described QPV_{BB84} is used as a toy model, since accepting or rejecting the location is based on a single bit drawn at random, and therefore a random bit (not necessarily originating from *pos*) would successfully lead the verifiers to accept the location with 50% probability. In reality, a decision about the location would be made by repeating the protocol so that "enough" data is collected to make a decision. For instance, in an ideal implementation, all the answers after a given number of repetitions—sequentially or in parallel—should be correct in order to accept the location.

See Figure 1.1 for a schematic representation of the QPV_{BB84} protocol. In the diagram, the verifiers V_0 and V_1 are placed equidistant from the position *pos* for visual clarity. Throughout this thesis, all protocol illustrations will adopt this convention for consistency and ease of interpretation. However, we emphasize that this arrangement is purely for illustrative purposes; the protocols do not require the verifiers to be equidistant from the prover, and the analysis remains valid for arbitrary verifier placements.

Security and limitations

We argued above that relativistic constraints do not allow a party to perfectly decode v in QPV_{BB84}. However, a more subtle threat arises when two (or more) collaborating adversaries attempt to simulate a single prover located at *pos*. The most general form of an attack in the one-dimensional QPV setting [BCF+14] consists of placing one adversary—referred to as Alice—between V_0 and *pos*, and another—Bob—between V_1 and *pos*. Then, due to relativistic constraints, they must operate under timing limitations. They act as follows:

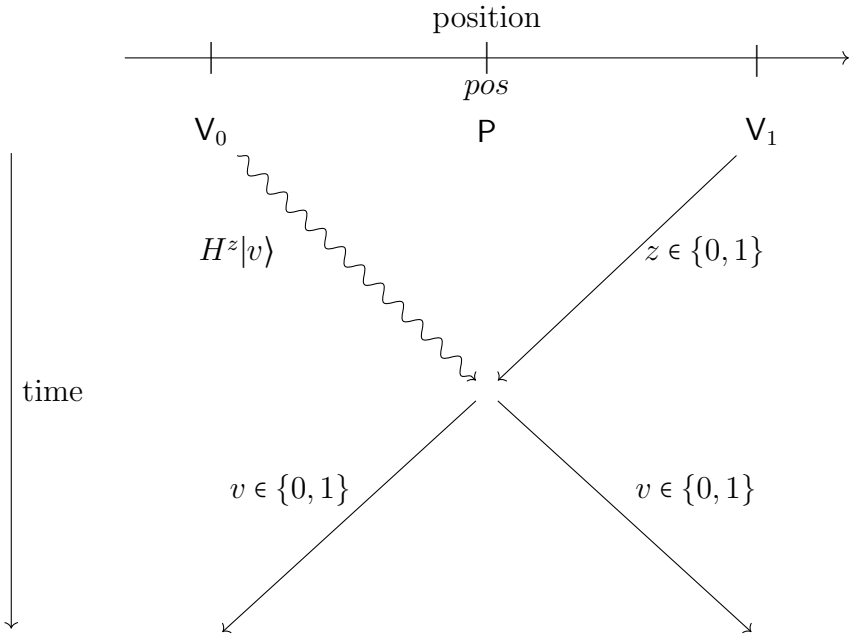


Figure 1.1: Steps 2 and 3 of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, where straight lines represent classical information and undulated lines represent quantum information. P is located at *pos*.

1. Prior to the protocol execution, Alice and Bob coordinate an attack strategy, which may involve pre-shared entanglement or classical/quantum resources.

2. During the protocol, Alice intercepts the message sent by V_0, and Bob intercepts the one from V_1. They each perform local (negligible-time) operations based on the intercepted data.

3. Within the time allowed by the speed-of-light constraint, Alice and Bob exchange information—classical or quantum—through a single round of simultaneous communication.

4. After this exchange, they each perform final local operations and respond to their closest verifier.

Since Alice and Bob can intercept all communication from the verifiers to the prover, introducing additional adversaries does not offer any further advantage. In this thesis, we will often say that attackers "pre-share entanglement", meaning that they share entanglement prior to the execution of the protocol, i.e. in step 1.

As with the protocol schematics discussed earlier, we adopt a symmetric representation of attacks for visual clarity: Alice and Bob will be depicted at the midpoints between V_0 and *pos*, and V_1 and *pos*, respectively, see Figure 1.2. This convention will be used throughout the thesis for illustrative purposes; however,

the analysis remains valid for adversaries located *anywhere* between *pos* and the verifiers.

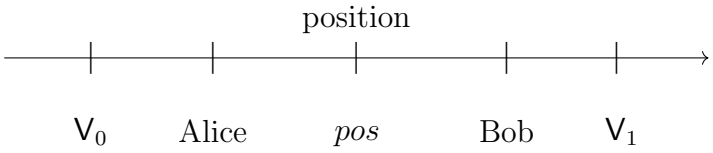


Figure 1.2: Schematic representation of the placement of two adversaries, Alice and Bob, in a generic attack on a one-dimensional QPV protocol.

Whereas the intuition behind the no-cloning theorem could suggest that Alice and Bob cannot both possess the qubit $H^z|v\rangle$ at the stage 4. of the attack, and thus recover v performing the measurement that P would, there exists a perfect attack [KMS11] that allows them to extract v. This attack consists of Alice and Bob sharing entanglement prior to the execution of the protocol and making use of quantum teleportation. In the attack, they proceed as follows :

1. Prior to the execution of the protocol, the adversaries prepare the maximally entangled state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$. Alice and Bob retain registers A and B, respectively.

2. Alice intercepts the qubit $H^z|v\rangle$ sent by V_0 and performs a teleportation measurement. Specifically, she applies a CNOT gate with the intercepted qubit as the control and her half of the entangled pair—register A—as the target. She then applies a Hadamard gate to the register corresponding to the intercepted qubit, and measures both qubits in the computational basis, obtaining two classical bits: the teleportation corrections c_1 (from the intercepted qubit) and c_2 (from register A). This sequence of operations—CNOT, Hadamard, and computational-basis measurement—effectively performs a measurement in the *Bell basis*, which is the standard method for implementing quantum teleportation. As a result, Bob's register collapses to the state $X^{c_1}Z^{c_2}H^z|v\rangle$, where X and Z are the Pauli-X and Pauli-Z matrices, respectively. He intercepts z sent by V_1 and measures this qubit in the computational basis if $z = 0$, or in the Hadamard basis if $z = 1$, and records the outcome as b. The measurement outcomes can be analyzed as follows:

   - Case $z = 0$: The state becomes

   $$X^{c_1}Z^{c_2}H^z|v\rangle = (-1)^{c_2}X^{c_1}|v\rangle = (-1)^{c_2}|v \oplus c_1\rangle, \tag{1.1}$$

   so a measurement in the computational basis yields $b = v \oplus c_1$.

- Case $z = 1$: In this case, the state becomes

$$X^{c_1} Z^{c_2} H|v\rangle = X^{c_1} Z^{c_2} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^v|1\rangle) = \frac{1}{\sqrt{2}}(X^{c_1}|0\rangle + (-1)^{v\oplus c_2} X^{c_1}|1\rangle)$$
$$= \frac{1}{\sqrt{2}}(|0 \oplus c_1\rangle + (-1)^{v\oplus c_2}|1 \oplus c_1\rangle).$$

  This is the state $H|v \oplus c_2\rangle$, up to a global phase, so a measurement in the Hadamard basis yields $b = v \oplus c_2$.

3. Alice and Bob simultaneously exchange classical messages: Alice sends the teleportation corrections (c_1, c_2) to Bob, and Bob sends his measurement outcome b to Alice.

4. After the exchange of information, each adversary can locally recover the original bit v as follows: if $z = 0$, then $v = b \oplus c_1$, if $z = 1$, then $v = b \oplus c_2$.

This attack provides a concrete example of how adversaries can perfectly spoof verifiers in a quantum position verification protocol. Naturally, a crucial question arises: is it possible to design a protocol that no attack can circumvent—one that achieves *unconditional security*? As it turns out, the answer to this question is negative. As was shown in [BCF+14], there exists a general attack, based on Alice and Bob performing quantum teleportation in step 2 of a general attack, which allows adversaries to convince the verifiers to *accept* the claimed position *pos* with a probability arbitrarily close to 1. Nevertheless, this attack does not invalidate quantum position verification entirely, as it requires Alice and Bob to share, during the preparation stage (step 1), a double-exponential amount of maximally entangled states (relative to the resources utilized in the protocol). Consequently, executing this attack is practically impossible. Moreover, the best-known general attack [BK11] still demands an exponential amount of pre-shared entanglement. This impracticality has sustained interest in showing security against attackers with bounded resources [KMSB06, KMS11, LL11, RG15, CL15, Spe16a, Dol22, DC22, GC20, CM23, BCS22, GLW16, EFPS24, ACC+24].

As is customary in the QPV literature, within a given attack model, we refer to the probability that the verifiers *accept* without the prover being at *pos* as the *success probability* of an attack. An upper bound on this probability is called the protocol's *soundness*.

1.3 Challenges of quantum position verification

The fact that all QPV protocols can be broken using a very large amount of pre-shared entanglement leads to the first fundamental challenge that all QPV protocols face—even under idealized conditions:

(i) *Entanglement Challenge* (**EC**): Entangled attackers. Although it is known that adversaries pre-sharing an arbitrary amount of entanglement can successfully break any QPV protocol, future implementations should aim for resilience against attackers sharing a bounded amount of entanglement.

Given that attackers who pre-share entanglement can perfectly break the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, a natural first step is to constrain adversaries by disallowing entanglement prior to protocol execution. Such an adversarial scenario, formally introduced in [BCF+14], is known in the literature as the *No Pre-shared Entanglement* (No-PE) model. Under this assumption, the intuitive reasoning derived from the no-cloning theorem indeed applies, preventing adversaries from reliably extracting v at step 4 of the attack. The optimal probability that the verifiers *accept* the claimed position *pos* in the No-PE model is $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$ [TFKW13]. Consequently, by repeating the protocol sequentially, verifiers can amplify security, increasing their chances of catching adversaries (i.e. of *rejecting* the claimed location) in the No-PE scenario.

Remarkably, even though in the No-PE model Alice and Bob may share arbitrary entanglement in step 4, optimality can be achieved by a straightforward attack: Alice, in step 2, measures the qubit $H^z|v\rangle$ in the *Breidbart basis* $\{|B_0\rangle, |B_1\rangle\}$, defined as

$$|B_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, \quad \text{and} \quad |B_1\rangle = \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle, \tag{1.2}$$

which corresponds to the projective measurement onto the state with maximal overlap with $|0\rangle$ and $|+\rangle$. Denoting Alice's measurement outcome by $a \in \{0, 1\}$, where outcomes 0 and 1 are associated to $|B_0\rangle$ and $|B_1\rangle$, respectively, she broadcasts a, and both adversaries reply with a to their closest verifier. The probability of correctly guessing v in this attack is $\frac{1}{2} + \frac{1}{2\sqrt{2}} = \cos^2(\pi/8) \approx 0.85$. See Figure 1.3 for a schematic representation of this attack.

Note that Bob plays no essential role in the attack; thus, it can be executed by a single adversary (Alice), who, after measuring $H^z|v\rangle$, immediately sends the outcome a to V_1, retains a copy of a as long as needed, and later forwards it to V_0 at the appropriate time.

Quantum position verification (QPV) seeks to confirm the physical location of an untrusted party. For the primitive to become a practical reality, its protocols must withstand real-world imperfections. So far, we have examined an idealized protocol ($\mathrm{QPV}_{\mathrm{BB84}}$), but moving from theory to experiment exposes two major implementation challenges—*in addition* to the fundamental problem of (**EC**) entangled attackers—that force us to rethink existing designs:

(ii) *Loss Challenge* (**LC**): Photon loss. In practice, a non-negligible fraction of photons is lost in transmission. For example, at the C-band telecom wavelength (∼1550 nm) a state-of-the-art single-mode fiber still incurs about 0.15

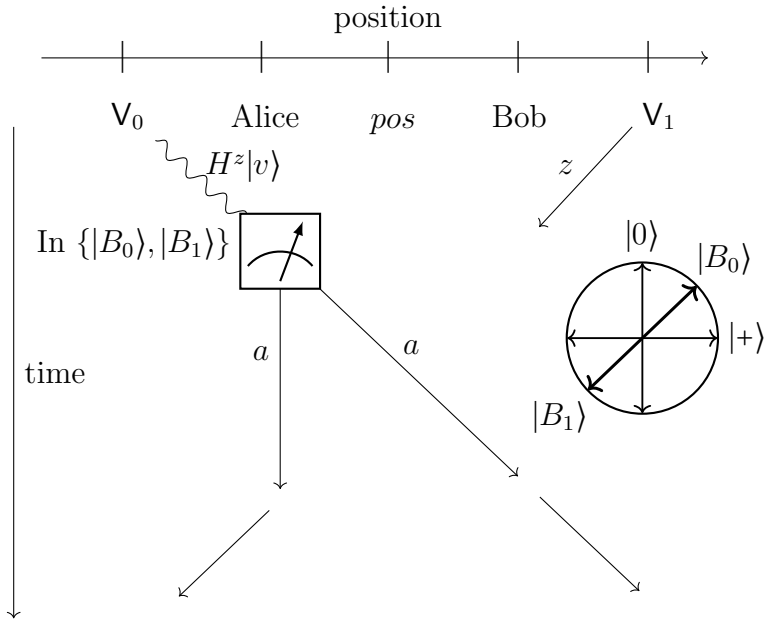


Figure 1.3: Schematic representation of an attack against the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol in the No-PE model that achieves the optimal success probability of $\frac{1}{2}+\frac{1}{2\sqrt{2}}$, based on measuring the state $H^z|v\rangle$ in the Breidbart basis.

dB/km attenuation [CZD19], in addition to coupling and detector inefficiencies[2]. Consequently, some quantum signals will fail to reach the prover. We model such loss by letting the prover report a missing quantum message with the special symbol '$\perp$', sent to the verifiers. A simple and intuitive way to see that loss compromises security can be demonstrated with the following trivial attack on $\mathrm{QPV}_{\mathrm{BB84}}$:

1. Prior to the execution of the protocol, Alice and Bob do not pre-share any quantum information. They agree to act as follows:
2. Alice intercepts $H^z|v\rangle$—since we do not have control of where the verifiers are located, Alice can position herself close to V_0 and intercept (almost) all of the qubits before they are lost. She draws a random bit $z' \in \{0,1\}$ and measures the qubit in the computational basis if $z' = 0$ or in the Hadamard basis if $z' = 1$, obtaining an outcome $a \in \{0,1\}$. Bob intercepts z and makes a copy.
3. Alice keeps a copy of a and z', and sends a copy to Bob. Similarly, Bob keeps a copy of z, and sends a copy to Alice.
4. The adversaries now hold (a, z, z') and proceed as follows:

[2]Photon loss can be significantly reduced in free-space communication, e.g. using quantum satellites [LCL+17].

- If $z' = z$, then Alice measured in the correct basis, so $a = v$. Both adversaries reply with a to their closest verifier.
- If $z' \neq z$, they claim the photon was lost and return the symbol $\perp$.

Whenever they do *not* claim loss, which occurs with probability $\Pr[z' = z] = \frac{1}{2}$, their answer is always correct. Consequently, if the honest-prover channel has an overall transmission rate of 50% or lower, this straightforward strategy achieves perfect acceptance, like the entanglement-based teleportation attack but without any shared entanglement or sophisticated quantum operations—only a single-qubit measurement.

(iii) *Slow Challenge* (**SC**): Significantly *slower-than-light propagation of quantum messages.* QPV relies on the strict timing limits imposed by special relativity, i.e. the fact that no information can travel faster than the speed of light in vacuum. In practice, however, photons carried through a quantum network—typically via optical fiber—propagate at only about two-thirds of the speed of light in vacuum [Agr10]. To account for this, one may consider modifying QPV protocols to give the prover additional time to respond, in line with the slower propagation of quantum messages. In this setting, the timing bound is no longer enforced by fundamental physical limits, but instead reflects a *technological* constraint—one that may be vulnerable to exploitation by adversaries. Furthermore, existing or planned quantum-network infrastructure will rarely connect the verifiers and prover along a single straight line; additional routing delays must be expected. A desirable goal is to have QPV protocols remain secure even when quantum messages travel well below the vacuum speed of light—including scenarios in which photons must follow detoured, lengthier paths.

See Figure 1.4 for a schematic representation of the three major challenges faced by QPV protocols—sometimes informally referred to as the "Bermuda triangle of QPV" in research talks and informal discussions.

Regarding the loss problem, we can distinguish two recent approaches in the literature. The first of which is to create protocols which are secure against any amount of loss, which we can call *fully loss-tolerant protocols.* This type of protocol was first introduced by Lim, Xu, Siopsis, Chitambar, Evans, and Qi [LXS+16], based on ideas from device-independent QKD. New examples and further analyses of fully loss-tolerant protocols were given by Allerstorfer, Buhrman, Speelman, and Verduyn Lunel [ABSL22b, ABSL22a]. Also of note is a recent work performing the first experiment that implements QPV in a lab setting [KPB+25]. These protocols could be excellent realistic candidates for a near-term implementation of QPV, but in the longer term they have two shortcomings: they are insecure against attackers sharing a small amount of entanglement—[ABSL22a] even show that if security against unbounded loss is required, this is unavoidable—and they require speed-of-light transmission of quantum information.

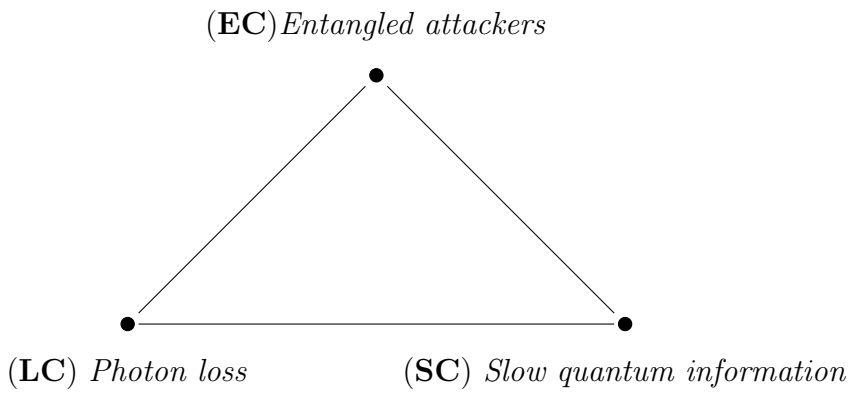


Figure 1.4: Illustration of the three principal challenges for quantum position verification.

Another approach, and the one pursued in this thesis, involves bounding the exact combination of loss rate and error rate that an attacker can achieve, thereby constructing what we call *partially loss-tolerant protocols*. The first published example of this is given by Qi and Siopsis [QS15], who propose extending the QPV_{BB84} protocol to more bases than either the computational or Hadamard to measure a qubit to give some loss-tolerance. A similar idea was independently proposed by Buhrman, Schaffner, Speelman, and Zbinden (available as [Spe16b, Chapter 5]). The key advantage of this approach, compared to fully loss-tolerant protocols, is that it will allow, with proper modifications, for the construction of QPV protocols that simultaneously address all three core challenges: photon loss, entanglement-based attacks, and the requirement for speed-of-light quantum communication.

1.4 Contributions and chapter overview

In this thesis, we work toward presenting and analyzing quantum position verification protocols that simultaneously bypass the three major challenges that they face: (**EC**) entangled attackers, (**LC**) photon loss, and (**SC**) slow quantum communication. We focus both on fundamental aspects of protocols that were not previously analyzed in the literature and on experimental constraints that pose a significant threat to secure QPV. The behavior of attackers in QPV can be modeled in terms of non-local correlations, for which we will state results that apply to other cryptographic primitives beyond position verification. We now summarize the main contributions of this thesis.

First, a natural question arises: since protocols are typically designed to tolerate a certain amount of *measurement error*, and given that our goal is to ensure security under bounded loss, could photon loss simply be treated as another form of noise?

In **Chapter 3**, we argue that it is in fact beneficial to treat loss and error as separate parameters, precisely because they differ substantially in their quantitative impact. For example, the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol admits a perfect attack in which adversaries claim a 'loss' in 50% of the rounds, as shown above. In contrast, the best-known attack that does not exploit loss introduces an error rate of approximately 0.15. This distinction highlights a crucial point: an experimental setup with a 49% photon loss could still enable secure QPV—yet it would be deemed insecure if those losses were treated as measurement errors.

In the chapter, we analyze the exact loss tolerance of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol in the No-PE model. We provide the optimal probability—along with an explicit optimal attack—with which adversaries can be accepted as being at the claimed position *pos*. We show that the protocol remains secure as long as the quantum channel between V_0 and P has a transmission rate exceeding 50%. Our analysis proceeds by reducing the probability of a successful attack (i.e. the probability that the verifiers *accept* the prover's location claim) to the winning probability of a specific type of non-local game that extends the notion of a *monogamy-of-entanglement* (MoE) game [TFKW13] to explicitly capture loss.

In such games, two distant players (taking the roles of Alice and Bob) may share an arbitrary quantum state—that they prepare—with a referee, who performs a fixed measurement based on a given input, and their task is to guess the outcome. By combining the Navascués–Pironio–Acín (NPA) hierarchy [NPA08] with additional linear constraints derived from both loss and error, we develop an *ad hoc* method that yields semidefinite programs (SDPs) whose solutions give the optimal winning probabilities.

However, the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol remains insecure if 50% or more of the photons are lost. In fact, using the above-mentioned optical fibers with 0.15 dB/km of attenuation, this threshold corresponds to a maximum secure distance of approximately 20 km (neglecting additional setup losses). It would be desirable to extend the applicability of QPV to greater distances. To that end, we introduce a family of extensions of $\mathrm{QPV}_{\mathrm{BB84}}$, which, in essence, encode the qubit sent by V_0 to P in $k \geq 3$ distinct bases. We then apply techniques similar to those used in the lossy analysis of $\mathrm{QPV}_{\mathrm{BB84}}$. Although with the above *ad hoc* method, tightness of the resulting bounds is not guaranteed for $k \geq 3$, we show that increasing k allows a larger constant fraction of photon loss to be tolerated while still maintaining security in the No-PE model. This, in turn, enables QPV to be implemented over longer distances.

In **Chapter 4**, we address a key limitation of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol: although it can tolerate up to 50% photon loss, and its extensions allow for even higher loss rates, these protocols remain vulnerable to two of the three major challenges faced by QPV. Specifically, (**EC**) a single maximally entangled state suffices for Alice and Bob to perfectly spoof the verifiers, and (**SC**) they require the qubit sent by V_0 to propagate at the speed of light in vacuum. Building on ideas introduced in [BCS22], we address this gap by presenting protocols that overcome

both (**EC**) and (**SC**) while preserving partial loss-tolerance, thereby providing candidate protocols that simultaneously bypass all three fundamental challenges of QPV. The core idea is to modify the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol in a way that disables the teleportation-based attack relying on a pre-shared maximally entangled state.

A crucial component of that attack is that Bob knows the basis z in step 2 and can measure his half of the EPR pair accordingly. Hiding the value of z thus prevents the attack. While z must be known at the position *pos* in order to execute $\mathrm{QPV}_{\mathrm{BB84}}$, it does not need to be known beforehand. Therefore, we can 'hide' z by encoding it as a function of two classical strings $x, y \in \{0,1\}^n$, where V_0 sends x and V_1 sends y to the prover, who reconstructs $z = f(x,y)$ for some Boolean function f. We denote this variant by $\mathrm{QPV}^f_{\mathrm{BB84}}$. The authors of [BCS22] showed that $\mathrm{QPV}^f_{\mathrm{BB84}}$ achieves soundness at most 0.98 against attackers who pre-share an amount of entanglement linear in n—the Bounded-Entanglement ($\mathrm{BE}(n)$) model. Since the amount of required entanglement grows with the size of the classical inputs, this approach offers a promising path toward practical implementation. However, as argued earlier, unless the combined loss and error remain below 2%, the protocol is no longer secure.

We show that the partial loss-tolerance results from Chapter 3 can be extended to analyze the lossy version of $\mathrm{QPV}^f_{\mathrm{BB84}}$ and analogous modifications of $\mathrm{QPV}_{\mathrm{BB84}}$, even for attackers who pre-share a number of entangled qubits linear in n. To do so, we define a new relaxation of the earlier semidefinite program used in the unentangled case, and demonstrate that its numerical bounds can be used to reprove a key lemma from [BCS22] in the context of our protocols. We note that in separate work co-authored by the author of this thesis, a suitable modification of the structure of $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol was shown to fully bypass the loss-tolerance issue, making the protocol secure against arbitrary transmission loss. The detailed exploration of that approach lies beyond the scope of this thesis; we refer the interested reader to [ABB+23].

In Chapters 3 and 4 we used the above *ad hoc* method to provide upper bounds in various scenarios that can be reduced to a monogamy-of-entanglement game with loss and errors. However, each application required combining the NPA hierarchy with the derivation of specific linear inequalities tailored to the setting at hand.

In **Chapter 5**, we introduce a general framework for analyzing loss and error—as well as other types of constraints—that applies to *any* monogamy-of-entanglement game that incorporates these imperfections. In [JMRW16], Johnston, Mittal, Russo, and Watrous introduced a generalization of MoE games known as *extended non-local games*. As in the MoE setting, Alice and Bob prepare a tripartite quantum state and send one subsystem to a referee, who performs a measurement. However, in extended non-local games, Alice and Bob may receive arbitrary questions, and they must respond such that a publicly known predicate involving the inputs and outputs is satisfied. This model subsumes MoE games

as a special case, where Alice and Bob receive as input the measurement that the referee performs and must guess the corresponding outcome. We introduce a modification of extended non-local games, which we call *lossy-and-constrained* extended non-local games, that takes into account errors, loss and the fact that certain answers are expected to be observed with a given frequency. These games are inspired by practical considerations, describing scenarios where honest parties receive quantum states over a lossy channel, and we aim to prevent security issues that can occur because of such transmission loss and other experimental imperfections. We show that analogous results to those in [JMRW16] hold in the *lossy-and-constrained* setting, including the existence of a hierarchy of SDPs converging to the optimal value attainable by quantum players. Compared to the earlier *ad hoc* method, the framework developed in Chapter 5 offers two clear advantages: first, a description of the game and the experimental parameters suffices to compute an upper bound; second, the method is guaranteed to converge to the optimal value.

We consider various monogamy-of-entanglement and extended non-local games and analyze their *lossy-and-constrained* versions. By computing the corresponding semidefinite programs, we demonstrate that several previously known results can be recovered by directly solving an SDP. Furthermore, we obtain new, tighter bounds—and in some cases, exact values—for the optimal strategies in these games. For instance, we derive tight upper bounds for the security of an extension of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol that uses three different bases to encode the qubits ($k = 3$), improving the results provided in Chapter 3.

It is worth highlighting that, for most of the games we analyze under loss or other constraints, the optimal values are already attained at the first level of the SDP hierarchy. This shows that the resulting programs are numerically tractable in practice, and that moving to higher levels of the hierarchy is often unnecessary. We apply these results to assess the security of quantum position verification protocols under experimental imperfections.

In **Chapter 6**, we analyze a setting closely related to extended non-local games: *Local Simultaneous State Discrimination* (LSSD), originally introduced in [MOST24]. In this scenario, a referee and two distant players (Alice and Bob) share a tripartite quantum state. However, unlike in extended non-local games (or MoE games)—where Alice and Bob prepare the shared state—it is the *referee* who prepares and distributes the state. The shared state is a classical-quantum-quantum (cqq) state, that is, of the form $\rho_{RAB} = \sum_{v\in\mathcal{V}} p(v)|v\rangle\langle v|_R \otimes \rho^v_{AB}$, where the referee retains register R, while Alice and Bob receive registers A and B, respectively. The referee then performs a projective measurement in the basis $\{|v\rangle\}_v$ on his local register. The task of Alice and Bob is to correctly guess the outcome of the referee's measurement.

LSSD problems arise naturally in the context of uncloneable cryptography [BL20, MST21, AKL+22, CLLZ21], where classical data is encoded into quantum states in such a way that an adversary cannot copy the encoded information. Depend-

ing on the resources available to the parties, different discrimination strategies become relevant. The authors of [MOST24] demonstrated that even when the shared state has a classical description, access to quantum entanglement can enhance the success probability of simultaneous state discrimination, and that access to even stronger correlations (no-signaling) can improve it further.

Since [MOST24] also showed that finding an optimal strategy for general three-party LSSD instances is NP-hard, studying these problems in full generality is likely challenging. However, meaningful progress can still be made by analyzing structured classes of LSSD games. In Chapter 6, we consider two such classes. For one of them, we show that the optimal winning probability using classical resources can always be achieved by a strategy with a specific structure. For the other, we establish structural properties of optimal no-signalling strategies under arbitrary number of parallel repetitions of any game in the corresponding class. We then focus on a particular instance that belongs to both classes—the *binary-symmetric-channel* game, originally introduced in [MOST24]. We study its two- and three-fold parallel repetitions, and determine the corresponding optimal success probabilities when Alice and Bob utilize classical, quantum, or no-signaling strategies.

In **Chapter 7**, we extend the game-based toolkit of the previous chapters with a new family of non-local games, *quantum-cloning games* (QCGs). As in monogamy-of-entanglement, extended non-local, and LSSD games, a QCG features distant players who may share an arbitrary quantum state with a referee before play begins; the crucial difference is that the players' responses are themselves *quantum states* rather than *classical* information. The referee then broadcasts the *same* classical question to every player and designates one of them; the selected player must end the game sharing a maximally entangled (EPR) pair with the referee. We first determine the optimal winning probability when the game is played by any number of parties k using arbitrary quantum resources, and we extend the analysis to the case where the target state is an arbitrary fixed bipartite state rather than an EPR pair.

We then show that QCGs are closely related to attacks on a widely studied QPV protocol: the *routing protocol*, denoted $\mathrm{QPV}_{\mathrm{rout}}$, first proposed in [KMS11]. The protocol is described as follows: steps 1 and 2 are identical to those of $\mathrm{QPV}_{\mathrm{BB84}}$; verifier V_0 prepares a BB84 state and transmits it to the prover, while verifier V_1 simultaneously sends a classical bit z. Then:

3. The prover must send the qubit to V_0 if $z = 0$ and to V_1 if $z = 1$.

4. Upon receipt, the destination verifier, V_z, measures the returned qubit in the basis used by V_0. The verifiers *accept* the claimed position if the qubit arrives at the time consistent with *pos*, it reaches the correct verifier, and the measurement outcome corresponds to the original state; otherwise they *reject*.

Beyond its theoretical appeal, $\mathrm{QPV}_{\mathrm{rout}}$ is an attractive candidate for free-space implementations of QPV, where photons propagate at the vacuum speed of light, because the prover's hardware could, in principle, be as simple as a mirror or an optical switch.

Although substantial progress has been made in understanding the routing protocol [BFSS13, CM23, BCS22, ABM+24, ACCM24], two important questions have remained open:

(a) While a teleportation-based attack—analogous to the one that breaks $\mathrm{QPV}_{\mathrm{BB84}}$ when the adversaries pre-share a maximally entangled state—also applies to the routing protocol, a full security analysis in the No-PE model was still missing.

(b) The security of the protocol under *parallel repetition*, where the verifiers run m copies in parallel and issue a single accept/reject decision, had not been investigated.

We address both of these problems in Chapter 7. First, we show that any attack on $\mathrm{QPV}_{\mathrm{rout}}$ in the No-PE model reduces to a quantum cloning game with $k = 2$, that is, played by two parties who will take the role of the attackers, Alice and Bob. Using the optimal winning probability for this two-player game, we derive an upper bound on the attackers' success probability and thereby establish the security of the protocol. We also give an explicit attack that attains this bound, proving that the result is tight.

Secondly, we study the two-player quantum cloning game under m-fold parallel repetition—denoted $\mathrm{QPV}_{\mathrm{rout}}^{\times m}$—and show that the optimal winning probability decays exponentially in m. Applying the same reduction, we establish security for $\mathrm{QPV}_{\mathrm{rout}}^{\times m}$ in both the No-PE model and the $\mathrm{BE}(m)$ model, where the attackers pre-share fewer than $0.228m$ qubits.

Security proofs for quantum position verification (QPV) generally rely on one of two strategies. The first approach, used in Chapters 3 to 5 and 7, is to bound the success probability of any attack by a constant below one, and then amplify security through sequential repetition over time. The second approach, exemplified by the parallel repetition of $\mathrm{QPV}_{\mathrm{rout}}$ analyzed in Chapter 7, directly shows that the attack success probability becomes exponentially small in the number of parallel rounds.

Security guarantees for quantum position verification protocols generally follow the structure of the protocol repetition. In sequentially repeated protocols, such as those studied in Chapters 3 to 5 and 7, the strategy is to first bound the success probability of a single-round attack by a constant below one, and then amplify security through sequential repetition over time. In contrast, for protocols using parallel repetition, such as the parallel version of $\mathrm{QPV}_{\mathrm{rout}}$ analyzed in Chapter 7, security is shown by directly bounding the adversary's success probability as exponentially small in the number of parallel rounds. Since QPV

protocols rely crucially on tight timing constraints, parallel repetition offers a clear advantage: it allows the verifiers to *accept* or *reject* the claimed location based on a *single* interaction with the prover. Moreover, a single interaction is necessary in order to verify the location of a non-static prover.

Despite its advantages, previous parallel-repetition results for QPV suffered from two important limitations:

- they required quantum information to travel at the vacuum speed of light—a significant technological challenge (drawback (**LC**) in Figure 1.4); and
- they remained insecure if the adversaries were allowed to pre-share one EPR pair per qubit sent in the protocol, meaning that the resources needed to break the protocol are comparable to those needed to implement it (drawback (**EC**) in Figure 1.4).

These limitations are exemplified in the parallel repetition of the routing protocol analyzed in Chapter 7. For QPV to become practically viable, it is essential to overcome them.

In **Chapter 8**, we bridge the above-mentioned gap by analyzing the m-fold parallel repetition of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, denoted by $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$, and establishing its security. In this protocol, the classical string $z \in \{0,1\}^m$, which determines how the m qubits sent by V_0 must be measured, is computed as $z = f(x,y)$, where $x, y \in \{0,1\}^n$ are classical strings sent by V_0 and V_1, and $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ is a publicly known function.

While Unruh [Unr14] proved security for this protocol assuming a quantum random oracle (and that quantum communication occurs at the speed of light in vacuum), we prove that $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$ achieves exponentially decaying soundness *in the plain model*, provided that the adversaries pre-share a number of qubits linear in n. This fundamentally ties the security of the protocol to the size of the *classical* information, not the quantum resources. Moreover, only the classical messages need to travel at the speed of light—the quantum messages can propagate arbitrarily slowly. Thus, a single interaction suffices for secure position verification, even allowing for experimental imperfections: we prove that $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$ tolerates a per-qubit measurement error[3] of up to 3.6%, a figure compatible with current quantum technology.

As a by-product of our analysis, we show that the soundness for a single instance ($m = 1$) is at most 0.8539. This essentially matches the best known attack, which, as described above, consists of Alice measuring the qubit sent by V_0 in the Breidbart basis (see Figure 1.3), which succeeds with probability $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85355$. This improves upon the 0.98 soundness bound previously established in [BCS22], representing an improvement of nearly an order of magnitude in

[3]We also analyze a relaxed version of the protocol in which the prover needs to succeed only on a fraction of the rounds.

error tolerance. As a result, our bounds remain practically useful even when sequential repetition is employed.

In **Chapter 9**, we turn to continuous-variable (CV) QPV. Nearly all QPV schemes studied to date rely on finite–dimensional quantum systems; the only exceptions are the continuous-variable (CV) protocols of [QS15, AEFR+23]. Continuous-variable quantum systems are relevant for quantum communication and quantum-limited detection and imaging techniques, as they provide a quantum description of the propagating electromagnetic field. Much research has been conducted on continuous-variable quantum key distribution (QKD). Initially proposed using discrete [Ral99, Hil00, Rei00] and Gaussian [CLA01] representations of squeezed states, a range of techniques were subsequently introduced for Gaussian-encoded continuous-variable quantum key distribution (CV-QKD) using coherent states [GG02, GAW+03, GCW+03, WLB+04].

The major advantage of CV-QKD over its discrete-variable (DV) analog is *practicality*, see e.g. [WPGP+12]. In essence, CV systems are much simpler to handle and leverage several decades of experience in coherent optical communication technology, unlike DV systems, no true single-photon preparation or detection is necessary, which is still expensive and technically challenging (especially if photon number resolution is desired) [QLP+15]. In contrast, homodyne and heterodyne measurements are much easier and cheaper to implement [GAW+03, JKJL+13]. Much existing infrastructure is geared towards handling light at low-loss telecom wavelengths (1310nm, 1550nm), whereas an ideal single-photon source in these wavelength bands still has to be discovered, and frequency up-conversion is challenging and introduces new losses and errors [Kum90, TiHT+10].

Motivated by these practical advantages, the first CV analog of the BB84-based $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, based on coherent states, denoted by $\mathrm{QPV}_{\mathrm{coh}}$, was analyzed in [AEFR+23], with security established in the No-PE model. A round of the $\mathrm{QPV}_{\mathrm{coh}}$ protocol is described as follows:

1. The verifiers V_0 and V_1 randomly choose a bit $z \in \{0,1\}$, and they draw two independent random variables $(\xi, \xi^{\perp})$ from the Gaussian distribution $\mathcal{N}_{0,\sigma^2}$, for $\sigma \gg 1$. Verifier V_0 prepares a coherent state $|\phi\rangle$ with quadratures $(x_0, p_0) = (\xi\cos\theta + \xi^{\perp}\sin\theta,\ \xi\sin\theta - \xi^{\perp}\cos\theta)$, where $\theta = 0$ if $z = 0$ and $\theta = \frac{\pi}{2}$ if $z = 1$.

2. V_0 sends $|\phi\rangle$ to P, and the verifier V_1 sends z to P such that all information arrives at P simultaneously. All the information is required to travel at the speed of light.

3. Immediately, P performs a homodyne measurement on $|\phi\rangle$ in the direction $\theta = 0$ if $z = 0$ or $\theta = \frac{\pi}{2}$ if $z = 1$, resulting in a value $\xi_{\mathsf{P}} \in \mathbb{R}$. The prover broadcasts the classical result ξ_{P} to both verifiers at the speed of light.

4. If V_0 and V_1 receive their respective answers at the time corresponding with *pos* and both are equal to and consistent with ξ (see a specific test

in Chapter 9 to determine it), the verifiers *accept* the location. Otherwise, they *reject*.

It was also shown that, in a similar way as described above for $\mathrm{QPV}_{\mathrm{BB84}}$, a CV EPR pair and teleportation suffice to perfectly break the protocol. Building upon the ideas of [BFSS13, BCS22], similarly as done in Chapters 4 and 8, in Chapter 9, we introduce an extension of $\mathrm{QPV}_{\mathrm{coh}}$ that bypasses the CV EPR attack by hiding the bit z into two classical bit strings $x, y \in \{0,1\}^n$ sent by V_0 and V_1, respectively, so that they need to be combined via a boolean function f to determine z, that is $z = f(x, y)$.

Importantly, we are able to show that the protocol remains secure against the CV-EPR attack using teleportation and, even more, to any attackers who pre-share CV entangled states with a cutoff at the photon number linear in the size of the classical information n. Moreover, the protocol remains secure even if the quantum information is sent arbitrarily slowly. We also present an analysis of the protocol for non-zero levels of attenuation and excess noise in the CV channel. We thus demonstrate that the desirable entanglement-scaling property of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ carries over to continuous variables, thereby opening the door to experimentally feasible, free-space CV implementations of quantum position verification.

In summary, in this thesis, we address the core theoretical and practical challenges facing quantum position verification. We present protocols, both in discrete and continuous variables, that simultaneously bypass the major problems of QPV; we provide a generic method—that can be numerically solved—to analyze quantum correlations under losses and errors in experimental setups; we further analytically study non-local correlations in LSSD scenarios; and we demonstrate that a single-round interaction suffices to securely implement position verification, presenting two protocols that achieve this—one more fundamental in nature, and the other more realistic. Our results establish that QPV protocols can remain secure under experimental constraints, paving the way for practical and robust quantum position verification.

Chapter 2

Preliminaries

This chapter collects the mathematical and physical background used throughout the thesis. In Section 2.1, we introduce notation and standard tools from linear algebra and probability theory. In Section 2.2, we describe quantum systems along with their evolution and measurements, and we review key concepts from quantum information theory in both discrete-variable and continuous-variable settings. The chapter concludes with an overview of convex optimization techniques in Section 2.3, followed by an explanation of the Navascués–Pironio–Acín (NPA) hierarchy in Section 2.4.

2.1 Notation and background

We write $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ for the natural, integer, real and complex numbers, respectively. A *bit* x is an element in $\{0,1\}$. For bits $x, y \in \{0,1\}$, their sum modulo 2 is denoted by $x \oplus y$. For $k \in \mathbb{N}$ we use the shorthand $[k] := \{0, 1, \ldots, k-1\}$. Fix an integer $n \geq 1$.

(i) For a set $\mathcal{X}$ we denote its n-fold Cartesian product by $\mathcal{X}^{\times n} := \mathcal{X} \times \cdots \times \mathcal{X}$.

(ii) The set $\{0,1\}^n$ consists of all binary strings of length n. Writing $x = x_1 \ldots x_n$ with $x_i \in \{0,1\}$, the *Hamming weight* is $w_H(x) := |\{i \in [n] \mid x_i = 1\}|$.

(iii) For $x, y \in \{0,1\}^n$ their *Hamming distance* is $d_H(x,y) := |\{\, i \in [n] \mid x_i \neq y_i \,\}|$.

(iv) For $k \in \mathbb{N}$ with $0 \leq k \leq n$, the *binomial coefficient* is $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$.

(v) The set of permutations from $[n]$ to $[n]$ is denoted by S_n.

(vi) A square matrix $M \in \mathbb{C}^{n \times n}$ is *Hermitian* if $M^\dagger = M$, where † denotes the conjugate transpose. A Hermitian matrix is *positive semidefinite*, denoted by $M \succeq 0$, if $v^\dagger M v \geq 0$ for all $v \in \mathbb{C}^n$; equivalently, all its eigenvalues are non-negative.

(vii) For functions $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$ we write,

$$f(n) = O\big(g(n)\big)$$

if there exist constants $C > 0$ and $n_0 \in \mathbb{N}$ such that $f(n) \leq C\, g(n)$ for every $n \geq n_0$. We write

$$f(n) = \Omega\big(g(n)\big)$$

if there exist constants $c > 0$ and $n_0 \in \mathbb{N}$ such that $f(n) \geq c\, g(n)$ for all $n \geq n_0$. (Thus f grows at least as fast as g up to constant factors.)

For $a \in \mathbb{C}$ we denote its complex conjugate by a^*. The identity matrix, with dimension clear from context, is $\mathbb{I}$, for a matrix M, we denote its transpose by M^T, and if M is a square matrix, its trace will be denoted by $\mathrm{Tr}[M]$. The Kronecker delta is $\delta_{ij} = 1$ if $i = j$ and 0 otherwise, and the indicator function is $\mathbf{1}_*(\mathbf{a}) = 1$ if $* = a$ and 0 otherwise. We will use log and ln for the logarithms in base 2 and the natural logarithm (base e), respectively.

Let X be a discrete random variable taking values in a finite alphabet $\mathfrak{X} = \{\mathtt{x}_1, \ldots, \mathtt{x}_d\}$. Its distribution is specified by $p_{\mathtt{x}_i} = \Pr[X = \mathtt{x}_i]$, where $\Pr[\cdot]$ denotes the probability of the event $\cdot$, and can be written as the probability vector $\mathbf{p} = (p_{\mathtt{x}_1}, \ldots, p_{\mathtt{x}_d}) \in \mathbb{R}^d$. The set of all such distributions is the *probability simplex* $\Delta_{d-1} := \left\{\mathbf{p} \in \mathbb{R}^d \;\middle|\; \sum_{i=1}^d p_{\mathtt{x}_i} = 1,\ p_{\mathtt{x}_i} \geq 0\right\}$, a $(d-1)$-dimensional manifold. If $d = 2$, and then $\mathbf{p} = (p, 1-p)$, for $p \in [0,1]$, and its *binary entropy* is defined as

$$h_b(p) = \begin{cases} -p \log p - (1-p)\log(1-p), & \text{if } p \in (0,1), \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

Note that the values at 0 and 1 are given by the limit $\lim_{p \to 0^+} p \log p = 0$. The expected value of X will be denoted by $\mathbb{E}[X]$.

Let $d \in \mathbb{N}$, for a vector $v = (v_1 \ \ldots \ v_d)^T \in \mathbb{C}^d$, $\|v\|_2 = \sqrt{\sum_i |v_i|^2}$. For $M \in \mathbb{C}^{d \times d}$ and $1 \leq p \leq \infty$, the *Schatten p-norm* of M is

$$\|M\|_p := \Big(\mathrm{Tr}\Big[\big(\sqrt{M^\dagger M}\big)^p\Big]\Big)^{1/p}. \tag{2.2}$$

The two norms of interest in this thesis are:

- Trace norm (Schatten 1-norm): $\|M\|_1 = \mathrm{Tr}\Big[\sqrt{M^\dagger M}\Big]$.
- Operator norm (Schatten ∞-norm): $\|M\|_\infty = \sup_{v \in \mathbb{C}^d : \|v\|_2 = 1} \|Mv\|_2$, which evaluates the largest singular value of M. We will denote the operator norm by $\|M\|$ when the context is clear.

2.2 Quantum information

In this section, we provide a brief overview of the basic principles of quantum mechanics relevant to this thesis. For a comprehensive treatment, we refer the reader to [NC11].
For a complex linear space $\mathscr{H}$, an *inner product* on $\mathscr{H}$ is a map $\langle\cdot,\cdot\rangle : \mathscr{H} \times \mathscr{H} \to \mathbb{C}$ such that, for all $\psi, \phi, \varphi \in \mathscr{H}$ and $\alpha, \beta \in \mathbb{C}$,

(i) $\langle\psi, \alpha\phi + \beta\varphi\rangle = \langle\psi, \alpha\phi\rangle + \beta\langle\psi, \varphi\rangle$,

(ii) $\langle\psi, \phi\rangle = \langle\phi, \psi\rangle^*$,

(iii) $\langle\psi, \psi\rangle \geq 0$,

(iv) $\langle\psi, \psi\rangle = 0$ if and only if $\psi = 0$.

A complex linear space with an inner product is called an *inner product space*, and the inner product induces a norm on $\mathscr{H}$ defined by $\|\psi\| = \sqrt{\langle\psi, \psi\rangle}$. A *Hilbert space* $\mathcal{H}$ is a complete inner product space.

If $\mathcal{H}$ is finite-dimensional, then $\mathcal{H}$ is isomorphic to $\mathbb{C}^d$ for some $d \in \mathbb{N}$. We will use Dirac notation, writing $|\psi\rangle \in \mathcal{H}$ for vectors and $\langle\psi|$ for their conjugate transpose, so that $\langle\psi, \phi\rangle = \langle\psi|\phi\rangle$. For a d-dimensional Hilbert space $\mathcal{H}$, $|\psi\rangle \in \mathcal{H}$ in *ket* notation is represented by

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix}, \tag{2.3}$$

and the associated *bra* is given by

$$\langle\psi| = (\psi_1^* \dots \psi_d^*). \tag{2.4}$$

This mathematical formalism underlies the physical interpretation of quantum mechanics, beginning with its foundational principles. The first postulate of quantum mechanics states:

Every isolated physical system is associated with a complex Hilbert space $\mathcal{H}$, called its state space*. The physical state of the system is fully specified by a (unit-norm) state vector $|\psi\rangle \in \mathcal{H}$, with $\||\psi\rangle\| = 1$. Vectors that differ only by an overall (global) phase represent the same physical state.*

The simplest quantum–mechanical system, which takes a central role in quantum information, is the *qubit*. A qubit has a two-dimensional state space. Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis for this space. Any pure state can then be written as

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \tag{2.5}$$

with complex *amplitudes* $\alpha_0, \alpha_1 \in \mathbb{C}$. The requirement that the state vector be normalized, $\langle\psi|\psi\rangle = 1$, is therefore equivalent to

$$|\alpha_0|^2 + |\alpha_1|^2 = 1,$$

a condition often referred to as the *normalization condition* for state vectors. We will refer to $\{|0\rangle, |1\rangle\}$ as the computational basis where, as common in the literature,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.6}$$

The notion of *computational basis* naturally extends to larger Hilbert spaces $\mathcal{H}$. We will focus on finite-dimensional Hilbert spaces, that is, spaces of the form $\mathcal{H}$ isomorphic to $\mathbb{C}^d$ for some $d \in \mathbb{N}$. In this case, the computational basis is the orthonormal set $\{|i\rangle\}_{i\in[d]}$, where each basis vector $|i\rangle$ is given by

$$|i\rangle = (0 \ldots 0\ 1\ 0 \ldots 0)^T, \tag{2.7}$$

with the single non-zero entry (equal to 1) at position i, counting from 0, and ^{T} denotes the transpose. Any quantum state $|\psi\rangle \in \mathcal{H}$ can then be expressed as a linear combination of the basis vectors:

$$|\psi\rangle = \sum_{i\in[d]} \alpha_i |i\rangle, \tag{2.8}$$

where each $\alpha_i \in \mathbb{C}$, and $\sum_{i\in[d]} |\alpha_i|^2 = 1$, ensuring that $|\psi\rangle$ is a unit vector.

When working with multiple quantum subsystems, it is convenient to label each one by a *register name*. We use a subscript to indicate the register to which a state or operator belongs. For example, register A is described by the Hilbert space $\mathcal{H}_A \cong \mathbb{C}^{d_A}$, and a state in that register is written $|\psi\rangle_A$. When two quantum systems are combined, the state space of the composite system is the tensor product of the individual state spaces. Thus, if system A is described by the Hilbert space $\mathcal{H}_A \cong \mathbb{C}^{d_A}$ with state $|\psi\rangle_A$, and system B by $\mathbb{C}^{d_B}$ with state $|\phi\rangle_B$, the joint state lives in

$$\mathcal{H}_A \otimes \mathcal{H}_B \ \cong\ \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \ \cong\ \mathbb{C}^{d_A d_B}$$

and is written in Dirac notation as $|\psi\rangle_A \otimes |\phi\rangle_B$, or, when no confusion can arise, simply $|\psi\rangle|\phi\rangle$.

A quantum state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be *separable* if there exist states $|\psi_1\rangle_A \in \mathcal{H}_A$ and $|\psi_2\rangle_B \in \mathcal{H}_B$ such that $|\psi\rangle = |\psi_1\rangle_A \otimes |\psi_2\rangle_B$. Otherwise, the state is said to be *entangled*. An important example of an entangled state is the so-called *EPR pair* $|\Phi^+\rangle$, named after Einstein, Podolsky, and Rosen [EPR35], and often referred to as a *maximally entangled state*, which is given by

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big). \tag{2.9}$$

Having specified how quantum states are represented and how composite systems are formed, we next need a rule for how the state of a quantum system changes with time. For an *isolated* system this rule is encapsulated by the second postulate of quantum mechanics:

The time evolution of a closed quantum system is described by a unitary transformation. Specifically, if the system is in the state $|\psi_1\rangle$ at time t_1, then at a later time t_2, its state is $|\psi_2\rangle = U|\psi_1\rangle$, where U is a unitary operator depending only on the initial and final times, satisfying $U^\dagger U = U^\dagger U = \mathbb{I}$.

A single-qubit unitary that plays a central role in quantum information processing is the *Hadamard operator*,

$$H = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H^\dagger H = HH^\dagger = I. \tag{2.10}$$

Acting on the computational basis it produces the equal superpositions $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$, where the resulting states are defined as

$$|+\rangle := \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big), \qquad |-\rangle := \tfrac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

The pair $\{|+\rangle, |-\rangle\}$ forms an orthonormal basis, called the *Hadamard* basis. Since $H^2 = \mathbb{I}$, repeated application returns the qubit to the computational basis: $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$. A state from the set $\{|0\rangle, |1\rangle, |+\rangle|-\rangle\}$ will be referred to as a BB84 state, in reference to the set of states used in the BB84 quantum key distribution protocol [BB84].

Another fundamental quantum gate is the *controlled-NOT* (CNOT) gate, a two-qubit unitary that, when acting on the computational basis, flips the state of the *target* qubit if and only if the *control* qubit is in the state $|1\rangle$, that is, it acts as follows: $|x\rangle|y\rangle \to |x\rangle|x \oplus y\rangle$, for $x, y \in \{0, 1\}$. Notably, when the CNOT gate is applied the product state $|+\rangle|0\rangle$ it produces the maximally entangled state $|\Phi^+\rangle$.

We have seen how an isolated system evolves unitarily in time. In practice, an experimenter must sometimes *measure* the system. The statistical outcomes and state changes associated with such observations are summarized by the third postulate of quantum mechanics:

A measurement on a quantum system is specified by a finite (or countable) collection of semidefinite positive matrices $\{M_i\}_{i\in I}$, for a countable set I, acting on the system's Hilbert space, called measurement operators*. The index $i \in I$ labels the possible outcomes of the experiment. Let $\mathfrak{I}$ be the random variable representing the measurement outcome. For a system in the state $|\psi\rangle$, the probability of obtaining outcome i is given by $\Pr[\mathfrak{I} = i] = \langle\psi|M_i^\dagger M_i|\psi\rangle$, and, conditioned on this outcome, the post-measurement state is given by $|\psi_i\rangle = \frac{M_i|\psi\rangle}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}}$. The operators satisfy the* completeness equation *$\sum_{i\in I} M_i^\dagger M_i = \mathbb{I}$, which guarantees that $\sum_{i\in I} \Pr[\mathfrak{I} = i] = 1$.*

A particularly important class of quantum measurements is that of *projective* (or *von Neumann*) measurements, which arise when the measurement operators $\{M_i\}_{i\in I}$ are orthogonal projectors $\{\Pi_i\}_{i\in I}$. Each projector satisfies $\Pi_i^2 = \Pi_i$, and they are mutually orthogonal: $\Pi_i\Pi_j = \delta_{ij}\Pi_i$ for all $i, j \in I$.

For a single qubit, a measurement in the computational basis is described by the projectors

$$\Pi_0 = |0\rangle\langle 0|, \qquad \Pi_1 = |1\rangle\langle 1|, \tag{2.11}$$

so that for a general qubit state as in (2.5), the measurement outcomes occur with probabilities

$$\Pr[\mathfrak{I} = 0] = |\alpha_0|^2, \qquad \Pr[\mathfrak{I} = 1] = |\alpha_1|^2,$$

and the qubit collapses to $|0\rangle$ or $|1\rangle$, respectively. Similarly, a projective measurement in the Hadamard basis is described by $\Pi'_0 = |+\rangle\langle +|, \qquad \Pi'_1 = |-\rangle\langle -|$.

Both computational and Hadamard basis measurements will be relevant in this thesis. For convenience, we adopt the following notation: for $v, z \in \{0, 1\}$, we define

$$|v^z\rangle\langle v^z| := H^z|v\rangle\langle v|H^z, \tag{2.12}$$

where z indicates the measurement basis, and v, the outcome—$H^0 = \mathbb{I}$ and $H^1 = H$. Specifically, when $z = 0$, the measurement is in the computational basis, and when $z = 1$, it is in the Hadamard basis. Throughout, we will therefore speak of outcome $v = 0$ as corresponding to the states $|0\rangle$ or $|+\rangle$, and outcome $v = 1$ to the states $|1\rangle$ or $|-\rangle$, depending on the chosen basis.

A particularly important two-qubit measurement is the *Bell basis measurement*, which is a projective measurement onto the orthonormal basis of maximally entangled states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$,known as the *Bell states*, where $|\Phi^+\rangle$ is as in Equation (2.9) and $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. This measurement plays a central role in quantum teleportation, described in Chapter 1. Operationally, a Bell measurement can be implemented by applying a CNOT gate (with the first qubit as control), followed by a Hadamard gate on the control qubit, and measuring both qubits in the computational basis.

2.2.1 Density matrix formalism

So far, we have described quantum systems exclusively with *vectors* in a Hilbert space. However, there is an alternative equivalent formulation using *density matrices*. The latter formulation shows advantages when dealing for instance with uncertainties over pure quantum states that can be reproduced with a certain probability, or when considering subsystems of a global quantum state.

Let I be a finite alphabet, and suppose that a quantum system is prepared in the pure states $\{|\psi_i\rangle\}_{i\in I}$ with probability p_i. The tuple $\{p_i, |\psi_i\rangle\}_{i\in I}$ is called an

ensemble of pure states. The associated *density matrix* is defined by

$$\rho := \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{2.13}$$

A density matrix satisfies $\rho^\dagger = \rho$, $\rho \geq 0$, and $\mathrm{Tr}[\rho] = 1$. The density matrix of a pure state, that is of an ensemble $\{1, |\psi\rangle\}$, is the rank 1 matrix $|\psi\rangle\langle\psi|$. Throughout this thesis, we will use the term *quantum state* to refer to both a state vector (ket) in a Hilbert space and a density matrix. For $\mathcal{H}$, $\mathcal{H}'$ finite-dimensional Hilbert spaces, $\mathcal{B}(\mathcal{H}, \mathcal{H}')$ denotes the set of bounded operators from $\mathcal{H}$ to $\mathcal{H}'$ and $\mathcal{B}(\mathcal{H}) = \mathcal{B}(\mathcal{H}, \mathcal{H})$. The set of density matrices on $\mathcal{H}$ is denoted by $\mathcal{S}(\mathcal{H})$ i.e. $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \geq 0, \mathrm{Tr}[\rho] = 1\}$.

To compare quantum states, we often require a notion of distance that captures how distinguishable they are. One such measure is the *purified distance*, which is defined in terms of the *fidelity* between two states. For $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, their fidelity is defined as $F(\rho, \sigma) := \mathrm{Tr}\left[\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right]$, and the purified distance is given by

$$\mathcal{P}(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}. \tag{2.14}$$

One can see that the three previously mentioned postulates can be equivalently described by

(i) *First postulate*: "The physical state of an isolated system with Hilbert space $\mathcal{H}$ is described by a *density operator* $\rho \in \mathcal{B}(\mathcal{H})$".

(ii) *Second postulate:* "If a closed system evolves from time t_1 to t_2 to the state ρ_1 to ρ_2, it does so under a unitary operator U as follows: $\rho_2 = U\rho_1 U^\dagger$".

(iii) *Third postulate:* "The outcomes of the measurement operators $\{M_i\}_{i \in I}$ have associated probabilities $\Pr[\mathfrak{I} = i] = \mathrm{Tr}\left[M_i^\dagger M_i \rho\right]$, and the post-measurement state (conditioned on outcome i) is given by $\rho_i = \frac{M_i \rho M_i^\dagger}{\mathrm{Tr}\left[M_i^\dagger M_i \rho\right]}$".

2.2.2 Quantum information in continuous variables

While most of this thesis is based on the discrete-variable setting, we will also make use of continuous-variable quantum information techniques in Chapter 9. For a comprehensive overview of the continuous-variable framework, we refer the reader to the review article [WPGP+12].

A quantum system is called a *continuous-variable* system when its Hilbert space is infinite-dimensional. The canonical example of a CV system is a collection of N bosonic modes—such as the quantized electromagnetic field—mathematically equivalent to N quantum harmonic oscillators. For each mode, one defines the *quadrature operators* $\hat{\mathbf{x}}_i, \hat{\mathbf{p}}_i$, $i = 1, \ldots, N$, satisfying the canonical commutation relations $[\hat{\mathbf{x}}_i, \hat{\mathbf{p}}_j] = \sqrt{-1}\hbar\delta_{ij}$, where $\hbar$ is Planck's constant over 2π. These operators

have continuous spectra,

$$\hat{\mathbf{x}}_i|\mathbf{x}_i\rangle = \mathbf{x}_i|\mathbf{x}_i\rangle, \qquad \hat{\mathbf{p}}_i|\mathbf{p}_i\rangle = \mathbf{p}_i|\mathbf{p}_i\rangle, \qquad \mathbf{x}_i, \mathbf{p}_i \in \mathbb{R}. \tag{2.15}$$

It is convenient to collect the quadrature operators into the vector $\hat{\mathbf{r}} := (\hat{\mathbf{x}}_1, \hat{\mathbf{p}}_1, \ldots, \hat{\mathbf{x}}_N, \hat{\mathbf{p}}_N)^T$.

Any density operator ρ on an N-mode bosonic space can be represented by its *Wigner function* [Wig32]. We focus on *Gaussian states*, whose Wigner function is a multivariate Gaussian

$$W_{\mathrm{G}}(\mathbf{r}) = \frac{1}{\pi^N \sqrt{\det \Gamma}} \exp\!\big\{-(\mathbf{r}-\mathbf{d})^T \Gamma^{-1} (\mathbf{r}-\mathbf{d})\big\}, \tag{2.16}$$

where the *displacement vector* $d_i = \mathrm{Tr}[\rho \hat{r}_i]$, and the entries of the *covariance matrix* Γ are given by

$$\Gamma_{ij} = \mathrm{Tr}\big[\rho\big((\hat{r}_i - d_i)(\hat{r}_j - d_j) + (\hat{r}_j - d_j)(\hat{r}_i - d_i)\big)\big]. \tag{2.17}$$

Two measurement schemes play a central role in CV information:

- *Homodyne measurement.* This corresponds to measuring the quadrature of a mode, either the position $\hat{\mathbf{x}}$ or the momentum $\hat{\mathbf{p}}$, via the projective measurements $\{|\mathbf{x}\rangle\langle\mathbf{x}|\}_{\mathbf{x}\in\mathbb{R}}$ and $\{|\mathbf{p}\rangle\langle\mathbf{p}|\}_{\mathbf{p}\in\mathbb{R}}$, respectively. A homodyne measurement in a rotated quadrature direction $\theta \in [0, 2\pi)$ corresponds to measuring the operator $\hat{\mathbf{x}}_\theta := \hat{\mathbf{x}}\cos\theta + \hat{\mathbf{p}}\sin\theta$. For a Gaussian state with displacement (x_0, p_0) and variance σ^2 along that quadrature, the measurement outcome x_θ is distributed as $x_\theta \sim \mathcal{N}(x_0\cos\theta + p_0\sin\theta, \sigma^2)$, where $\mathcal{N}$ denotes the normal (Gaussian) distribution with the mean and variance given by its first and second arguments, respectively.

- *Heterodyne measurement.* This corresponds to a simultaneous measurement of both position and momentum quadratures of a mode, typically implemented by mixing the quantum mode with vacuum on a balanced beam splitter, and then performing homodyne measurements on the position and momentum quadratures of the resulting output modes, or in a θ and $\theta + \pi/2$ directions, instead of position and momentum (corresponding to $\theta = 0$). The heterodyne measurement of a one-mode Gaussian state with displacement (x_0, p_0) produces two Gaussian distributions, centered around $x_0/\sqrt{2}$ and $-p_0/\sqrt{2}$ respectively.

2.3 Convex optimization

Convex optimization provides a powerful framework for analyzing and solving a wide range of problems in quantum information theory. In this section, we briefly review the two classes of convex optimization problems most relevant to this thesis: linear programming (LP) and semidefinite programming (SDP).

Linear programming, will be particularly relevant in Chapter 6, and Semidefinite programming will play an important role in Chapters 3 to 5. We provide basic definitions and properties here, focusing on the aspects most frequently used in the later chapters. For a comprehensive introduction to convex optimization, including LP and SDPs, we refer the reader to [BV04, Wat18].

2.3.1 Linear programming

A *linear program* (LP) is an optimization problem in which both the objective function and the constraints are linear. The standard form of a linear program that optimizes over $x \in \mathbb{R}^n$, subject to m inequality and k equality constraints, is

$$\begin{aligned} \textit{Primal problem:} \qquad \text{minimize: } & \langle c, x\rangle = \sum_{i=1}^{n} c_i x_i \\ \text{subject to: } & Ax + b \geq 0, \\ & A_{\text{eq}} x + b_{\text{eq}} = 0, \end{aligned} \tag{2.18}$$

where $x, c \in \mathbb{R}^n$, $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$, $A_{\text{eq}} \in \mathbb{R}^{k\times n}$, $b_{\text{eq}} \in \mathbb{R}^k$. Its dual, which optimizes over $\lambda \in \mathbb{R}^m$ and $\nu \in \mathbb{R}^k$, is given by

$$\begin{aligned} \textit{Dual problem:} \qquad \text{maximize: } & -\left(\langle b, \lambda\rangle + \langle b_{\text{eq}}, \nu\rangle\right) = -\sum_{i=1}^{m} b_i \lambda_i - \sum_{i=1}^{k} b_{\text{eq},i} \nu_i \\ \text{subject to: } & A^{\mathsf{T}}\lambda + A_{\text{eq}}^{\mathsf{T}}\nu - c = 0, \\ & \lambda \geq 0. \end{aligned} \tag{2.19}$$

For any feasible x and (λ, ν)—that is, any x satisfying the primal constraints and any (λ, ν) satisfying the dual constraints—we have the *weak-duality* inequality

$$\langle c, x\rangle \;\geq\; -\Big(\langle b, \lambda\rangle + \langle b_{\text{eq}}, \nu\rangle\Big),$$

so every dual feasible point provides a lower bound on the primal objective. If at least one of the two problems is feasible and the other is feasible and bounded, *strong duality* is guaranteed: the primal and dual optimal solutions are equal (there is no duality gap). The necessary and sufficient optimality certificate is

$$A^{\mathsf{T}}\lambda + A_{\text{eq}}^{\mathsf{T}}\nu = c, \quad \lambda \geq 0, \quad \lambda_i \Big(Ax + b\Big)_i = 0 \;\text{ for all } i.$$

There exist efficient numerical algorithms for solving linear programs. The two principal families are the *simplex* method—introduced by Dantzig [Dan47] and improved through many modern variants—and polynomial-time *interior-point* methods, beginning with Karmarkar's algorithm [Kar84]. In contrast, no simple closed-form procedure is known for solving an arbitrary LP analytically. While one could, in principle, enumerate every vertex of the feasible polyhedron—an optimal solution is guaranteed to lie at (at least) one extreme point by the Fundamental Theorem of Linear Programming—the number of such vertices grows combinatorially, so exhaustive search is feasible only for toy instances. In Chapter 6 we will provide analytical solutions for certain LPs.

2.3.2 Semidefinite programming

In this section, we will follow the formalism in [Wat18]. Let $Herm(\mathbb{C}^{n\times n})$ and $Pos(\mathbb{C}^{n\times n})$ denote the sets of Hermitian and positive semidefinite matrices in $\mathbb{C}^{n\times n}$. Let $\Phi : \mathcal{B}(\mathbb{C}^n) \to \mathcal{B}(\mathbb{C}^m)$ be a *Hermiticity-preserving* map, and $A \in Herm(\mathbb{C}^{n\times n})$, $B \in \mathbb{C}^{m\times m}$. A *semidefinite program* (SDP), described by the triple (Φ, A, B), optimizes a linear functional over the cone of positive-semidefinite Hermitian matrices, similar to a LP over a real vector. The standard form of an SDP that optimizes over $X \in Pos(\mathbb{C}^{n\times n})$ is:

$$\begin{aligned} \textit{Primal problem:} \qquad \text{minimise: } & \mathrm{Tr}\big[A^\dagger X\big] =: \langle A, X\rangle \\ \text{subject to: } & \Phi(X) = B; \\ & X \succeq 0, \end{aligned} \tag{2.20}$$

Its dual, which optimizes over $Y \in Herm(\mathbb{C}^{m\times m})$, is given by

$$\begin{aligned} \textit{Dual problem:} \qquad \text{minimise: } & \mathrm{Tr}\big[B^\dagger Y\big] =: \langle B, Y\rangle \\ \text{subject to: } & \Phi^*(Y) \succeq B; \\ & Y \in Herm(\mathbb{C}^{m\times m}), \end{aligned} \tag{2.21}$$

where $\Phi*$ denotes the dual of Φ. The *feasible primal* and *dual* sets are defined as $\mathcal{A}_P = \{X \in Pos(\mathbb{C}^{n\times n}) : \Phi(X) = B\}$ and $\mathcal{B}_D = \{Y \in Herm(\mathbb{C}^{m\times m}) : \Phi^*(Y) \succeq A\}$. The optimum values associated to (2.20) and (2.21) are, respectively, defined as

$$\alpha = \sup_{X\in\mathcal{A}_P} \mathrm{Tr}\big[A^\dagger X\big] \quad \text{and} \quad \beta = \inf_{Y\in\mathcal{B}_D} \mathrm{Tr}\big[B^\dagger Y\big]. \tag{2.22}$$

Weak duality guarantees that for every primal-feasible $X \in \mathcal{A}_P$ and dual-feasible $Y \in \mathcal{B}_D$ one has $\mathrm{Tr}[A^\dagger X] \le \mathrm{Tr}[B^\dagger Y]$, so the optimal values satisfy $\alpha \le \beta$.

Slater's theorem [Sla59], states that if

1. α is finite and exists $Y \in Herm(\mathcal{C}^{m\times m})$ with $\Phi^*(Y) \succ A$, there exists $X \in \mathcal{A}_P$ such that $\alpha = \mathrm{Tr}[A^\dagger X]$,
2. β is finite and exists $X \in Pos(\mathcal{C}^{n\times n})$ with $\Phi(X) = B$, there exists $Y \in \mathcal{B}_D$ such that $\beta = \mathrm{Tr}[B^\dagger Y]$,

moreover, in both cases,

$$\alpha = \beta. \tag{2.23}$$

These optimizers satisfy the *complementary-slackness* relation $AX = \Phi^*(Y)X$, which serves as a succinct certificate of optimality.

Despite the absence of a generic analytic recipe for producing primal-dual solutions of SDPs—unlike LPs, enumeration of extreme points is hopeless because the cone of positive semi-definite matrices has infinitely many extremal points—it is nonetheless possible to solve moderate-scale SDPs to high precision with polynomial-time *interior-point* algorithms [NN94, Ali95, VB96].

2.4 Non-local games and the NPA hierarchy

Semidefinite programs arise in quantum information theory, in particular when optimizing over quantum states, measurements, or correlations subject to physical constraints. This connection becomes especially powerful in the study of non-local correlations and device-independent protocols, where one seeks to characterize the set of correlations attainable by quantum mechanics using convex optimization.

One of the central tools for characterizing quantum correlations in a device-independent framework is the *NPA hierarchy*, introduced by Navascués, Pironio, and Acín [NPA08]. The hierarchy provides a converging sequence of semidefinite programs that approximate the set of quantum correlations. In this section, we introduce the basic structure of the NPA hierarchy and explain how it connects to semidefinite programming.

In order to analyze non-local correlations, it is common to use the framework of *non-local games*, see e.g. [BCP+14]. Consider a bipartite system where two *distant* parties, Alice and Bob, have "black box" access to it. Let $\mathcal{X}, \mathcal{Y}, \mathcal{A}$, and $\mathcal{B}$ be finite (non-empty) alphabets. In a non-local game, Alice and Bob receive questions $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively, and their task is to produce outcomes $a \in \mathcal{A}$ and $b \in \mathcal{B}$. They win the game if $V(a, b|x, y) = 1$, for a certain publicly-known predicate $V : \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$. The behavior of the black box is completely characterized by the probability of getting outcomes a and b having measured x and y, $p(a, b|x, y)$, and the set of all probabilities, $\{p(a, b|x, y)\}$, encoded in a stochastic matrix $P \in \mathcal{B}(\mathbb{R}^{\mathcal{X}} \otimes \mathbb{R}^{\mathcal{Y}}, \mathbb{R}^{\mathcal{A}} \otimes \mathbb{R}^{\mathcal{B}})$, where $\mathcal{B}$ denotes the set of linear operators, such that $P(a, b|x, y) = p(a, b|x, y)$, is called behavior. The winning probability of the game specified by a given predicate V, if the questions are drawn from the distribution $q(x, y)$, is given by

$$\omega = \sum_{x,y,a,b} q(x, y)V(a, b|x, y)p(a, b|x, y) = \langle K, P\rangle, \tag{2.24}$$

where K is the matrix with entries given by $K(a, b|x, y) = q(x, y)V(a, b|x, y)$. Recall that $\langle K, P\rangle = \mathrm{Tr}[K^\dagger P]$.

2.4.1. Definition. *A behavior P is quantum if there exists a pure state $|\psi\rangle$ in a Hilbert space $\mathcal{H}$, a set of measurement operators $\{A_a^x\}_{a\in\mathcal{A}}$ for Alice, and a set of measurement operators $\{B_b^y\}_{b\in\mathcal{B}}$ for Bob such that for all $a \neq a' \in \mathcal{A}$ and $b \neq b' \in \mathcal{B}$,*

$$p(a, b|x, y) = \langle\psi|A_a^x B_b^y|\psi\rangle, \tag{2.25}$$

with the measurement operators satisfying

1. $A_a^{x\dagger} = A_a^x$ *and* $B_b^{y\dagger} = B_b^y$,
2. $A_a^x A_{a'}^x = 0$ *and* $B_b^y B_{b'}^y = 0$,
3. $\sum_{a\in\mathcal{A}} A_a^x = \mathbb{I}$ *and* $\sum_{b\in\mathcal{B}} B_b^y = \mathbb{I}$,

4. $[A_a^x, B_b^y] = 0$.

The set of all quantum (commuting) behaviors is denoted by $\mathcal{Q}_{co}$.

Similarly, a behavior P belongs to the set of *tensor product* quantum behaviors $\mathcal{Q}$ if the Hilbert space can be written as $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and the measurement operators for Alice and Bob act on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, and fulfil the same constraints as in Definition 2.4.1 (notice that commutativity is immediately implied because of the tensor product structure). Notice that by construction, $\mathcal{Q} \subseteq \mathcal{Q}_{co}$ and for finite dimensional Hilbert space, they turn out to be identical [NPA08]. The set $\mathcal{Q}$ corresponds to the set of correlations that the distant parties Alice and Bob can attain.

The maximum winning probability using a quantum behavior P is given by

$$\omega^*(\mathcal{G}) = \sup_{P \in \mathcal{Q}} \langle K, P \rangle. \tag{2.26}$$

In [NPA08], Navascués, Pironio, and Acín (NPA) introduced an infinite hierarchy of conditions satisfied by any set of quantum correlations $\mathcal{Q}_{\text{co}}$. Each level of the hierarchy can be tested using semidefinite programming, and the full hierarchy characterizes the set $\mathcal{Q}_{\text{co}}$.

We will now construct a positive semidefinite matrix G whose entries contain the values $p(a, b|x, y)$ from (2.25), and then impose linear constraints on G that capture the above conditions on the measurement operators A_a^x and B_b^y. The rows and columns of G will be indexed by

$$\Sigma_1 := \{\varepsilon\} \sqcup \Sigma_A \sqcup \Sigma_B \qquad \text{where} \qquad \Sigma_A := \mathcal{X} \times \mathcal{A}, \quad \Sigma_B := \mathcal{Y} \times \mathcal{B}. \tag{2.27}$$

For each $s \in \Sigma_1$, define a vector in $\mathcal{H}$ as follows:

$$|\psi(s)\rangle := \begin{cases} |\psi\rangle & \text{if } s = \varepsilon, \\ A_a^x |\psi\rangle & \text{if } s = (x, a) \in \Sigma_A, \\ B_b^y |\psi\rangle & \text{if } s = (y, b) \in \Sigma_B, \end{cases} \tag{2.28}$$

and let $G \in \mathbb{R}^{\Sigma_1 \times \Sigma_1}$ be the Gram matrix of these vectors:

$$G_{s,t} := \langle \psi(s) | \psi(t) \rangle, \qquad \forall s, t \in \Sigma_1. \tag{2.29}$$

Since G is a Gram matrix, it is clearly positive semidefinite:

$$G \succeq 0. \tag{2.30}$$

Notice that G contains all of the values $p(a, b|x, y)$ from Equation (2.25), as well as some additional values such as $\langle \psi | \psi \rangle$, $\langle \psi | A_a^x | \psi \rangle$, and others.

Because of the various relations among the measurement operators A_a^x and B_b^y listed earlier, the Gram matrix G is subject to the following linear constraints:

1. Since $|\psi\rangle$ is a normalized state, $\langle\psi|\psi\rangle = 1$ and thus

$$G_{\varepsilon,\varepsilon} = 1. \tag{2.31}$$

2. Due to the completeness relations $\sum_{x\in\mathcal{X}} A_a^x = \mathbb{I} = \sum_{y\in\mathcal{Y}} B_b^y$, we have that for any vector $|v\rangle \in \mathcal{H}$, $\sum_{x\in\mathcal{X}}\langle\psi|A_a^x|v\rangle = \langle\psi|v\rangle$ and $\sum_{x\in\mathcal{X}}\langle v|A_a^x|\psi\rangle = \langle v|\psi\rangle$, and similarly for B_b^y.

   Letting $|v\rangle = |\psi(s)\rangle$ for some $s \in \Sigma_1$, this translates to

$$\sum_{x\in\mathcal{X}} G_{(x,a),s} = G_{\varepsilon,s}, \qquad \sum_{x\in\mathcal{X}} G_{s,(x,a)} = G_{s,\varepsilon}, \qquad \forall a \in \mathcal{A}, s \in \Sigma_1, \tag{2.32}$$

$$\sum_{y\in\mathcal{Y}} G_{(y,b),s} = G_{\varepsilon,s}, \qquad \sum_{y\in\mathcal{Y}} G_{s,(y,b)} = G_{s,\varepsilon}, \qquad \forall b \in \mathcal{B}, s \in \Sigma_1. \tag{2.33}$$

3. Since within each measurement the projectors are orthogonal, we also have $\langle\psi|A_a^x A_{a'}^x|\psi\rangle = 0 = \langle\psi|B_b^y B_{b'}^y|\psi\rangle$ and thus

$$G_{(x,a),(x',a)} = 0, \qquad \forall x \neq x' \in \mathcal{X}, a \in \mathcal{A}, \tag{2.34}$$

$$G_{(y,b),(y',b)} = 0, \qquad \forall y \neq y' \in \mathcal{Y}, b \in \mathcal{B}. \tag{2.35}$$

4. Since A_a^x are projectors, $\langle\psi|A_a^x A_a^x|\psi\rangle = \langle\psi|A_a^x|\psi\rangle$ and likewise for B_b^y, so

$$G_{(x,a),(x,a)} = G_{(x,a),\varepsilon} = G_{\varepsilon,(x,a)}, \qquad \forall x \in \mathcal{X}, a \in \mathcal{A}, \tag{2.36}$$

$$G_{(y,b),(y,b)} = G_{(y,b),\varepsilon} = G_{\varepsilon,(y,b)}, \qquad \forall y \in \mathcal{Y}, b \in \mathcal{B}. \tag{2.37}$$

5. Since the two sets of projectors commute, $\langle\psi|A_a^x B_b^y|\psi\rangle = \langle\psi|B_b^y A_a^x|\psi\rangle$, we have

$$G_{(x,a),(y,b)} = G_{(y,b),(x,a)}, \qquad \forall x \in \mathcal{X}, y \in \mathcal{Y}, a \in \mathcal{A}, b \in \mathcal{B}. \tag{2.38}$$

Let $\mathcal{Q}_1 \subset \mathbb{R}^{\mathcal{X}\times\mathcal{X}\times\mathcal{A}\times\mathcal{B}}$ denote the set of all correlations Q such that there exists a matrix $G \in \mathbb{R}^{\Sigma_1\times\Sigma_1}$ which satisfies

$$G_{(x,a),(y,b)} = p(a,b|x,y), \qquad \forall x \in \mathcal{X}, y \in \mathcal{Y}, a \in \mathcal{A}, b \in \mathcal{B}, \tag{2.39}$$

as well as $G \succeq 0$ and the linear constraints in (2.31) to (2.38). Note that deciding the membership of Q_{co} in $\mathcal{Q}_1$ is a semidefinite feasibility problem—it requires finding a positive semidefinite matrix $G \succeq 0$ subject to linear constraints.

Since, by construction, $\mathcal{Q} \subseteq \mathcal{Q}_1$, we have that

$$\omega := \sup_{P\in\mathcal{Q}} \langle K, Q\rangle \leq \sup_{P\in\mathcal{Q}_1} \langle K, Q\rangle =: \omega_1. \tag{2.40}$$

The value ω_1 corresponds to the bound on the optimal winning probability of the game given by the *first level* of the NPA hierarchy. We can compute it by a semidefinite program as follows.

Define a symmetric matrix $H \in \mathbb{R}^{\Sigma_1 \times \Sigma_1}$ with entries

$$H_{(a,x),(b,y)} := H_{(y,b),(a,x)} := \frac{1}{2} K(a,b,x,y), \qquad \forall a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y} \tag{2.41}$$

and 0 otherwise. Then $\langle K, Q \rangle = \mathrm{Tr}[HG]$ is a linear function of G, so we can compute the value of $\omega_1(\mathcal{G})$ via a semidefinite program that maximizes $\mathrm{Tr}[HG]$ over all positive semidefinite matrices G satisfying the conditions listed above.

The *second level* of the NPA hierarchy is obtained by a similar SDP that involves a larger *extended* Gram matrix G whose rows and columns are indexed by[1]

$$\Sigma_2 := \Sigma_1 \sqcup (\Sigma_A \times \Sigma_A) \sqcup (\Sigma_A \times \Sigma_B) \sqcup (\Sigma_B \times \Sigma_B). \tag{2.42}$$

We extend the original set of vectors $|\psi(s)\rangle$ from Equation (2.28) by defining new vectors for the remaining elements $s \in \Sigma_2 \setminus \Sigma_1$ as follows:

$$|\psi(s)\rangle := \begin{cases} A_a^x A_{a'}^{x'} |\psi\rangle & \text{if } s = ((x,a),(x',a')) \in \Sigma_A \times \Sigma_A, \\ A_a^x B_{b'}^{y'} |\psi\rangle & \text{if } s = ((x,a),(y',b')) \in \Sigma_A \times \Sigma_B, \\ B_b^y B_{b'}^{y'} |\psi\rangle & \text{if } s = ((y,b),(y',b')) \in \Sigma_B \times \Sigma_B. \end{cases} \tag{2.43}$$

As before in Equation (2.29), the entries of the extended G are also given by inner products $\langle \psi(s) | \psi(t) \rangle$ for all $s, t \in \Sigma_2$, and we impose additional linear constraints on them similar to those in Equations (2.31) to (2.38) to capture the fact that Alice and Bob's operators describe mutually commuting projective measurements.

We denote by $\mathcal{Q}_2 \subset \mathbb{R}^{\mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y}}$ the set of all correlations Q for which there exists an extended Gram matrix $G \in \mathbb{R}^{\Sigma_2 \times \Sigma_2}$ that agrees with Q on Σ_1, see Equation (2.39), and which satisfies the linear constraints for the second level of the NPA hierarchy. Note that $\mathcal{Q}_2 \subseteq \mathcal{Q}_1$ since the second level imposes additional constraints compared to the first level. Intuitively, the *ℓ-th* level of the NPA hierarchy is obtained by considering the Gram matrix of the vectors of the level $\ell - 1$ plus new vectors obtained from products of ℓ projectors, see [Wat21, NPA08] for a more formal description. The hierarchy is complete in the sense that $\lim_{\ell \to \infty} \mathcal{Q}_\ell = \mathcal{Q}_{co}$.

In this thesis, we will consider the SDP for an intermediate level of the NPA hierarchy between $\mathcal{Q}_1$ and $\mathcal{Q}_2$, the so-called level "1+AB", where G is the Gram matrix for the set of vectors labelled by

$$\Sigma_{1+AB} := \Sigma_1 \sqcup (\Sigma_A \times \Sigma_B). \tag{2.44}$$

[1] We omit $\Sigma_B \times \Sigma_A$ since Alice and Bob's operators commute.

Chapter 3
Loss in single-qubit position verification

Quantum position verification (QPV) protocols typically encode quantum states onto photons—as natural carriers that travel at the speed of light—to transmit information between the verifiers and the prover. In practice, a significant fraction of these photons is lost during transmission, as discussed in Chapter 1; recall that, for instance, at the C-band telecom wavelength ($\sim 1550\,\mathrm{nm}$), state-of-the-art single-mode optical fibers exhibit attenuation of approximately $0.15\,\mathrm{dB/km}$ [CZD19]. This accounts only for transmission loss; additional losses due to coupling inefficiencies and imperfect detectors must also be considered. Crucially, such losses can severely compromise the security of QPV protocols.

In this chapter, we analyze the exact loss tolerance of one of the most widely studied position-verification protocols in the literature: $\mathrm{QPV}_{\mathrm{BB84}}$. We show that by explicitly distinguishing loss from noise—rather than treating it merely as another form of error—security in the No Pre-shared Entanglement (No-PE) model can be retained even when nearly half of the quantum messages are lost. However, due to the structure of the protocol, there is a fundamental threshold: $\mathrm{QPV}_{\mathrm{BB84}}$ becomes insecure once the loss rate reaches 50%.

To address this limitation, we introduce a family of extensions of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol that offer improved resilience to photon loss, thereby enabling QPV to be implemented over longer distances and in more lossy environments.

The results presented in this chapter are based on the following publication:

- *Phys. Rev. Lett. 131, 140802*, "Single-Qubit Loss-Tolerant Quantum Position Verification Protocol Secure against Entangled Attackers," by Llorenç Escolà-Farràs, and Florian Speelman [EFS23].

3.1 Introduction

The $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, which will play a central role in this chapter, was originally introduced in [KMS11]. As outlined in Chapter 1, the protocol proceeds as follows: one verifier, V_0, sends a BB84 state to the prover, while the other verifier, V_1, simultaneously sends a classical bit $z \in \{0,1\}$ indicating the basis (computational or Hadamard) in which the prover must measure the state. The prover immediately measures the incoming qubit accordingly and broadcasts the measurement outcome to both verifiers. All communication is assumed to occur at the speed of light.

As discussed in Chapter 1, this protocol can be perfectly broken by adversaries who pre-share a single EPR pair. This observation motivated the study of the protocol in the *No Pre-shared Entanglement* (No-PE) model, where the adversaries are not allowed to share any entanglement prior to the protocol's execution. Security in this model is motivated by the fact that generating and distributing high-quality entanglement over long distances remains technologically challenging, so the No-PE model captures currently practical limitations. In this setting, the protocol was shown to be secure in [BCF+14], with soundness amplification under parallel repetition provided in [TFKW13]. A tighter bound was later derived in [RG15], albeit in a slightly weaker model where the adversaries are allowed a round of classical communication rather than quantum, making direct comparisons difficult.

Despite its theoretical appeal, implementing $\mathrm{QPV}_{\mathrm{BB84}}$ in practice faces serious challenges, especially regarding photon loss in experimental setups. Two principal approaches have emerged in the literature for addressing loss:

(i) *Fully loss-tolerant protocols.* This class of protocols remains secure under arbitrarily high photon loss, with examples in [LXS+16, ABSL22b, ABSL22a]. While promising for realistic implementations, these protocols have two notable limitations: (a) they tolerate only a limited amount of adversarial entanglement [ABSL22a], and (b) they require near-light-speed transmission of quantum information.

(ii) *Partially loss-tolerant protocols.* In this approach, one explicitly bounds the joint loss and error rates that an attacker can induce, with examples in [QS15] and [Spe16b, Chapter 5].

Both limitations (a) and (b) persist for the protocols analyzed in this chapter. However, with a slight modification—namely, the introduction of classical information alongside quantum messages—we resolve these issues in Chapter 4. Notably, this type of modification is incompatible with fully loss-tolerant protocols, which rely solely on quantum communication.

Since protocols are typically designed to tolerate a certain level of *error*, and since we aim for robustness against photon loss, could the latter not simply be

treated as another form of noise? In this chapter, we argue that distinguishing these parameters is essential because they differ fundamentally in their quantitative impact. We analyze the security of $\mathrm{QPV}_{\mathrm{BB84}}$ in the presence of photon loss, focusing on adversaries in the No-PE model. The best existing bounds in the lossless setting stem from reductions to *monogamy-of-entanglement* (MoE) games [TFKW13]. We extend this framework with binary answers to allow for a third possible response—loss—and reduce the soundness analysis to computing the optimal winning probability in such an extended game. We show that a naive mixture of optimal strategies for the extreme cases yields the best attack.

Our analysis relies on a three-party scenario: a referee and two players (who will take the role of the adversaries), where the referee performs a fixed measurement and the players aim to guess the outcome. While SDP relaxations for two-party scenarios are well-established [Weh06, NPA08], three-party settings introduce new complications. We overcome these using the Navascués–Pironio–Acín (NPA) hierarchy [NPA08] combined with additional linear constraints that we derive from the nature of the protocol.

We then examine a natural extension of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, in which V_0 and V_1 encode the qubit in $k \geq 3$ distinct bases. Although tightness is not guaranteed for $k \geq 3$, our numerical analysis reveals that increasing the number of encoding bases significantly improves loss tolerance. For example, with $k = 5$ and low measurement error, the protocol remains secure even when nearly 80% of the photons are lost.

A similar extension was studied by Qi and Siopsis [QS15], but under a more restrictive adversarial model. Their analysis assumes that attackers immediately perform a projective measurement on each incoming qubit and communicate only classically. By contrast, our framework allows arbitrary local quantum operations and a single round of quantum communication. By reducing the problem to an (extended) monogamy-of-entanglement game, we capture this broader set of strategies—an expansion that, as shown in [ABSL22a], can fundamentally affect security guarantees. Moreover, our protocol works for any number of encoding bases $k \geq 3$, while the construction in [QS15] requires a large number of bases.

This chapter also improves upon the unpublished results of [Spe16b, Chapter 5], which first employed SDP techniques to analyze QPV under photon loss. Their numerical estimates were less tight—for instance, their bound for $\mathrm{QPV}_{\mathrm{BB84}}$ deviated by nearly a factor of two from the values obtained in our analysis. Our approach sharpens these bounds substantially.

The method we develop for enabling SDP analysis in a three-party setting has potential applications beyond QPV and may extend to a broader class of cryptographic tasks that can be framed in a similar game-theoretic language. This broader applicability lies beyond the scope of this thesis, and we refer the reader to [EFS23] for an illustration of its use in quantum key distribution.

3.2 The $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ protocol

In this section, we describe the lossy version of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol and its generic attack in the No-PE model. We will use η to denote the total transmission rate of photons from V_0, who sends qubits, to P. In addition, we assume that an honest prover to have error rate p_{err}, due to imperfections such as measurement errors or noise in the quantum channel transmitting the qubits. We define one round of the lossy-$\mathrm{QPV}_{\mathrm{BB84}}$ protocol as follows:

3.2.1. Definition. *Let η denote the transmission rate of the qubits sent from V_0 to P. We define one round of the lossy-BB84 QPV protocol, denoted by $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, as follows:*

1. *V_0 and V_1 secretly agree on random bits $v, z \in \{0,1\}$. Then, V_0 prepares the qubit state $|\phi\rangle = H^z|v\rangle \in \{|0\rangle, |1\rangle, |+\rangle\,|-\rangle\}$.*

2. *V_0 and V_1 send $|\phi\rangle$ and z to P, respectively, with both signals propagating at the speed of light in vacuum. The two verifiers coordinate so that the qubit and the classical bit arrive at pos simultaneously.*

3. *Immediately, P measures the received qubit in the basis z and broadcasts her outcome, either 0 or 1, to V_0 and V_1. If she did not receive the qubit, i.e. the photon was lost, she sends $\perp$. Therefore, the possible answers from P are $v_{\mathsf{P}} \in \{0,1,\perp\}$.*

4. *If*

   (a) *V_0 and V_1 receive their respective answers at the time corresponding with pos, and they are equal, i.e. both receive the same v_{P}, then, if*

   - *$v_{\mathsf{P}} = v$, the verifiers record 'Correct', denoted by 'c',*
   - *$v_{\mathsf{P}} = 1 - v$, the verifiers record 'Wrong', denoted by 'w',*
   - *$v_{\mathsf{P}} = \perp$, the verifiers record 'No photon', denoted by '$\perp$',*

   (b) *otherwise, they record 'Abort', denoted by '↯', and abort the protocol rejecting the location.*

See Figure 1.1 for a schematic of the original $\mathrm{QPV}_{\mathrm{BB84}}$ protocol. By replacing the prover's output $v \in \{0,1\}$ with $v_{\mathsf{P}} \in \{0,1,\perp\}$, the same figure represents steps 2 and 3 of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$. Note that setting $\eta = 1$ and $p_{\mathrm{err}} = 0$ recovers the original $\mathrm{QPV}_{\mathrm{BB84}}$ protocol.

In order to *accept* or *reject* the location, the verifiers run r sequential rounds of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$. Let r_{C}, r_{W}, $r_{\perp}$ and $r_{↯}$ denote the number of times that the verifiers output 'Correct', 'Wrong', 'No photon' and 'Abort', respectively, after

the r rounds. Given transmission rate η and error probability p_{err}, the verifiers expect

$$\begin{aligned} r_{\mathrm{C}} &\approx r\eta(1-p_{err}), & r_{\mathrm{W}} &\approx r\eta p_{err}, \\ r_{\perp} &\approx r(1-\eta), & r_{\lightning} &= 0. \end{aligned} \tag{3.1}$$

The symbols $\approx$ are due to the fact that in an implementation, the above values would only be reached for $r \to \infty$. To make a decision based on the observed outcomes, one must first define what it means for them to be sufficiently "close" to the expected values in (3.1). To this end, we introduce a binary test (Definition 3.2.2) that determines whether the prover's location should be *accepted* or *rejected* based on the received data.

Assume that after r sequential repetitions, the verifiers did not receive any 'Abort' answers, otherwise they *reject* the location. Notice that the verifiers remain strict with $r_{\lightning}$, since an honest party would never send a different answer to V_0 that to V_1, and using current technology, her answers will arrive on time, and therefore a single '$\lightning$' answer will suffice to reject the location of the prover. Denote by $\mathbf{a}_i \in \{\mathrm{C}, \perp, \mathrm{W}\}$ whether the answer they recorded in the round i was 'Correct', 'No photon', or 'Wrong'. Consider the payoff function $T_i(\mathbf{a}_i) = \sin^2\frac{\pi}{8}\mathbf{1}_{\mathrm{C}}(\mathbf{a}_i) - \sin^2\frac{\pi}{8}\mathbf{1}_{\perp}(\mathbf{a}_i) - \cos^2\frac{\pi}{8}\mathbf{1}_{\mathrm{W}}(\mathbf{a}_i)$, for every round i of the protocol. Let

$$\Gamma_r = \sum_{i=1}^{r} T_i(\mathbf{a}_i), \tag{3.2}$$

be the total *score* after r rounds. Fix a parameter $\varepsilon_{\mathrm{h}} > 0$, which determines the confidence level of the test that we introduce.

3.2.2. Definition. *Let* $\varepsilon_h > 0$. *For the* $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ *protocol executed sequentially* r *times, we define the acceptance test* $\mathsf{T}^{r\mathrm{BB84}}_{\varepsilon_h}$*, also referred to as the decision criterion, as follows: the verifiers* accept *the prover's location if*

$$\Gamma_r \geq r(\alpha - \delta), \tag{3.3}$$

where $\delta = \sqrt{\frac{\cos^4\frac{\pi}{8}\ln(1/\varepsilon_h)}{r}}$*. Otherwise, they* reject.

We will next see that the test $\mathsf{T}^{r\mathrm{BB84}}_{\varepsilon_{\mathrm{h}}}$ is *complete*: an honest implementation of the protocol will be accepted, except with negligible probability. For an honest prover (hp), we have that, for every round i,

$$\mathbb{E}[T_i^{hp}] = \sin^2\frac{\pi}{8}\eta(1-p_{err}) - \sin^2\frac{\pi}{8}(1-\eta) - \cos^2\frac{\pi}{8}\eta p_{err} =: \alpha(\eta, p_{err}), \tag{3.4}$$

and therefore, $\mathbb{E}[\Gamma_r^{hp}] = r\alpha$. For simplicity, we will assume the dependence on η and p_{err} in α implicit. Then, by Hoeffding's inequality [Hoe63], see Lemma 3.2.3, an honest prover will be accepted except with probability at most ε_{h}.

3.2.3. Lemma. *Let $T_1, \ldots, T_r$ be independent bounded random variables with $T_i \in [x_a, x_b]$, for all $i \in \{1, \ldots, r\}$, with $-\infty < x_a \leq x_b < \infty$. Then, for all $\delta \geq 0$, the following holds:*

$$\Pr\left[\frac{1}{r}\sum_{i=1}^{r}(T_i - \mathbb{E}[T_i]) \geq \delta\right] \leq e^{-\frac{2r\delta^2}{(x_b - x_a)^2}}. \tag{3.5}$$

In addition, we will see that for any attackers in the No-PE model—which, as discussed in Chapter 1, imposes only that no entanglement is shared prior to the execution of the protocol in each round—the test $\mathsf{T}^{r\mathrm{BB84}}_{\varepsilon_{\mathrm{h}}}$ is *sound*: any attackers in this model will be rejected with high probability—in particular, we will show exponentially high probability (in r). This test is engineered from the analysis of the correlations attainable by attackers in Section 3.2.1, ensuring that they are rejected except with negligible probability; see the proof of Theorem 3.2.11 for details of its construction.

We say that a protocol is *secure* in a given model if it admits a test that is both complete and sound (for any adversaries acting according to the model). Next, we will show that $\mathsf{T}^{r\mathrm{BB84}}_{\varepsilon_{\mathrm{h}}}$ fulfills both conditions for a certain range of transmission rate η and qubit error p_{err} and thus showing that $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ is secure.

In order to prove security for $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, in Section 3.2.1 we first show that, in a round, for a range of values of η and p_{err}, any adversaries in the No Pre-shared Entanglement (No-PE) model are unable to reproduce the outcome probabilities specified in (3.1). This provides intuitive evidence that attackers cannot mimic the behavior of an honest prover, and that their actions can be statistically distinguished. We will later show that the test $\mathsf{T}^{r\mathrm{BB84}}_{\varepsilon_{\mathrm{h}}}$ achieves this.

For the security analysis, we will consider the *purified* version of $\mathrm{QPV}_{\mathrm{BB84}}$, which is equivalent to it. In this version, instead of V_0 sending BB84 states, V_0 prepares an EPR pair $|\Phi^+\rangle_{VP}$ and sends the register P to the prover and keeps register V. At a later moment, V_0 performs the measurement $\{H^z|v\rangle\langle v|_V H^z\}_{v\in\{0,1\}}$ in his register V. In this way, the verifiers delay the choice of basis in which the qubit is encoded, which, in contrast to the above *prepare-and-measure* version, will make any attack independent of the state sent by V_0.

Whereas it is well-known that adversaries sharing an unbounded amount of entanglement can always successfully break any QPV protocol [BCF+14], the proof of the security of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol under attackers that do not pre-share entanglement [BCF+14] opened a branch of study, motivated by adversarial models that restrict attackers in a more realistic way. The most generic attack to $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ (purified version) in the No-PE model consists of:

1. Alice and Bob prepare an arbitrary quantum state σ_{A_0}, and Alice holds it. Since the attackers do not pre-share entanglement, any quantum operation that Bob could later perform as a function of z can be included in Alice's operation (see e.g. [BCF+14, TFKW13]).

2. Alice intercepts the qubit register P, and applies an arbitrary quantum channel $\mathcal{E}_{PA_0\to AB}$ to it, and to σ_{A_0}. The subscript $PA_0 \to AB$ indicates that the map has input and output registers PA_0 and AB, respectively. Let ρ_{VAB} be the resulting state, that is, $\mathbb{I}_V \otimes \mathcal{E}_{PA_0\to AB}(|\Phi^+\rangle\langle\Phi^+|_{VP} \otimes \sigma_{A_0}) = \rho_{VAB}$. Alice possesses registers A and B, and V_0 holds V. On the other side, Bob intercepts z, and copies it.

3. Alice keeps register A of ρ and sends register B to Bob. Bob keeps a copy of z and sends a copy to Alice.

4. After one round of simultaneous communication, each party performs a POVM $\{A^z_a\}_{a\in\{0,1,\perp\}}$ and $\{B^z_b\}_{b\in\{0,1,\perp\}}$, on registers A and B of the state ρ, and they send answers a, b, respectively, to their corresponding closest verifier.

See Figure 3.1 for a schematic representation of a generic attack to $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ in the No-PE model. The tuple $\mathbf{S}_\eta := \{\rho, A^z_a, B^z_b\}_{z,a,b}$ will be called a *strategy* for $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$.

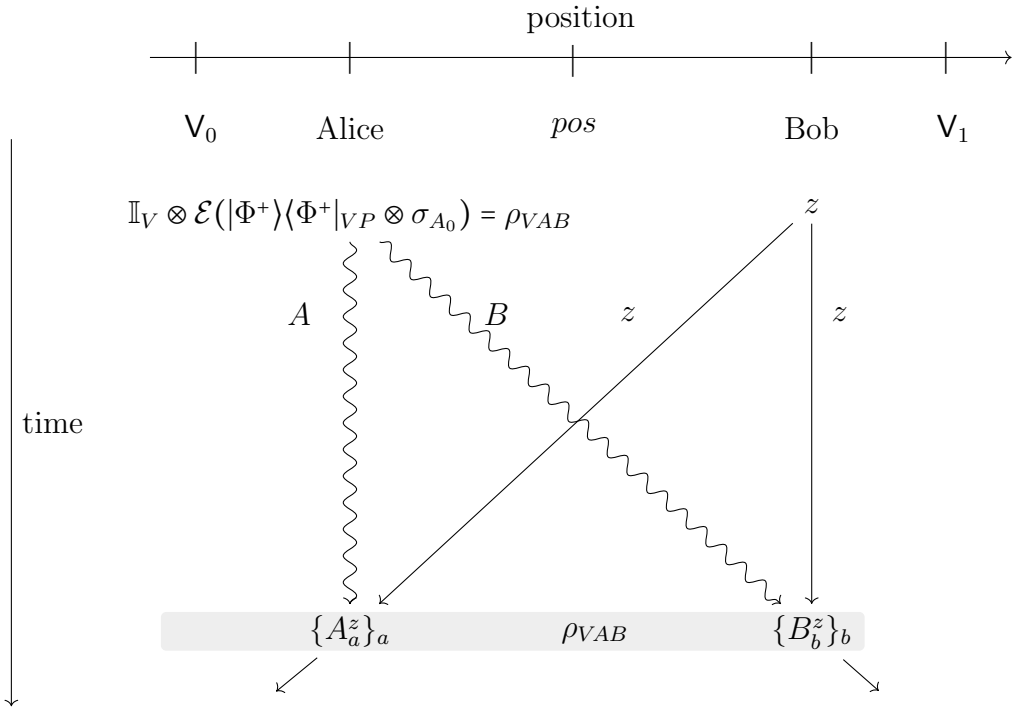


Figure 3.1: Schematic representation of a generic attack to $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ in the No-PE model. Straight and undulated lines represent classical and quantum information, respectively. The gray-shaded region represents the state ρ_{VAB}.

To illustrate how photon loss can be exploited by adversaries, we briefly recall the simple guessing attack discussed in Chapter 1. Suppose the verifiers expect

that an honest prover would have a transmission rate of at most $\eta \leq \frac{1}{2}$, meaning that half or more of the photons are lost in transit. In contrast, since the adversaries may position themselves closer to the verifiers and intercept most of the transmitted photons, we give them the extra power of intercepting all of them. The attack proceeds as follows: Alice selects a random bit $\tilde{z} \in \{0,1\}$, measures the received qubit in the $\tilde{z}$-basis, and forwards the outcome and $\tilde{z}$ to Bob. After a single round of simultaneous communication, both attackers know whether the guess was correct. If $\tilde{z} = z$, they return the measurement outcome; otherwise, they claim photon loss, i.e. output $\perp$. Since the basis guess is correct with probability 1/2, this strategy succeeds with probability 1/2—matching the expected success rate of an honest prover under $\eta = \frac{1}{2}$. We refer to this strategy as the *guessing strategy*, denoted $\mathbf{S}_{\text{guess}}$.

The probabilities that the verifiers, after the attackers' actions (for the random variable V_{AB}) record 'Correct', 'Wrong, 'No photon', and 'Abort' (different answers) are thus, respectively, given by

$$q_{\mathrm{C}} := \Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{C}] = \frac{1}{2} \sum_{a,z\in\{0,1\}} \mathrm{Tr}[\rho V_a^z \otimes A_a^z \otimes B_a^z], \tag{3.6}$$

$$q_{\mathrm{W}} := \Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{W}] = \frac{1}{2} \sum_{a,z\in\{0,1\}} \mathrm{Tr}[\rho V_a^z \otimes A_{1-a}^z \otimes B_{1-a}^z], \tag{3.7}$$

$$q_{\perp} := \Pr[\mathrm{V}_{\mathrm{AB}} = \perp] = \frac{1}{2} \sum_{z\in\{0,1\}} \mathrm{Tr}[\rho \mathbb{I}_V \otimes A_{\perp}^z \otimes B_{\perp}^z], \tag{3.8}$$

$$q_{\lightning} := \Pr[\mathrm{V}_{\mathrm{AB}} = \lightning] = \frac{1}{2} \sum_{a\neq b\in\{0,1,\perp\},z\in\{0,1\}} \mathrm{Tr}[\rho \mathbb{I} \otimes A_a^z \otimes B_b^z]. \tag{3.9}$$

In every round $i \in \{1,\ldots,r\}$ of the protocol (executed sequentially r times), the attackers will pick a strategy $\mathbf{S}_\eta^i$ that can depend on the previous rounds. A strategy $\mathbf{S}_\eta^i$ will induce a probability vector $\mathbf{q}^i = (q_{\mathrm{C}}^i, q_{\perp}^i, q_{\mathrm{W}}^i, q_{\lightning}^i)$. In an honest implementation,

$$\begin{aligned} &\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{C}] = \eta(1-p_{err}) =: p_{\mathrm{C}}, \qquad &&\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{W}] = \eta p_{err} =: p_{\mathrm{W}}, \\ &\Pr[\mathrm{V}_{\mathrm{AB}} = \perp] = 1-\eta =: p_{\perp}, &&\Pr[\mathrm{V}_{\mathrm{AB}} = \lightning] = 0 =: p_{\lightning}. \end{aligned} \tag{3.10}$$

This defines a probability vector $\mathbf{p}_{hp} = (p_{\mathrm{C}}, p_{\perp}, p_{\mathrm{W}}, p_{\lightning})$ that the honest prover would ideally reproduce. An attack is *successful* if the verifiers cannot distinguish if their data came from the distribution $\mathbf{p}_{hp}...\mathbf{p}_{hp}$ (r times) or from $\mathbf{q}^1...\mathbf{q}^r$. As mentioned above, in Section 3.2.2 we provide a test to distinguish between these two cases based on the received data.

3.2.1 Exact loss-tolerance of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$

A single round attack to $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$ for $\eta = 1$ can be identified with a so-called monogamy-of-entanglement (MoE) game, introduced by Tomamichel, Fehr, Kaniewski

and Wehner in [TFKW13], formalized below in Definition 3.2.4 and generalized by Johnston, Mittal, Russo, and Watrous [JMRW16]. The authors of [TFKW13] showed that the optimal probability that the attackers are correct in one round of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol is $\cos^2(\frac{\pi}{8})$. Moreover, they show strong parallel repetition, i.e. if $\mathrm{QPV}_{\mathrm{BB84}}$ is executed m times in parallel, the probability that the attackers are correct is at most $(\cos^2(\frac{\pi}{8}))^m$. Here we consider an *extension* of a MoE game, which we will call *lossy* MoE game, that will capture a round attack of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$—specifically step 4—and extensions of it, see Section 3.3.

3.2.4. Definition. *Let $\mathcal{Z}$ and $\mathcal{V}$ be finite non-empty alphabets. Let V_v^z be POVMs of the same finite dimension for all $(z,v) \in \mathcal{Z} \times \mathcal{V}$, and let $\mathcal{M} := \{V_v^z\}_{z,v}$. A* lossy *monogamy-of-entanglement game with parameter $\eta \in [0,1]$, played by a referee, with associated Hilbert space $\mathcal{H}_R$, and two collaborative parties Alice and Bob, denoted by*

$$\mathsf{G}_\eta := (\eta, \mathcal{M}), \tag{3.11}$$

is described as follows:

1. *Alice and Bob, with associated Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, prepare a quantum state $\rho_{RAB} \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_A \otimes \mathcal{H}_B)$.*

2. *They send register R to the referee, holding on registers A and B, respectively. The two parties are no longer allowed to communicate.*

3. *The referee chooses $z \in \mathcal{Z}$ uniformly at random and measures register R using $\{V_v^z\}_v$ to obtain the measurement outcome v. Then, he announces z to Alice and Bob.*

4. *The collaborative parties make a guess for v and they win the game if and only if both either guess v correctly or both answer $\perp$ (with probability $1-\eta$). In order to obtain the answers, Alice and Bob perform POVMs $\{A_a^z\}_{a\in\mathcal{V}\cup\{\perp\}}$ and $\{B_a^z\}_{a\in\mathcal{V}\cup\{\perp\}}$ on their local registers, respectively. The tuple $\mathbf{S}_\eta := \{\rho_{RAB}, A_v^z, B_v^z\}_{v\in\mathcal{V}\cup\{\perp\},z\in\mathcal{Z}}$ will be called a* strategy *for $\mathcal{G}_\eta$.*

The lossy constraint, i.e. answering $\perp$ with probability $1-\eta$, is given by

$$\frac{1}{|\mathcal{Z}|}\sum_{z\in\mathcal{Z}} \mathrm{Tr}[\rho_{RAB}\mathbb{I}_V \otimes A_\perp^z \otimes B_\perp^z] = 1-\eta. \tag{3.12}$$

See Figure 3.2 for a schematic representation of a lossy MoE game. A monogamy-of-entanglement game G as introduced in [TFKW13] is recovered by setting $\eta = 1$, i.e. $\mathsf{G} = \mathsf{G}_{\eta=1}$. The winning probability of a lossy MoE game G_η, given a strategy $\mathbf{S}_\eta = \{\rho_{RAB}, A_v^z, B_v^z\}_{v\in\mathcal{V}\cup\{\perp\},z\in\mathcal{Z}}$, is given by

$$\omega(\mathsf{G}_\eta, \mathbf{S}_\eta) = \frac{1}{|\mathcal{Z}|}\sum_{v,z} \mathrm{Tr}[\rho_{RAB} V_v^z \otimes A_v^z \otimes B_v^z]. \tag{3.13}$$

The optimal winning probability is given by the supremum of (3.13) over all possible strategies, i.e.

$$\omega(\mathsf{G}_\eta) := \sup_{\mathbf{S}_\eta} \omega(\mathsf{G}_\eta, \mathbf{S}_\eta). \tag{3.14}$$

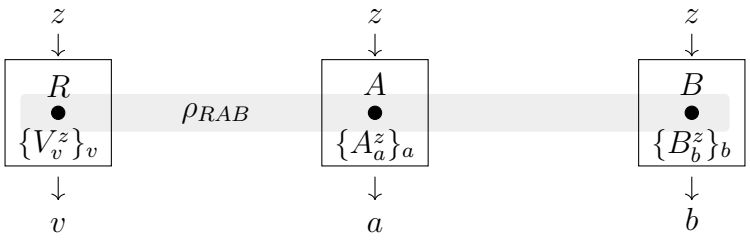


Figure 3.2: Schematic representation of a lossy monogamy-of-entanglement game. The gray-shaded region represents the tripartite quantum state ρ_{RAB} prepared by Alice and Bob and shared amongst the three parties. The referee, Alice and Bob are denoted by R, A and B, respectively.

3.2.5. Remark. *(The guessing strategy).* Consider a lossy monogamy-of-entanglement game where $\{V_v^z\}_{v,z}$ are projective measurements. Then, Alice and Bob can make a guess $\tilde{z}$ for z that will be correct with probability $\frac{1}{|\mathcal{Z}|}$. They can pick a fixed answer $a \neq \perp$ and send a state $|\psi\rangle \in \mathcal{H}_R$ that lives in the subspace that $V_a^{\tilde{z}}$ projects onto, i.e. $V_a^{\tilde{z}}|\psi\rangle = |\psi\rangle$. Then, if they receive $z = \tilde{z}$, they answer a and otherwise, they answer $\perp$. This strategy based on guessing z is such that Alice and Bob are going to be correct with probability $\frac{1}{|\mathcal{Z}|}$ and will answer $\perp$ with probability $1 - \frac{1}{|\mathcal{Z}|}$; they will never give a wrong answer.

As shown in [TFKW13], any strategy can be purified in the sense that, by enlarging the Hilbert spaces if necessary, one may assume $\rho_{RAB} = |\psi\rangle\langle\psi|_{RAB}$ for some pure state $|\psi\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A \otimes \mathcal{H}_B$, and that the local measurements $\{A_a^z\}_a$ and $\{B_b^z\}_b$ are projective for all $z \in \mathcal{Z}$. From now on, we will assume our strategies are of this purified form.

Next, we describe the G^{BB84} game, originally introduced in [TFKW13], which was used by the authors to show security of $\mathrm{QPV}_{\mathrm{BB84}}$ in the No-PE model. We will later use its lossy version to show security of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$.

3.2.6. Example. The *BB84 monogamy-of-entanglement game* is described as follows. Alice and Bob prepare a quantum state and send a qubit from it to the referee, who chooses uniformly at random to measure the qubit either in the computational or the Hadamard basis. Upon knowing the choice of basis, the task of Alice and Bob is to guess the measurement outcome. Using the above terminology, the game is given by

$$\mathsf{G}^{BB84} = (\eta = 1, \mathcal{M}), \tag{3.15}$$

where $\mathcal{M} = \{V_0^z, V_1^z\}_{z\in\{0,1\}}$, with $V_0^z = H^z|0\rangle\langle 0|H^z$ and $V_1^z = H^z|1\rangle\langle 1|H^z$, where H is the Hadamard transformation. Varying $\eta \in [0,1]$ defines the lossy BB84 MoE game, denoted by G_{η}^{BB84}.

The G^{BB84} game can be associated with an attack to the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol in the sense that having a strategy to break the protocol in the No-PE model implies having a strategy for the MoE game [TFKW13, Section 5], and therefore

$$\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{C}] \leq \omega(\mathsf{G}^{BB88}). \tag{3.16}$$

In a similar manner, it follows that having a strategy $\mathbf{S}_{\eta}^{BB84}$ for G_{η}^{BB84} implies having a No-PE strategy for $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$. The idea is that in step 4 in the attack described above, the attackers start with a tripartite state shared among the verifier, Alice and Bob and their task is to correctly guess the measurement outcome of the measurement which is performed on the verifier's register. In the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol case, verifier V_0 plays the role of the referee with associated Hilbert space $\mathcal{H}_V = \mathbb{C}^2$, with $\mathcal{Z} = \{0,1\}$ and $\mathcal{V} = \{0,1\}$. In the purified version of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, V_0 performs the measurement $\mathcal{M} = \{V_0^z = H^z|0\rangle\langle 0|H^z, V_1^z = H^z|1\rangle\langle 1|H^z\}_{z\in\{0,1\}}$, and the two collaborative parties, who correspond to the attackers, want to break the protocol by guessing the verifier's outcome. We refer the reader to step 4 of the attack on $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, illustrated in Figure 3.1 and note that it corresponds to a lossy MoE game[1], depicted in Figure 3.2.

The strategy $\mathbf{S}_{\mathrm{TFKW}} = \{|\psi\rangle\langle\psi|, A_a^z = \delta_{a0}, B_a^z = \delta_{a0}\}$, where $|\psi\rangle_V = \cos\frac{\pi}{8}|0\rangle_V + \sin\frac{\pi}{8}|1\rangle_V$, gives the optimal probability of winning the G^{BB84} game [TFKW13] (see discussion below) and thus the optimal probability of being correct attacking the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol is upper bounded by

$$\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{C}] = \frac{1}{2}\sum_{a,z}\mathrm{Tr}[|\psi\rangle\langle\psi|V_a^z \otimes A_a^z \otimes B_a^z] = \cos^2\frac{\pi}{8}. \tag{3.17}$$

This strategy also gives $\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{W}] = \sin^2\frac{\pi}{8}$ and $\Pr[\mathrm{V}_{\mathrm{AB}} = \lightning] = 0$. Comparing these probabilities with (3.10), and considering that $\eta = 1$, the attackers could successfully attack one round of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol if $p_{err} \geq \sin^2\frac{\pi}{8} \simeq 0.15$. In terms of an attack to $\mathrm{QPV}_{\mathrm{BB84}}$, the strategy $\mathbf{S}_{\mathrm{TFKW}}$ comes from the attack described as follows (see Figure 1.3): Alice intercepts the state sent by V_0 and measures it in the *Breidbart* basis $\{\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle\}$—associated with 0 and 1, respectively—i.e. a projective measurement onto the state that has maximum overlap with $|0\rangle$ and $|+\rangle$. Then, Alice broadcasts the outcome a, and both attackers answer a to their respective closest verifier.

Notice that if in a attack the attackers actually answer, meaning that they do not respond '$\perp$', we have

$$\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{C} \mid \mathrm{V}_{\mathrm{AB}} \neq \perp] + \Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{W} \mid \mathrm{V}_{\mathrm{AB}} \neq \perp] + \Pr[\mathrm{V}_{\mathrm{AB}} = \lightning \mid \mathrm{V}_{\mathrm{AB}} \neq \perp] = 1. \tag{3.18}$$

[1]Although not represented in the figure, V_0 performs the measurement $\{V_v^z\}_v$ in his local register V of the state ρ_{VAB}.

In fact, since for QPV we impose $\Pr[\mathrm{V_{AB}} = \lightning] = 0$, the above expression reduces to

$$\Pr[\mathrm{V_{AB}} = \mathrm{C} \mid \mathrm{V_{AB}} \neq \perp] + \Pr[\mathrm{V_{AB}} = \mathrm{W} \mid \mathrm{V_{AB}} \neq \perp] = 1. \tag{3.19}$$

We define the probability of winning, p_{win} as the maximum probability of being correct conditioned on answering, i.e. $p_{win} \coloneqq \max \Pr[\mathrm{V_{AB}} = \mathrm{C} \mid \mathrm{V_{AB}} \neq \perp]$, which has the interpretation of the normalized (over the conclusive answers) optimal probability of answering 'CORRECT'. Showing that p_{win} has a constant gap below one would imply that, over the conclusive rounds, the attackers cannot be correct as many times as they want, and if p_{win} is below the expected value of an honest prover, i.e. $\eta(1 - p_{err})$, the attackers will not be able to mimic her behavior. On the other hand, for our security approach, we will consider the probability that the attackers can actually play (answer)—not answering '$\perp$'—in the G_{η}^{BB84} game, i.e. given a strategy $\mathbf{S}_{\eta} = \{|\psi\rangle, A_a^z, B_b^z\}_{z,a,b}$, the probability that they answer, p_{ans},

$$p_{ans} \coloneqq \Pr[\mathrm{V_{AB}} = \mathrm{C}] + \Pr[\mathrm{V_{AB}} = \mathrm{W}] = \frac{1}{2} \sum_{a,z \in \{0,1\}} \langle \psi | A_a^z B_a^z | \psi \rangle, \tag{3.20}$$

where we used the following simplified notation: when clear from the context, tensor products, identities and ψ will be omitted, e.g. $\langle \psi | V_0^z \otimes A_1^x \otimes B_1^z | \psi \rangle = \langle V_0^z A_1^z B_1^z \rangle$. Moreover, if attackers want to mimic an honest prover, they have to be consistent with the error p_{err}, that is,

$$\frac{\langle V_0^z A_1^z B_1^z \rangle}{\langle V_0^z (A_0^z + A_1^z)(B_0^z + B_1^z) \rangle} \leq p_{err}, \qquad \frac{\langle V_1^z A_0^z B_0^z \rangle}{\langle V_1^z (A_0^z + A_1^z)(B_0^z + B_1^z) \rangle} \leq p_{err}, \tag{3.21}$$

where we impose that the error rate for both outputs 0 and 1 is upper bounded by the same amount for all inputs z.

Notice that if $p_{ans} = 1$ while satisfying (3.21), the attackers can always attack the protocol without being caught. Using (3.20), the security of the protocol can be regarded as the maximum probability that the attackers can respond without being caught, and the protocol will be proven to be secure if the attackers cannot reproduce $p_{ans} \geq \eta$ for a given p_{err}, we formalize this idea in the following definition.

3.2.7. DEFINITION. *We define the security region SR of the* $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$ *protocol as the set of pairs* $(p_{err}, p_{ans}) \in [0,1] \times [0,1]$ *for which no strategy* $\mathbf{S}_{\eta}^{BB84}$ *(and thus no successful No-PE strategy) exists that breaks the* $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$ *protocol with the corresponding error and response rate. A subset of SR will be denoted by SSR. We define the attackable region AR as the complementary set of the SR. A subset of AR will be denoted as SAR.*

Therefore, our interest relies on maximizing expression (3.20) over all the strategies $\mathbf{S}_{\eta}^{BB84}$ fulfilling (3.21) to break the $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$ protocol. However, unlike the set of probabilities achievable by classical physics, the set of probabilities

attainable by quantum mechanics, $\mathcal{Q}$, has uncountably many extremal points, see e.g. [BCP+14], and therefore it makes the optimization problem a tough task. On the positive side, in [NPA08], Navascués, Pironio and Acín (NPA) introduced a recursive way to construct subsets $\mathcal{Q}_\ell \supset \mathcal{Q}_{\ell+1} \supset \mathcal{Q}$ for all $\ell \in \mathbb{N}$ with the property that each of them can be tested using SDP and are such that $\cap_{\ell\in\mathbb{N}}\mathcal{Q}_\ell = \mathcal{Q}_{co}$, where $\mathcal{Q}_{co} \supset \mathcal{Q}$ is the set of probabilities obtained by Alice and Bob performing commuting measurements on a joint Hilbert space instead of tensor product measurements. For finite-dimensional Hilbert spaces, both sets are equivalent.

For all $a, b \in \{0, 1, \perp\}$ and all $z, z' \in \{0, 1\}$, the elements $\langle A_a^z B_b^{z'}\rangle$ will appear in the maximization problem solvable via SDP, and they are bounded by linear constraints given by $\mathcal{Q}_\ell$, see Section 2.4. In addition to these constraints, we impose the additional linear constraints which we derive from $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, i.e. since in the protocol the verifiers abort if they receive different messages, from (3.9),

$$\langle A_a^z B_b^z\rangle = 0 \quad \forall a \neq b \in \{0, 1, \perp\}, \forall z \in \{0, 1\}, \tag{3.22}$$

and the prover subject to a measurement error p_{err}, see Proposition 3.2.8.

3.2.8. Proposition. *Let* $a, b \in \{0, 1\}$. *For all* $z, z' \in \{0, 1\}$, *the terms* $\langle A_a^z B_b^{z'}\rangle$ *can be bounded by* p_{err} *by the following inequality:*

$$\sum_{ab}(2 - \|V_a^z + V_b^{z'}\|)\langle A_a^z B_b^{z'}\rangle \leq p_{err}\sum_a(\langle A_a^z B_a^z\rangle + \langle A_a^{z'} B_a^{z'}\rangle). \tag{3.23}$$

The proof of Proposition 3.2.8 is a particular case of the proof of Proposition 3.3.2. The value of p_{ans} in (3.20) can be therefore upper bounded by the SDP problem:

$$\boxed{\begin{array}{l}\max \dfrac{1}{2}\displaystyle\sum_{z,a\in\{0,1\}}\langle A_a^z B_a^z\rangle; \\ \text{subject to: the linear constraints for } \mathbf{S}_\eta^{BB84} \in \mathcal{Q}_\ell, \\ \qquad\qquad \text{and equations (3.22) and (3.23).}\end{array}} \tag{3.24}$$

Where, abusing notation, we denoted $\mathbf{S}_\eta^{BB84} \in \mathcal{Q}_\ell$ meaning that the probabilities obtained from $\mathbf{S}_\eta^{BB84}$ belong to the set $\mathcal{Q}_\ell$. Figure 3.3 shows the solution of the SDP (3.24) for different values of p_{err} for the first and second level of the NPA hierarchy using the Ncpol2sdpa package [Wit15] in Python. The values above the solution for any given p_{err} represent points there does not exist an attack such that $p_{ans} \geq \eta$ and therefore correspond to SSR, the area represented in light blue in Figure 3.3. The results plotted in Figure 3.3 coincide with the tight bound of the winning probability of the MoE game attacking the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, since p_{ans} reaches 1 for $p_{err} = 0.1464 \simeq \sin^2(\pi/8)$.

3.2.9. Proposition. *The function* $p_{ans}(p_{err})$ *for* $p_{err} \in [0, 1]$ *obtained by the solution of* (3.24) *is monotonically increasing, i.e. if* $p_{err}^0 \leq p_{err}^1$, *then* $p_{ans}(p_{err}^0) \leq p_{ans}(p_{err}^1)$.

Proof:
Proposition 3.2.9 follows from the fact that $p_{ans}(p^1_{err})$ is obtained by an SDP which is a relaxation of the restrictions of the SDP providing $p_{ans}(p^0_{err})$. □

Informally, Proposition 3.2.9 assures that between two numerical solutions for different p_{err} there are no 'abrupt jumps', more specifically, in Figure 3.3, any solution between two plotted points cannot be greater than the point on the right.

Consider the strategy $\mathbf{S}^{BB84}_{mix}|_p$ given by the probabilistic mixture of playing the strategy $\mathbf{S}_{\text{TFKW}}$ with probability p and $\mathbf{S}_{guess} = \{|0\rangle\langle 0|, A^0_a = \delta_{a0}, A^1_a = \delta_{a\perp}, B^0_a = \delta_{a0}, B^1_a = \delta_{a\perp}\}$ with probability $1-p$, conditioned on answering. As long as $p_{ans} < 1$, for each p, this mixture gives a unique pair of (p_{err}, p_{ans}) (for $p_{ans} = 1$, take the minimum p_{err}), and we equivalently denote $\mathbf{S}^{BB84}_{mix}|_p$ by the corresponding (p_{err}, p_{ans}) as $\mathbf{S}^{BB84}_{mix}|_{(p_{err},p_{ans})}$. The values of p_{ans} obtained by this strategy, see continuous line in Figure 3.3, provide a region where the protocol is attackable, i.e. a SAR.

Since the SSR obtained from the second level of the NPA hierarchy and the SAR obtained from $\mathcal{S}^{BB84}_{mix}|_p$ are such that $SSR \cup SAR = [0,1] \times [0,1]$, up to infinitesimal precision, it means that they correspond to SR and AR, respectively, i.e. the solutions of the SDP (3.24) for $\ell = 2$ converge to the quantum value and are tight. This means that Figure 3.3 represents a full characterization of the security of the $\text{QPV}^{\eta}_{\text{BB84}}$ protocol under photon loss with attackers that do not pre-share entanglement, and the light blue region encodes all the points (p_{err}, η) where the protocol is secure. The result is summarized as follows:

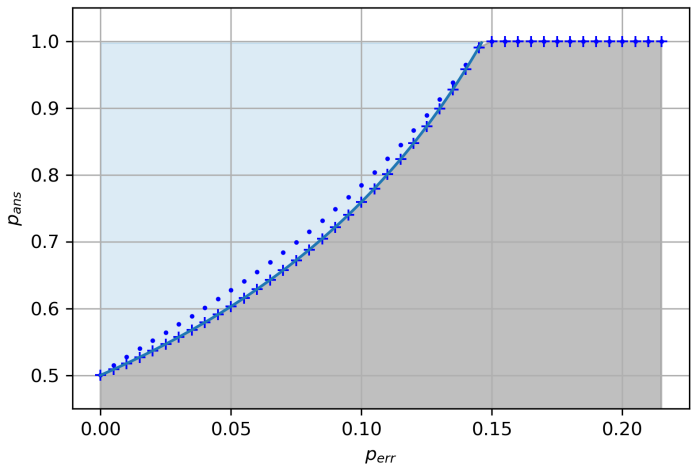


Figure 3.3: Solutions of the first, $\ell = 1$, (blue dots) and second level, $\ell = 2$, (blue pluses) of the NPA hierarchy for the SDP (3.24). The light blue and the gray area correspond to SR and AR, respectively. The continuous line represents $\mathbf{S}^{BB84}_{mix}|_p$.

3.2.10. RESULT. *In the No-PE model, if attackers answer with probability* η *and never respond inconsistent answers, the optimal probability that they answer '*CORRECT*' in a round of* $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ *for* $\eta \in [\frac{1}{2}, 1]$ *is given by*

$$\max \Pr\{\mathrm{V}_{\mathrm{AB}} = \mathrm{C}\} = \cos^2\left(\frac{\pi}{8}\right)\eta + \sin^2\left(\frac{\pi}{8}\right)(1-\eta). \tag{3.25}$$

3.2.2 Sequential repetition of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

Recall that in every round of the protocol, attackers will pick a strategy $\mathbf{S}^i_\eta$ that can depend on the previous rounds. Assume that the verifiers did not receive any 'ABORT' answers, otherwise, they reject the location. Let Γ^{att}_r denote the total score that the attackers (att) get, defined in (3.2). In the next theorem, we show that attackers in the No-PE model will fail the test $\mathsf{T}^{r\mathrm{BB84}}_{\varepsilon_{\mathrm{h}}}$ with exponentially high probability.

3.2.11. THEOREM. *Consider the* r *sequential repetition of* $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$. *Let* $\varepsilon_h > 0$, η *and* p_{err} *be such that* $\alpha - \delta > 0$, *with* $\delta = (\cos^4\frac{\pi}{8}\ln(1/\varepsilon_h)/r)^{1/2}$. *Then, any sequential strategy to attack* $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ *in the No-PE model fulfills that* $\mathbb{E}[\Gamma^{att}_r] \leq 0$. *Moreover, the probability that the attackers are accepted in the* $\mathsf{T}^{r\mathrm{BB84}}_{\varepsilon_h}$ *test is exponentially small:*

$$\Pr[\Gamma^{att}_r \geq r(\alpha - \delta)] \leq e^{-r(\alpha-\delta)^2/2}. \tag{3.26}$$

Theorem 3.2.11 shows that there exists a test which is both complete and sound, and thus, the $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ is secure for the corresponding η and p_{err}. The existence of this test implies that after r rounds, attackers will be *caught* with exponentially high probability.

The points (η, p_{err}) such that $\alpha > 0$ correspond to the blue region in Figure 3.3 and also below the black dots in Figure 3.4—the above $\alpha - \delta$ corresponds to a shift that can be made small by increasing the number of sequential repetitions. The proof of Theorem 3.2.11 is a particular case of the proof of Theorem 4.2.13.

3.3 The $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ protocol

In Section 3.2.1, we showed security of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ in the No-PE model. Nevertheless, the protocol was shown to be secure only for transmission rate $\eta > \frac{1}{2}$, which is still very hard for current technology to achieve. For this reason, we propose a family of protocols that generalize $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ by encoding the bit v in more bases, rather than just the computational or Hadamard basis. We will see that similar techniques as in Section 3.2.1 can be used to prove security for this family of protocols. In this section, we generalize the results of Section 3.2.1, showing security in the No-PE model and reaching arbitrary constant photon loss tolerance.

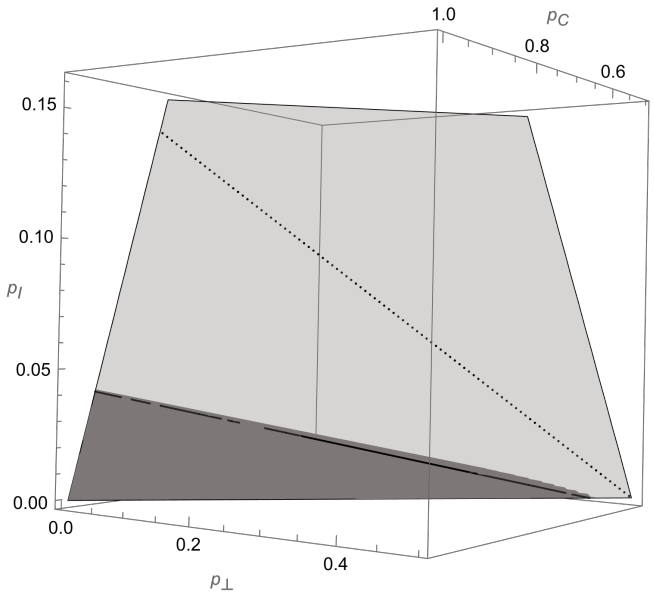


Figure 3.4: Probability simplex Δ_2 for probabilities $(p_{\mathrm{C}}, p_{\perp}, p_{\mathrm{I}})$ taking respective values on $\mathfrak{X} = \{\mathrm{C}, \perp, \mathrm{I}\}$, where I (incorrect) denotes either W or $\lightning$. Black dots correspond to numerical solutions of (3.24) for $\ell = 2$. The dark region is the set of probabilities that Theorem 4.2.11 excludes, and the black straight line is the intersection between Δ_2 and the plane $\gamma_{\mathrm{C}} p_{\mathrm{C}} - \gamma_{\perp} p_{\perp} - \gamma_{\mathrm{I}} p_{\mathrm{I}} = 0$.

Independently and around the same time, Buhrman, Schaffner, Speelman, Zbinden [Spe16b, Chapter 5] and Qi and Siopsis [QS15] introduced extensions of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol. Both are based on allowing the verifiers to choose among more than two different qubit bases, which for the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol corresponded to the computational and the Hadamard basis. The protocol in [Spe16b] allows V_0 choosing among k bases, for an arbitrary $k \geq 2$, different orthonormal bases in the meridian $\varphi = 0$ of the Bloch sphere depending on the angle $\theta \in [0, \pi)$, where these are uniformly distributed, i.e. $\theta \in \{\frac{0}{k}\pi, ..., \frac{k-1}{k}\pi\}$, and the bases are $\{|0_\theta\rangle, |1_\theta\rangle\}$, where

$$|0_\theta\rangle := \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \qquad |1_\theta\rangle := \sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle. \tag{3.27}$$

Recall that the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol is recovered taking $k = 2$, where $\theta = 0$ and $\theta = \frac{\pi}{2}$ correspond to the computational and Hadamard basis, respectively. On the other hand, the extension in [QS15] allows the verifiers to choose among k encoding bases over the whole Bloch sphere, however such an extension only works for k large enough and not all large integers are allowed.

Here we present a similar extension allowing to choose k random bases over the Bloch sphere for all $k \geq 2$, which works regardless whether k is large or small, and we prove that this translates to better security in case terms of the loss-tolerance of the quantum information in an experimental implementation. We

add the φ parameter corresponding to the azimuth angle to the states in (3.27) as a phase $e^{i\varphi}$ in front of $|1\rangle$, in a similar way as in [QS15]. We do however use a slightly different procedure than [QS15] to compute the precise angles, to make the basis choice more uniform (see below).

3.3.1 Discrete uniform choice of basis over the Bloch sphere

In order to avoid accumulation of points in the sphere around the poles due to the unit sphere area element $d\Omega = \sin\theta d\theta d\varphi$, a continuous uniform distribution of points can be made by taking [Wei]

$$\theta = \cos^{-1}(2u-1), \qquad \varphi = 2\pi v, \tag{3.28}$$

where u and v are uniformly distributed over the interval $(0,1)$. Notice that allowing $\varphi \in [0, 2\pi)$ would imply having duplicate bases (i.e. the same basis vectors in different order), thus, φ will be restricted to take values in the range $[0,\pi)$. Moreover, in the discrete case we are interested also in the north pole of the sphere ($\theta = 0$), corresponding to the computational basis, and therefore in order to include it, discretizing the sphere with k_θ different θ and with k_φ different φ, the 0 must be included in the range of u, i.e. $u \in \{\frac{0}{k_\theta}, ..., \frac{k_\theta-1}{k_\theta}\}$. Similarly, in order to have the Hadamard basis (and the bases in between them in the meridian $\varphi = 0$), $v \in \{\frac{0}{k_\varphi}, \ldots, \frac{k_\varphi-1}{k_\varphi}\}$. Let $\tilde{u} := k_\theta u$ and $\tilde{v} := k_\varphi v$, which determine the $k_\theta k_\varphi$ points of the discretization. Let $z := \tilde{u}\tilde{v} \equiv k_\varphi \tilde{u} + \tilde{v}$, therefore, given $z \in [k_\theta k_\varphi]$, one can recover $\tilde{u} = \lfloor x/k_\varphi \rfloor$ and $\tilde{v} = x \bmod k_\varphi$, where $\lfloor * \rfloor$ stands for the floor function. Notice that this discrete parametrization has k_φ degenerate points for $\tilde{u} = k_\theta - 1$, corresponding to $(\theta = 0, \varphi)$, which can be easily removed by z taking values in the range $\{0, ..., m-1\}$, where $k := k_\varphi(k_\theta - 1) + 1$. Therefore, we can discretize the bases in the Bloch sphere depending on z so that $\forall z \in [k]$,

$$\theta(z) = \arccos\left(\frac{2}{k_\theta}(\lfloor z/k_\varphi \rfloor + 1) - 1\right), \qquad \varphi(z) = \pi\frac{z \bmod k_\varphi}{k_\varphi}. \tag{3.29}$$

Then the protocol is extended allowing the verifiers to choose among the bases $\{|0_z\rangle, |1_z\rangle\}$ for $z \in [k]$, where

$$|0_z\rangle = \cos\frac{\theta(z)}{2}|0\rangle + e^{i\varphi(z)}\sin\frac{\theta(z)}{2}|1\rangle, \ |1_z\rangle = \sin\frac{\theta(z)}{2}|0\rangle - e^{i\varphi(z)}\cos\frac{\theta(z)}{2}|1\rangle. \tag{3.30}$$

Note that for any k, we can discretize the bases in as many ways as divisors $k-1$ has in the following way: one chooses the number of θ and φ as $(k_\theta, k_\varphi) = (d_k + 1, \frac{k-1}{d_k})$, for each d_k divisor of $k-1$. As examples, the choice $(k, k_\theta, k_\varphi) = (2, 2, 1)$ corresponds to the computational and Hadamard bases, and the choice $(k, k_\theta, k_\varphi) = (3, 2, 2)$ to the computational, Hadamard bases and the basis formed by the eigenvectors of the Pauli Y matrix.

Based on Section 3.3.1, we introduce an extension of the $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ protocol, which we denote by $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$, where $k_{\theta\varphi}$ is the sort notation of (k, k_θ, k_φ).

3.3.1. Definition. *Let η denote the transmission rate of the qubits sent from V_0 to P, and let $k_{\theta\varphi}$ be as described above. We define one round of the $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ protocol as follows:*

1. *V_0 and V_1 secretly agree on $v \in \{0,1\}$ and $z \in [k]$. Then, V_0 prepares the qubit state $|v_z\rangle$ as in (3.30).*
2. *V_0 sends the qubit $|v_z\rangle$ to P, and V_1 sends z to P coordinating their times so that they arrive at pos at the same time.*
3. *Immediately, P measures the received qubit in the basis $\{|0_z\rangle, |1_z\rangle\}$ and broadcasts her outcome to V_0 and V_1. If, due to experimental losses, the qubit did not arrive at pos, P broadcasts 'No photon' with the symbol $\perp$. Denote the response by v_{P}.*
4. *If*
   (a) *V_0 and V_1 receive their respective answers at the time corresponding with pos, and they are equal, i.e. both receive the same v_{P}, then, if*
      - *$v_{\mathsf{P}} = v$, the verifiers record 'Correct', denoted by 'c',*
      - *$v_{\mathsf{P}} = 1 - v$, the verifiers record 'Wrong', denoted by 'w',*
      - *$v_{\mathsf{P}} = \perp$, the verifiers record 'No photon', denoted by '$\perp$',*

   (b) *otherwise, they record 'Abort', denoted by '↯', and abort the protocol rejecting the location.*

Notice that $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ is recovered for $k = 2$, with the unique choice of $k_\theta = 2$ and $k_\varphi = 1$. In order to *accept* or *reject* the location, the verifiers run $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ sequentially r times. The verifiers *accept* the prover's location if the answers they receive match with η and p_{err}, which is the same condition as for $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, see (3.1). Analogous to $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, for each choice of $k_{\theta\varphi}$, from the analysis of the correlations shown below in Section 3.3, one can construct a decision test to make the binary decision to either *accept* or *reject*, see proof of Theorem 3.2.11 for how to construct it.

3.3.2 Security of the $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ and improved loss-tolerance

Analogous to the analysis of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ in Section 3.2.1, for the security analysis, we will consider the purified version of $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$, where, in Definition 3.3.1, in step 1, V_0 instead of preparing the qubit $|0_z\rangle$, prepares the EPR pair $|\Phi^+\rangle$, sends one qubit register to P, and keeps the other register. In a later moment, V_0 measures

his local register in the basis $\{|0_z\rangle, |1_z\rangle\}$. An attack on the $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ protocol can be associated with a monogamy-of-entanglement game in the following way: fix $k_{\theta\varphi}$, and let V be the register of the qubit of V_0, with associated Hilbert space $\mathcal{H}_V = \mathbb{C}^2$, with $\mathcal{Z} = [k]$ and $\mathcal{V} = \{0,1\}$. Verifier V_0 performs the collection of measurements,

$$\mathcal{M}^{k_{\theta\varphi}} = \{V_0^z, V_1^z\}_{z\in\{0,\dots,k-1\}}, \tag{3.31}$$

where $V_0^z = |0_z\rangle\langle 0_z|$ and $V_1^z = |1_z\rangle\langle 1_z|$, with implicit dependence on $k_{\theta\varphi}$ (see (3.29) and (3.30)). The two collaborating parties in the MoE game correspond to the attackers who aim to break the protocol with their guess. Then, the attackers Alice and Bob, with associated Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, have to win against the verifiers both giving the same outcome to them or declaring photon loss. Thus, having a strategy to attack the protocol implies having a strategy for the lossy MoE game specified by the choice of $k_{\theta\varphi}$:

$$\mathsf{G}_{\eta}^{k_{\theta\varphi}} = (\eta, \mathcal{M}^{k_{\theta\varphi}}). \tag{3.32}$$

A strategy for $\mathsf{G}_{\eta}^{k_{\theta\varphi}}$ is given by $\mathbf{S}_{\eta}^{k_{\theta\varphi}} = \{|\psi\rangle, A_a^z, B_a^z\}_{a\in\{0,1\}\cup\{\perp\}, z\in[k]}$.

In [TFKW13] the following upper bound to win a generic MoE game $\mathsf{G} = (\{V_v^z\}_{z,v})$ is given:

$$\omega(\mathsf{G}) \leq \frac{1}{|\mathcal{Z}|} + \frac{|\mathcal{Z}|-1}{|\mathcal{Z}|}\sqrt{\max_{z\neq z'\in\mathcal{Z}}\max_{v,v'\in\mathcal{V}} \|\sqrt{V_v^z}\sqrt{V_{v'}^{z'}}\|^2}. \tag{3.33}$$

The security analysis of the $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ protocol will be based, in the same way as the $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ protocol, on maximizing the probability that the attackers 'play' without being caught:

$$p_{ans} = \frac{1}{k}\sum_{z\in[k], a\in\{0,1\}} \langle\psi|A_a^z B_a^z|\psi\rangle. \tag{3.34}$$

As in the $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ protocol, the constraints will be the linear constraints implied by $\mathbf{S}_{\eta}^{k_{\theta\varphi}} \in \mathcal{Q}_{\ell}$, the analogous to (3.22), i.e.

$$\langle A_a^z B_b^z\rangle = 0 \quad \forall a \neq b \in \{0,1,\perp\}, \forall z \in [k], \tag{3.35}$$

and the inequalities given in Proposition 3.3.2 bounded by p_{err}.

3.3.2. Proposition. *Let* $a, b \in \{0,1\}$, $\alpha_i^a = \langle i_{x'}|a_x\rangle$ *and* $\beta_i^b = \langle i_x|b_{x'}\rangle$ *for* $i \in \{0,1\}$. *The terms* $\langle A_a^z B_b^{z'}\rangle$ *can be bounded by* p_{err} *by the two inequalities below:*

$$\sum_{ab}(2 - \|V_a^z + V_b^{z'}\|)\langle A_a^z B_b^{z'}\rangle \leq p_{err}\sum_a(\langle A_a^z B_a^z\rangle + \langle A_a^{z'} B_a^{z'}\rangle), \tag{3.36}$$

and

$$\sum_{a,b}\Big(4 - \|(1+|\beta_a^b|^2)V_a^z + (1+|\alpha_b^a|^2)V_b^{z'} + \beta_0^b\beta_1^{b*}|0_z\rangle\langle 1_z| + \beta_0^{b*}\beta_1^b|1_z\rangle\langle 0_z| + \alpha_0^a\alpha_1^{a*}|0_{z'}\rangle\langle 1_{z'}|$$
$$+ \alpha_0^{a*}\alpha_1^a|1_{z'}\rangle\langle 0_{z'}|\|\Big)\langle A_a^z B_b^{z'}\rangle \leq p_{err}\Big((2+\max_{i,j}|\beta_i^j|^2)\sum_a\langle A_a^z B_a^z\rangle + (2+\max_{i,j}|\alpha_i^j|^2)\sum_a\langle A_a^{z'} B_a^{z'}\rangle\Big). \tag{3.37}$$

The proof of Proposition 3.3.2 relies on combining both expressions in (3.21), using $A_0^z + A_1^z \preceq \mathbb{I}$ and $B_0^{z'} + B_1^{z'} \preceq \mathbb{I}$ and bounding terms by the norm of the sums of the projectors V_a^z.

Proof:

Combining both expressions in (3.21), using the properties of the projectors and equation (3.35), we obtain the inequality

$$\langle V_1^z A_0^z B_0^z\rangle + \langle V_0^z A_1^z B_1^z\rangle \leq p_{err}(\langle A_0^z B_0^z\rangle + \langle A_1^z B_1^z\rangle). \tag{3.38}$$

Because of (3.35), from (3.38) we get

$$\langle V_1^z A_0^z\rangle + \langle V_0^z A_1^z\rangle \leq p_{err}(\langle A_0^z B_0^z\rangle + \langle A_1^z B_1^z\rangle), \tag{3.39}$$

$$\langle V_1^z B_0^z\rangle + \langle V_0^z B_1^z\rangle \leq p_{err}(\langle A_0^z B_0^z\rangle + \langle A_1^z B_1^z\rangle), \tag{3.40}$$

$$\langle V_1^z A_0^z\rangle + \langle V_0^z B_1^z\rangle \leq p_{err}(\langle A_0^z B_0^z\rangle + \langle A_1^z B_1^z\rangle), \tag{3.41}$$

$$\langle V_1^z B_0^z\rangle + \langle V_0^z A_1^z\rangle \leq p_{err}(\langle A_0^z B_0^z\rangle + \langle A_1^z B_1^z\rangle). \tag{3.42}$$

We will use the above inequalities to find linear constraints on the entries of the Gram matrix G corresponding to $\langle A_a^z B_b^{z'}\rangle$. Consider

$$\begin{aligned} 2\langle A_a^z B_b^{z'}\rangle &= 2\langle \mathbb{I}\otimes A_a^z \otimes B_b^{z'}\rangle = \langle (V_a^z + V_{1-a}^z) A_a^z B_b^{z'}\rangle + \langle (V_b^{z'} + V_{1-b}^{z'}) A_a^z B_b^{z'}\rangle \\ &= \langle (V_a^z + V_b^{z'}) A_a^z B_b^{z'}\rangle + \langle V_{1-a}^z A_a^z B_b^{z'}\rangle + \langle V_{1-b}^{z'} A_a^z B_b^{z'}\rangle, \end{aligned} \tag{3.43}$$

then, summing over a and b, we get

$$\begin{aligned} 2\sum_{ab}\langle A_a^z B_b^{z'}\rangle &= \sum_{ab}\langle ((V_a^z + V_b^{z'})) A_a^z B_b^{z'}\rangle + \langle V_1^z A_0^z (B_0^{z'} + B_1^{z'})\rangle + \langle V_0^z A_1^z (B_0^{z'} + B_1^{z'})\rangle + \\ &\quad \langle V_1^{z'} (A_0^z + A_1^z) B_0^{z'}\rangle + \langle V_0^{z'} (A_0^z + A_1^z) B_1^{z'}\rangle \\ &\leq \sum_{ab}\langle ((V_a^z + V_b^{z'})) A_a^z B_b^{z'}\rangle + \langle V_1^z A_0^z\rangle + \langle V_0^z A_1^z\rangle + \langle V_1^{z'} B_0^{z'}\rangle + \langle V_0^{z'} B_1^{z'}\rangle, \end{aligned} \tag{3.44}$$

where we used that $A_0^z + A_1^z \preceq \mathbb{I}$ and $B_0^{z'} + B_1^{z'} \preceq \mathbb{I}$. Then, using (3.39) and (3.40), we recover (3.36).

On the other hand, recall that $V_a^z = |a_z\rangle\langle a_z|$ and $V_b^{z'} = |b_{z'}\rangle\langle b_{z'}|$, and we can write

$$|a_z\rangle = \alpha_0^a |0_{z'}\rangle + \alpha_1^a |1_{z'}\rangle, \qquad |b_{z'}\rangle = \beta_0^b |0_z\rangle + \beta_1^b |1_z\rangle, \tag{3.45}$$

where $\alpha_i^a = \langle i_{z'}|a_z\rangle$ and $\beta_j^b = \langle j_z|b_{z'}\rangle$, where the dependence on z and z' is omitted for simplicity. We write the projectors V_a^z and $V_b^{z'}$ in the other basis in such a way that

$$\begin{aligned} V_a^z &= |\alpha_0^a|^2 V_0^{z'} + |\alpha_1^a|^2 V_1^{z'} + \alpha_0^a \alpha_1^{a*} |0_{z'}\rangle\langle 1_{z'}| + \alpha_0^{a*}\alpha_1^a |1_{z'}\rangle\langle 0_{z'}|, \\ V_b^{z'} &= |\beta_0^b|^2 V_0^z + |\beta_1^b|^2 V_1^z + \beta_0^b \beta_1^{b*} |0_z\rangle\langle 1_z| + \beta_0^{b*}\beta_1^b |1_z\rangle\langle 0_z|. \end{aligned} \tag{3.46}$$

Plugging (3.46) in (3.43), summing (3.43) and summing over a and b in $\{0,1\}$,

$$
\begin{aligned}
4\sum_{a,b}\langle A_a^z B_b^{z'}\rangle = \langle((1+|\beta_0^0|^2)V_0^z + (1+|\alpha_0^0|^2)V_0^{z'} + \beta_0^0\beta_1^{0*}|0_z\rangle\langle 1_z| + \beta_0^{0*}\beta_1^0|1_z\rangle\langle 0_z| + \\
\alpha_0^0\alpha_1^{0*}|0_{z'}\rangle\langle 1_{z'}| + \alpha_0^{0*}\alpha_1^0|1_{z'}\rangle\langle 0_{z'}|)A_0^z B_0^{z'}\rangle + (2+|\beta_1^0|^2)\langle V_1^z A_0^z B_0^{z'}\rangle + (2+|\alpha_1^0|^2)\langle V_1^{z'} A_0^z B_0^{z'}\rangle + \\
\langle((1+|\beta_0^1|^2)V_0^z + (1+|\alpha_1^0|^2)V_1^{z'} + \beta_0^1\beta_1^{1*}|0_z\rangle\langle 1_z| + \beta_0^{1*}\beta_1^1|1_z\rangle\langle 0_z| + \\
\alpha_0^0\alpha_1^{0*}|0_{z'}\rangle\langle 1_{z'}| + \alpha_0^{0*}\alpha_1^0|1_{z'}\rangle\langle 0_{z'}|)A_0^z B_1^{z'}\rangle + (2+|\beta_1^1|^2)\langle V_1^z A_0^z B_1^{z'}\rangle + (2+|\alpha_0^0|^2)\langle V_0^{z'} A_0^z B_1^{z'}\rangle + \\
\langle((1+|\beta_1^0|^2)V_1^z + (1+|\alpha_0^1|^2)V_0^{z'} + \beta_0^0\beta_1^{0*}|0_z\rangle\langle 1_z| + \beta_0^{0*}\beta_1^0|1_z\rangle\langle 0_z| + \\
\alpha_0^1\alpha_1^{1*}|0_{z'}\rangle\langle 1_{z'}| + \alpha_0^{1*}\alpha_1^1|1_{z'}\rangle\langle 0_{z'}|)A_1^z B_0^{z'}\rangle + (2+|\beta_0^0|^2)\langle V_0^z A_1^z B_0^{z'}\rangle + (2+|\alpha_1^1|^2)\langle V_1^{z'} A_1^z B_0^{z'}\rangle + \\
\langle((1+|\beta_1^1|^2)V_1^z + (1+|\alpha_1^1|^2)V_1^{z'} + \beta_0^1\beta_1^{1*}|0_z\rangle\langle 1_z| + \beta_0^{1*}\beta_1^1|1_z\rangle\langle 0_z| + \\
\alpha_0^1\alpha_1^{1*}|0_{z'}\rangle\langle 1_{z'}| + \alpha_0^{1*}\alpha_1^1|1_{z'}\rangle\langle 0_{z'}|)A_1^z B_1^{z'}\rangle + (2+|\beta_0^1|^2)\langle V_0^z A_1^z B_1^{z'}\rangle + (2+|\alpha_0^1|^2)\langle V_0^{z'} A_1^z B_1^{z'}\rangle.
\end{aligned}
\tag{3.47}
$$

Using that $A_0^z + A_1^z \preceq \mathbb{I}$ and $B_0^{z'} + B_1^{z'} \preceq \mathbb{I}$ and (3.39) and (3.40), as in the derivation of (3.36), and bounding the terms that do not correspond to $\langle V_{1-a} A_a B_b\rangle$ or $\langle V'_{1-b} A_a B_b\rangle$ by the operator norm, we obtain (3.37). □

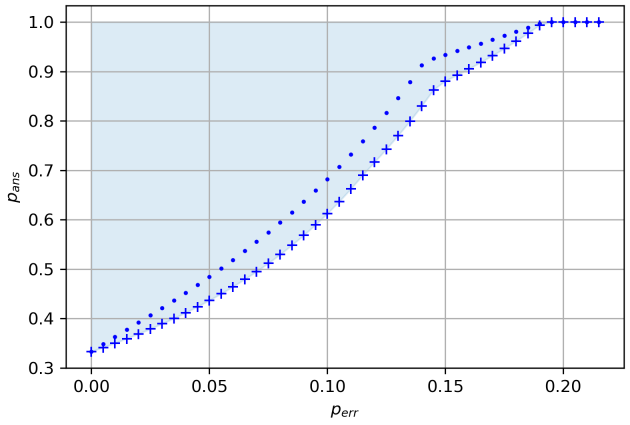


Figure 3.5: Solutions of the first (blue dots) and second level (blue pluses) of the NPA hierarchy for the SDP (3.48) highlighting a $SSR \subseteq SR$ of the $\mathrm{QPV}^{\eta}_{(3,2,2)}$ protocol in light blue.

Therefore, using the above constraints, p_{ans} can be upper bounded by the SDP problem:

$$
\boxed{
\begin{aligned}
&\max \frac{1}{k}\sum_z (\langle A_0^z B_0^z\rangle + \langle A_1^z B_1^z\rangle); \\
&\text{subject to: the linear constraints for } \mathbf{S}_{\eta}^{k_{\theta\varphi}} \in \mathcal{Q}_{\ell}, \\
&\qquad\qquad \text{and equations (3.35), (3.36) and (3.37).}
\end{aligned}
}
\tag{3.48}
$$

Figure 3.5 shows an SSR for the $\mathrm{QPV}^{\eta}_{(3,2,2)}$ protocol, defined analogous as in Definition 3.2.7, obtained from the solutions of the SDP (3.48) using the Ncpol2sdpa package [Wit15] in Python, see [EFS] for the code. Notice that Figure 3.5 shows that the security region for this protocol is greater than the SR of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, meaning that it is more secure. However, analytical bounds on the best attack for these MoE games (even for the lossless case) are so far only known for the BB84 game, and therefore we can not show tightness of our results beyond the $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ protocol—a gap between our best upper bounds and lower bounds remains. We close this gap in Chapter 5. Numerical results from (3.48) show that for different arbitrary k, p_{ans} for $p_{err} = 0$ is upper bounded by $\frac{1}{k}$, which is attainable by the strategy of Alice randomly guessing z, measuring in this basis, broadcasting the outcome and answering if she was correct and otherwise claiming no photon.

As stated above, finding the smallest p_{err} such that $p_{ans} = 1$ can be used to upper bound the winning probability p_{win}. Figure 3.6 shows the values upper bounding p_{win} with the SDP (3.48), showing security of the protocol for different (k, k_θ, k_φ), compared with the upper bound obtained by (3.33) [TFKW13], when the attackers always 'play', where significant differences between both methods can be appreciated. The security of the sequential repetition of $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ is obtained as in the proof of Theorem 4.2.13 adjusting the parameters accordingly for the particular choice of $k_{\theta\varphi}$.

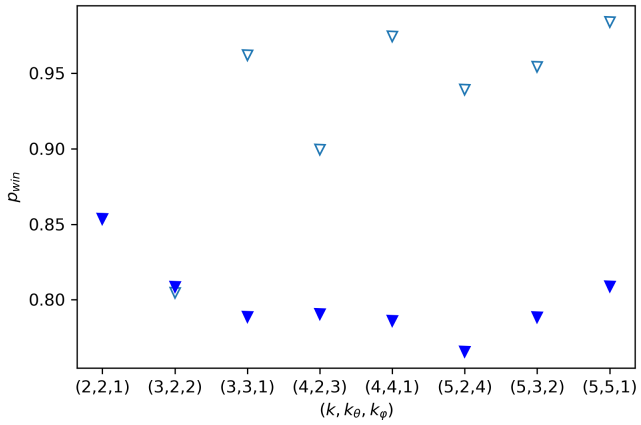


Figure 3.6: Upper bounds of p_{win} using (3.33) (empty triangles) and the solution of SDP (3.48) (solid triangles) for the $\mathrm{QPV}^{\eta}_{k_{\theta\varphi}}$ protocol for different values of (k, k_θ, k_φ).

Chapter 4

Loss and entanglement in single-qubit position verification

To realize quantum position verification (QPV) in practice, a protocol must withstand the three main challenges identified in Chapter 1: (i) adversaries sharing pre-entanglement, (ii) photon loss, and (iii) slower-than-light propagation of quantum messages. In Chapter 3, we addressed (ii) by designing *partially loss-tolerant* protocols—schemes that remain secure provided the loss rate stays below a fixed threshold. However, challenges (i) and (iii) were still unresolved in that setting.

A complementary line of work [BCS22] extends QPV_{BB84} by introducing additional *classical* information. This modification yields security against adversaries who pre-share a number of entangled qubits that scales linearly with the size of the classical data. Since classical information is much cheaper and easier to handle than quantum resources, the protocol's soundness can be amplified simply by increasing the classical input size. Moreover, only the timing of these classical messages is relevant—transmitting classical information near the speed of light in vacuum is feasible with current technology (e.g. radio waves)—so the scheme also circumvents challenge (iii). However, it still falls short in addressing the critical issue of photon loss (ii).

In this chapter, we close that gap. Combining the loss-analysis techniques from Chapter 3 with the approach of [BCS22], we study a lossy version of QPV_{BB84} with extra classical information and show that it stays secure even when slightly under 50% of the photons are lost. We then generalize our results to variants of the protocol that achieve greater loss tolerance.

The results presented in this chapter are based on the following publication:

- *Phys. Rev. Lett. 131, 140802*, "Single-Qubit Loss-Tolerant Quantum Position Verification Protocol Secure against Entangled Attackers," by Llorenç Escolà-Farràs, and Florian Speelman [EFS23].

4.1 Introduction

Attackers who pre-share an arbitrary amount of entanglement can, in principle, successfully break *any* quantum position verification (QPV) protocol, since generic attacks exist that allow the verifiers to *accept* a claimed location *pos* with probability arbitrarily close to one [BCF+14]. However, the best-known construction of such an attack requires the adversaries to pre-share an *exponential* number of entangled qubits [BK11], which is far beyond realistic assumptions, even for future fault-tolerant quantum computers. Thus, although information-theoretic security in QPV is ruled out in general, there remains hope for practical security against powerful but resource-bounded adversaries.

Most QPV protocols in the literature have been shown to be insecure even under modest amounts of pre-shared entanglement, see e.g. [KMS11]. A significant advance came in [BFSS13], where the authors first analyzed a modification of $\mathrm{QPV}_{\mathrm{BB84}}$ involving the addition of *classical* information to the protocol, and demonstrated that this improved its security. By incorporating the classical inputs into the protocol, they were able to increase the quantum resources required for a successful attack, thereby making the protocol more resistant to adversaries with limited entanglement. This idea was further developed and analyzed in [BCS22]. The advantage can intuitively be seen for the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, where the verifiers agree on a BB84 state $H^z|v\rangle$, and send v and z to the prover. The prover must measure the received qubit in the basis indicated by z and report the outcome. The known attack described in Chapter 1 relies on the adversaries pre-sharing a single EPR pair and using teleportation, with Bob measuring in the basis z received from V_1. This attack is disabled by "hiding" the value of z from Bob prior to communication with Alice. To do so, one can split z into two n-bit strings $x, y \in \{0,1\}^n$ sent by V_0 and V_1, respectively. A public Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ determines $z = f(x,y)$, which can only be computed for the first time at the claimed location *pos* due to relativistic constraints. We denote this extension as $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. The adversaries can only reconstruct z after a round of simultaneous communication, once x and y have been exchanged. In [BCS22], it was shown that this modification not only prevents the teleportation-based attack using a single EPR pair, but in fact prevents *any* attack in which the adversaries pre-share a number of qubits that scales linearly with n.

In this chapter, we analyze the security of the lossy version of this protocol, denoted $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$, where $\eta \in [0,1]$ is the transmission rate of photons from V_0 to P. Following a relaxation of the semidefinite programming approach using Chapter 3, we show that a central technical lemma from [BCS22] has a lossy analog. Specifically, if adversaries—after one round of communication—prepare a quantum state that performs well for some basis z, then this same state (or any state close to it) must necessarily perform significantly worse for the complementary basis $1 - z$. A key observation is that the adversaries cannot know z before

they exchange x and y, and therefore any state they prepare beforehand cannot depend explicitly on z. This lack of adaptability constrains the attackers. Furthermore, we show that these states must be sufficiently far apart, which places a lower bound on the dimension of the quantum system required to implement such an attack.

To formalize the dimensional constraints, we make the observation that the set of states of a given fixed dimension is isomorphic to a real unit hypersphere, and similarly for the sets of unitaries, which will be the actions that the attackers will perform before they communicate. We then use δ-nets of the unit spheres whose elements are to be interpreted as quantum states and unitary operations that will be used to approximate/discretize the actions of the attackers. We will see that with these δ-nets, one can construct a compression of a function f. Then, using a counting argument, we will show that if the dimension of the state the attackers pre-share is not large enough, the number of compressions they can implement is exponentially far from the number of Boolean functions f that can be implemented. From this, we derive our first main result: $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ remains secure against adversaries with a linear number of entangled qubits, as long as the photon loss rate is slightly below 50%—essentially matching the threshold found in Chapter 4 but now in a significantly stronger model (though at the cost of reduced error tolerance).

Remarkably, the protocol requires the honest prover to manipulate only a single qubit (a basic measurement), whereas adversaries must manage a linearly-sized entangled quantum state. For example, if each verifier sends 1 kB of classical information, then the protocol is secure against adversaries holding fewer than $4{\cdot}10^3$ pre-shared qubits.

Since we consider both photon loss and measurement error, the verifiers do not receive binary answers in each round—each response can be correct, incorrect, or a loss. As a result, there is no well-defined per-round probability of attack failure, and thus no immediate notion of *catching* the attackers in a single round. A decision to *accept* or *reject* the claimed location must therefore be made based on statistical evidence accumulated over many rounds. In this chapter, we analyze the sequential repetition of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ and introduce a non-trivial statistical test that an honest prover passes with exponentially high probability, whereas any adaptive adversary—i.e. one who adjusts their strategy based on intermediate outcomes—will be caught with exponentially high probability (in the number of rounds). The test is based on the geometry of the 2-dimensional probability simplex, which captures the distribution over the three possible responses. This approach is applicable more broadly and was later generalized by the author in [ABB+23].

Finally, to enable QPV over longer distances, we must address a structural limitation of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$. As described in Chapter 1, a trivial attack succeeds whenever adversaries correctly guess the basis z (with probability at least 1/2, depending on the function f), and reject rounds in which their guess is incorrect.

This strategy allows them to simulate loss rates of 50% or more while always responding correctly when they do not claim loss. To overcome this limitation, we extend the protocol by increasing the number of possible measurement bases, as previously explored in Chapter 3. Specifically, we consider versions where $z = f(x, y)$ takes values in $[k]$, and the qubit must be measured in one of $k \geq 3$ bases. We show that the security techniques developed for $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ can be adapted to this setting, yielding security even at higher loss rates, which improve as k increases. Notably, for $k = 5$ and small error, the protocol remains secure against adversaries who pre-share only a linear number of qubits in n, even when nearly 70% of the photons are lost.

4.2 The $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ protocol

In this section, we describe the lossy version of the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol and its generic attack. We will use $\eta \in [0, 1]$ to represent the photon transmission rate from V_0 to P, and p_{err} to denote the probability that an honest prover returns an incorrect response due to noise or imperfections in the quantum channel. We define one round of the lossy-$\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol as follows:

4.2.1. Definition. *Let $n \in \mathbb{N}$, and consider a $2n$-bit boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. We define one round of the lossy-function-BB84 protocol, denoted by $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$, as follows:*

1. *V_0 and V_1 secretly agree on random bit strings $x, y \in \{0,1\}^n$ and a bit $v \in \{0,1\}$, and let $z = f(x, y)$. Then, V_0 prepares the qubit state $H^z|v\rangle \in \{|0\rangle, |1\rangle, |+\rangle\,|-\rangle\}$.*

2. *V_0 sends the qubit $H^z|v\rangle$, and x to P, whereas V_1 sends y to P, coordinating their times so that the messages arrive simultaneously at pos. The classical information is required to travel at the speed of light, whereas the quantum information can be sent arbitrarily slow.*

3. *Immediately, P computes $z = f(x, y)$, measures the received qubit in the basis z, and broadcasts her outcome, either 0 or 1, to V_0 and V_1. If she did not receive the qubit, i.e. the photon was lost, she sends $\perp$. Therefore, the possible answers from P are $v_{\mathsf{P}} \in \{0, 1, \perp\}$.*

4. *If*

   (a) *V_0 and V_1 receive their respective answers at the time corresponding to pos, and they are equal, i.e. both receive the same v_{P}, then, if*

   - *$v_{\mathsf{P}} = v$, the verifiers record 'Correct', denoted by 'c',*
   - *$v_{\mathsf{P}} = 1 - v$, the verifiers record 'Wrong', denoted by 'w',*

- $v_{\mathsf{P}} = \perp$, *the verifiers record '*No photon*', denoted by '*$\perp$*',*

*(b) otherwise, they record '*Abort*', denoted by '*$\lightning$*', and abort the protocol rejecting the location.*

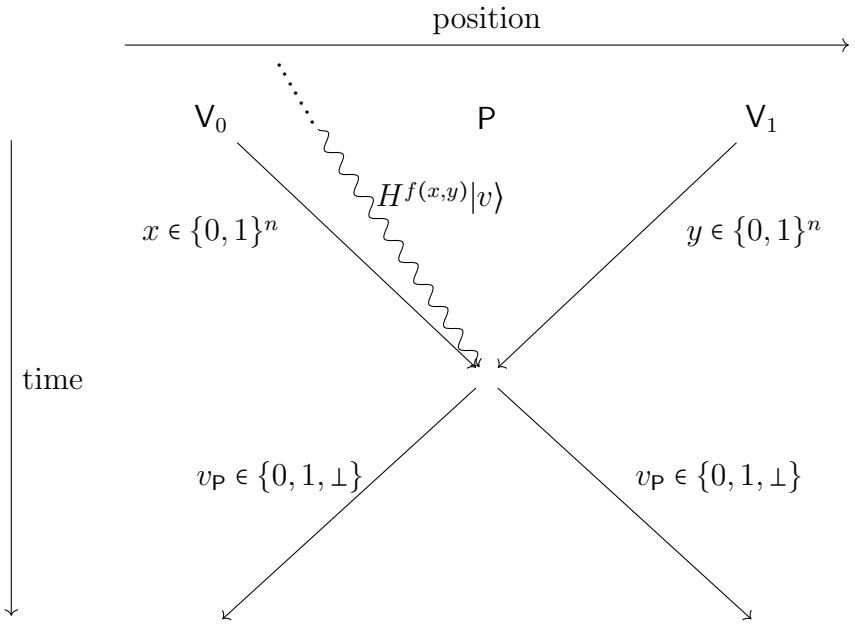


Figure 4.1: Steps 2. and 3. of the $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ protocol, where straight lines represent classical information and undulated lines represent quantum information.

See Figure 4.1 for a schematic representation of steps 2 and 3. Notice that $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ corresponds to $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ for $\eta = 1$ and $p_{err} = 0$. In the same way as for $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, after r rounds, the verifiers expect the answers to satisfy (3.1).

Similarly to $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ in Section 3.2.2, here, we present a binary test to either *accept* or *reject* the location based on the observed data. Let $\mathbf{a}_i \in \{\mathrm{C}, \perp, \mathrm{I}\}$ denote whether the answer that the verifiers recorded in the round i was 'Correct', 'No photon', and 'Wrong' (or 'Abort')[1], respectively. Consider the payoff function

$$T_i^{ent}(\mathbf{a}_i) = \gamma_{\mathrm{C}}\mathbf{1}_{\mathrm{C}}(\mathbf{a}_i) - \gamma_{\perp}\mathbf{1}_{\perp}(\mathbf{a}_i) - \gamma_{\mathrm{I}}\mathbf{1}_{\mathrm{I}}(\mathbf{a}_i), \tag{4.1}$$

where $(\gamma_{\mathrm{C}}, \gamma_{\perp}, \gamma_{\mathrm{I}}) = \frac{1}{\sqrt{488625947}}(943, 1107, 22057)$ and the superscript *ent* is due to that this payoff will be used to securely verify the location even if attackers who pre-share entanglement intend to break $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$. Let

$$\Gamma_r^{ent} = \sum_{i=1}^{r} T_i^{ent}(\mathbf{a}_i), \tag{4.2}$$

[1]The symbol 'I' caputres the *incorrect* answers 'W' and '$\lightning$'.

be the total *score* after r rounds. We next introduce the following acceptance test with confidence level ε_{h}.

4.2.2. Definition. *Let $\varepsilon_h > 0$. For the $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ protocol executed sequentially r times, we define the acceptance test $\mathsf{T}_{\varepsilon_h}^{rf-\mathrm{BB84}}$, also referred to as the decision criterion, as follows: the verifiers* accept *the prover's location if*

$$\Gamma_r^{ent} \geq r(\alpha^{ent} - \delta), \tag{4.3}$$

where $\delta = \sqrt{\frac{4\ln(1/\varepsilon_h)}{r}}$. Otherwise, they reject.

For an honest prover (hp), for every i,

$$\mathbb{E}[T_i^{ent,hp}] = \gamma_{\mathrm{C}}\eta(1-p_{err}) - \gamma_{\perp}(1-\eta) - \gamma_{\mathrm{I}}\eta p_{err} : \alpha^{ent}(\eta, p_{err}), \tag{4.4}$$

and therefore, $\mathbb{E}[\Gamma_r^{ent,hp}] = r\alpha^{ent}$ for simplicity we will assume the dependence on η and p_{err} implicit. By Hoeffding's inequality, see Lemma 3.2.3, with $T_i^{ent} \in [-\frac{22057}{\sqrt{488625947}}, \frac{943}{\sqrt{488625947}}] \subset [-1,1]$, an honest prover will be accepted except with small probability at most ε_{h}, and therefore the test $\mathsf{T}_{\varepsilon_{\mathrm{h}}}^{rf-\mathrm{BB84}}$ is *complete*. We will show that, any attackers who pre-share a linear amount of qubits in n, after r sequential executions of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$, will fail the test with exponentially high probability, and thus showing *soundness*. Showing both completeness and soundness will prove that $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ is *secure*.

Similarly as $\mathsf{T}_{\varepsilon_{\mathrm{h}}}^{r\mathrm{BB84}}$, this test is engineered from the analysis of the correlations attainable by attackers in Section 4.2, ensuring that they are rejected except with negligible probability; see the proof of Theorem 4.2.13 for details of its construction.

As introduced in Chapter 3, for the security analysis, we will consider the purified version of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$, which is equivalent to it, and the difference relies on, V_0 preparing an EPR pair $|\Phi^+\rangle_{VP}$, keeping a qubit register V, and sending the register P to the prover. In a later moment, the V_0 performs the measurement $\{V_v^{f(x,y)} = H^{f(x,y)}|v\rangle\langle v|_V H^{f(x,y)}\}_{v\in\{0,1\}}$ in his local register V_0.

Consider a general attack to the $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ protocol, where Alice and Bob take the same role as in Section 3.2.1, but in addition, prior to the execution of the protocol, they can pre-share entanglement. In the most general attack to $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$, Alice and Bob proceed as follows:

1. Alice intercepts the qubit state with register P sent by V_0, and applies an arbitrary quantum operation to it and to a local register that she possesses, possibly entangling them. She keeps part of the resulting state, and sends the rest to Bob. Since the qubit P can be sent arbitrarily slow by V_0 (the verifiers only time the classical information), this happens before Alice and Bob can intercept x and y.

2. Alice intercepts x and Bob intercepts y. At this stage, Alice, Bob, and V_0 share a quantum state $|\varphi\rangle$, make a partition and let q be the number of qubits that Alice and Bob each hold, recall that V_0 holds a qubit with register V, and thus the three parties share a quantum state $|\varphi\rangle$ of $2q+1$ qubits. Alice and Bob apply a unitary $U^x_{A_{\mathrm{k}}A_{\mathrm{c}}}$ and $V^y_{B_{\mathrm{k}}B_{\mathrm{c}}}$ on their local registers $A_{\mathrm{k}}A_{\mathrm{c}} =: A$ and $B_{\mathrm{k}}B_{\mathrm{c}} =: B$, where k and c denote the registers that will be kept and communicated, respectively. Due to the Stinespring dilation, we consider unitary operations instead of quantum channels. They end up with the quantum state $|\psi_{xy}\rangle = \mathbb{I}_V \otimes U^x_{A_{\mathrm{k}}A_{\mathrm{c}}} \otimes V^y_{B_{\mathrm{k}}B_{\mathrm{c}}}|\varphi\rangle$.

3. Alice sends register A_{c} and x to Bob (and keeps register A_{k}), and Bob sends register B_{c} and y to Alice (and keeps register B_{k}).

4. Alice and Bob perform POVMs $\{A^{xy}_a\}_{a\in\{0,1,\perp\}}$ and $\{B^{xy}_b\}_{b\in\{0,1,\perp\}}$ on their local registers $A_{\mathrm{k}}B_{\mathrm{c}} =: A'$ and $B_{\mathrm{k}}A_{\mathrm{c}} =: B'$, and answer their outcomes a and b to their closest verifier, respectively.

See Figure 4.2 for a schematic representation of the general attack to $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$. The tuple $\mathbf{S}_\eta^{f-\mathrm{BB84}} := \{|\varphi\rangle, U^x, V^y, \{A^{xy}_a\}_a, \{B^{xy}_b\}_b\}_{x,y}$ will be called a q-qubit strategy for $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$. Then, given the strategy $\mathbf{S}_\eta^{f-BB84}$, the probabilities that the verifiers, after the attackers' actions (for the random variable V_{AB}, as denoted above) record Correct (c), Wrong (w), No photon ($\perp$), and Abort ($\lightning$) are, respectively, given by

$$\begin{aligned}
\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{c}] &= \frac{1}{2^{2n}} \sum_{a\in\{0,1\},x,y\in\{0,1\}^n} \mathrm{Tr}\Big[|\psi_{xy}\rangle\langle\psi_{xy}|V_a^{f(x,y)} \otimes A^{xy}_a \otimes B^{xy}_a\Big],\\
\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{w}] &= \frac{1}{2^{2n}} \sum_{a\in\{0,1\},x,y\in\{0,1\}^n} \mathrm{Tr}\Big[|\psi_{xy}\rangle\langle\psi_{xy}|V_a^{f(x,y)} \otimes A^{xy}_{1-a} \otimes B^{xy}_{1-a}\Big],\\
\Pr[\mathrm{V}_{\mathrm{AB}} = \perp] &= \frac{1}{2^{2n}} \sum_{x,y\in\{0,1\}^n} \mathrm{Tr}[|\psi_{xy}\rangle\langle\psi_{xy}|\mathbb{I}_V \otimes A^{xy}_\perp \otimes B^{xy}_\perp],\\
\Pr[\mathrm{V}_{\mathrm{AB}} = \lightning] &= \frac{1}{2^{2n}} \sum_{a\neq b\in\{0,1,\perp\},x,y\in\{0,1\}^n} \mathrm{Tr}\Big[|\psi_{xy}\rangle\langle\psi_{xy}|\mathbb{I}_V \otimes A^{xy}_a \otimes B^{xy}_b\Big].
\end{aligned} \tag{4.5}$$

4.2.1 Security of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$

Our goal is to show that if the number of qubits q that the attackers hold at the beginning of the protocol is linear, then, given that they do not respond '$\perp$', their probability of being correct is strictly less than the corresponding probability of the honest prover. To this end, we define a relaxation of the condition of being correct, and we consider q-qubit strategies which have a high chance that the verifiers record Correct at the end of the protocol. More specifically, we will define a set of quantum states that are 'good' for a given fixed input, conditioned

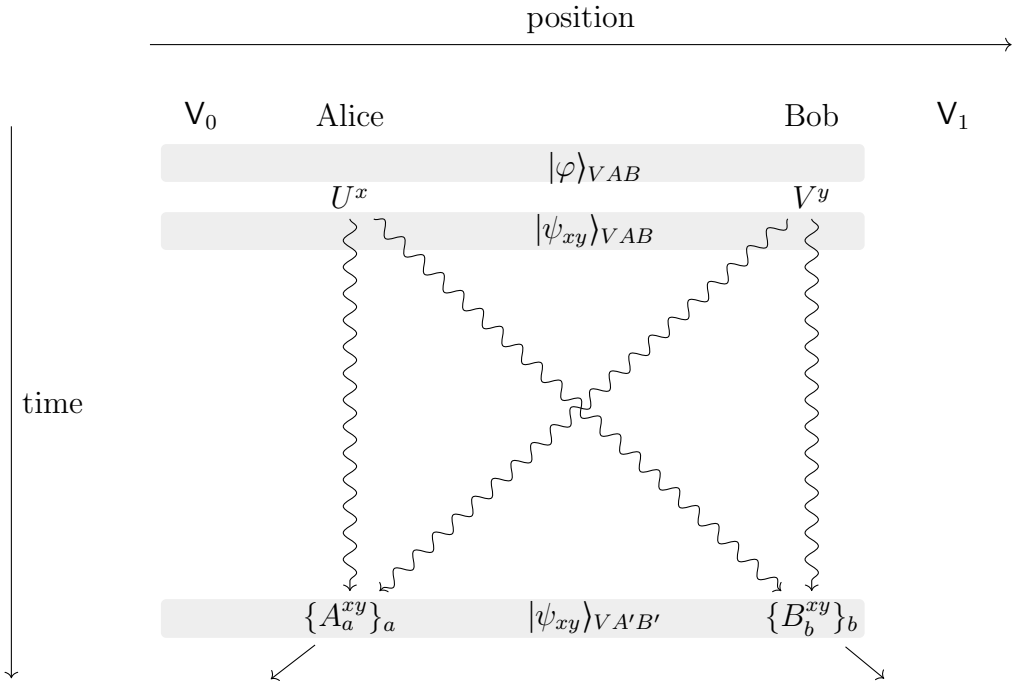


Figure 4.2: Schematic representation of a general attack on $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$. Straight lines represent classical information, and undulated lines represent quantum information, including x and y. The gray-shaded regions represent the corresponding tripartite quantum states in them. Since the attacks share the same structure, by correspondingly modifying the dimension of $|\varphi\rangle$ (and thus $|\psi_{xy}\rangle$), and the range of the outputs a, and b, the diagram also depicts a generic attack to the m-fold parallel repetition of $\mathrm{QPV}_{\mathrm{BB84}}^{f}(\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m})$, and to the $\mathrm{QPV}_{\mathrm{coh}}^{f}$ protocol, analyzed in Chapters 8 and 9, respectively.

on actually playing. The first definition, which is an extension of Definition 4.1 in [BCS22], considers single round attacks that are 'good' for $l \leq 2^{2n}$ pairs of x, y. The reason to do so is that the attackers could be wrong for pairs that might be asked with exponentially small probability.

4.2.3. Definition. *Let $\varepsilon \geq 0$ and $l \in \mathbb{N}$. A q-qubit strategy*

$$\mathbf{S}_{\eta}^{f-BB84} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$$

for $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ is (ε,l)-perfect *if there exists a set $\mathcal{L}$ with $|\mathcal{L}| \geq l$, such that the attackers*

1. *'respond' with probability η on these pairs:*

$$\mathrm{Tr}[|\psi_{xy}\rangle\langle\psi_{xy}|\mathbb{I}_V \otimes A_{\perp}^{xy} \otimes B_{\perp}^{xy}] = 1 - \eta \ \forall (x,y) \in \mathcal{L}, \tag{4.6}$$

2. *and, up to* ε*, they are* Correct *at least with the same probability as an honest prover:*

$$\sum_{a\in\{0,1\}} \mathrm{Tr}\Big[|\psi_{xy}\rangle\langle\psi_{xy}|V_a^{f(x,y)}\otimes A_a^{xy}\otimes B_a^{xy}\Big] \geq \eta\big((1-p_{err})-\varepsilon\big)\ \forall (x,y)\in\mathcal{L}. \quad (4.7)$$

4.2.4. Definition. *Let Alice and Bob hold arbitrary registers* A *and* B*, respectively, and let* $\varepsilon\geq 0$*. Let* V *be a qubit register. We define the set* $\mathcal{S}_z^\varepsilon$ *as*

$$\mathcal{S}_z^\varepsilon := \{|\psi\rangle_{VAB} \mid \exists\ \textit{POVMs}\ \{A_a^z\}\ \textit{and}\ \{B_b^z\}\ \textit{acting on}\ A\ \textit{and}\ B,\ \textit{respectively such that}\ (4.9)\ \textit{and}\ (4.10)\ \textit{are fulfilled}\}, \quad (4.8)$$

where

$$\sum_{a\in\{0,1\}} \mathrm{Tr}[|\psi\rangle\langle\psi|V_a^z\otimes A_a^z\otimes B_a^z] \geq \eta\big((1-p_{err})-\varepsilon\big), \quad (4.9)$$

and

$$\mathrm{Tr}[|\psi\rangle\langle\psi|\mathbb{I}_V\otimes A_\perp^z\otimes B_\perp^z] = 1-\eta. \quad (4.10)$$

Given basis $z\in\{0,1\}$, and a state $|\psi\rangle$, fulfilling responding $a=b\neq\perp$ with probability η and $\perp$ with probability $1-\eta$ on this z, and never responding $a\neq b$, the (normalized) maximum probability of being correct for such input is given by

$$p_\psi^{z,\eta} := \frac{1}{\eta} \max_{\substack{\{A_a^z,B_a^z\}_{a\in\{0,1,\perp\}} \\ \text{with } \mathrm{Tr}\left[|\psi\rangle\langle\psi|A_a^zB_b^z\right]=0,\forall a\neq b\in\{0,1,\perp\}, \\ \text{and } \mathrm{Tr}[|\psi\rangle\langle\psi|A_\perp^zB_\perp^z]=1-\eta}} \sum_{a\in\{0,1\}} \mathrm{Tr}[|\psi\rangle\langle\psi|V_a^zA_a^zB_a^z], \quad (4.11)$$

where $\{A_a^z,B_a^z\}_{a\in\{0,1,\perp\}}$ are POVMs. Due to Theorem 3.2.10, from the SDP (3.24), we have that there exists a function $w:[0,1]\to[1-\cos^2(\frac{\pi}{8}),1]$ such that for all states $|\psi\rangle$, regardless of their dimension, upper bounds the following quantity:

$$\frac{1}{2}\big(p_\psi^{0,\eta}+p_\psi^{1,\eta}\big)\leq w(\eta). \quad (4.12)$$

Moreover, consider the following relaxation of (4.11), where the restrictions are such that the attackers respond with different answers with probability ϵ and have a response rate in the interval $[(1-\eta)-\epsilon,(1-\eta)+\epsilon]$,

$$\tilde{p}_\psi^{z,\eta,\epsilon} = \frac{1}{\eta} \max_{\substack{\{A_a^z,B_a^z\}_{a\in\{0,1,\perp\}} \\ \text{with } \mathrm{Tr}\left[|\psi\rangle\langle\psi|A_a^zB_b^z\right]\leq\epsilon,\forall a\neq b\in\{0,1,\perp\}, \\ \text{and } (1-\eta)-\epsilon\leq\mathrm{Tr}[|\psi\rangle\langle\psi|A_\perp^zB_\perp^z]\leq(1-\eta)+\epsilon}} \sum_{a\in\{0,1\}} \mathrm{Tr}[|\psi\rangle\langle\psi|V_a^zA_a^zB_a^z]. \quad (4.13)$$

On the other hand, let $\epsilon=0.001$, and consider the relaxation of (3.24) consisting of replacing (3.22) by $\langle A_a^zB_b^z\rangle\leq\epsilon\ \forall a\neq b\in\{0,1,\perp\}$, $\forall z\in\{0,1\}$ and (3.23) by $\sum_{ab}(2-\|V_a^z+V_b^{z'}\|)\langle A_a^zB_b^{z'}\rangle\leq p_{err}(4\epsilon+\sum_a\langle A_a^zB_a^z\rangle+\langle A_a^{z'}B_a^{z'}\rangle)+8\epsilon$, where the latter

inequality is obtained analogously to (3.23) by bounding the terms $\langle A_a^z B_b^z \rangle \leq \epsilon$, for all $a \neq b$. This implies that there exists a function $\tilde{w}^\epsilon : [0,1] \to (1-\cos^2(\frac{\pi}{8})+\epsilon, 1]$, obtained by the relaxation of the SDP (and allowing extra ϵ for the response rate), such that for all states $|\psi\rangle$, regardless of their dimension, upper bounds the performance of the attackers who are allowed to respond different answers with probability ϵ and have a response rate in the interval $[(1-\eta)-\epsilon, (1-\eta)+\epsilon]$:

$$\frac{1}{2}\left(\tilde{p}_\psi^{0,\eta,\epsilon} + \tilde{p}_\psi^{1,\eta,\epsilon}\right) \leq \tilde{w}^\epsilon(\eta), \tag{4.14}$$

and $\tilde{w}^\epsilon(\eta)$ is such that $w(\eta) \leq \tilde{w}^\epsilon(\eta)$. This inequality is due to the fact that the latter is obtained by a relaxation of the constraints of the SDP of the former.

Due to the fact that $p_{win} + p_{err} \leq 1$, the plot in Figure 3.3 can be represented in terms of the winning probability p_{win}, see Section 4.2.1. The plotted points in Section 4.2.1 represent a numerical approximation of the functions $w(\eta)$ and $\tilde{w}^\epsilon(\eta)$.

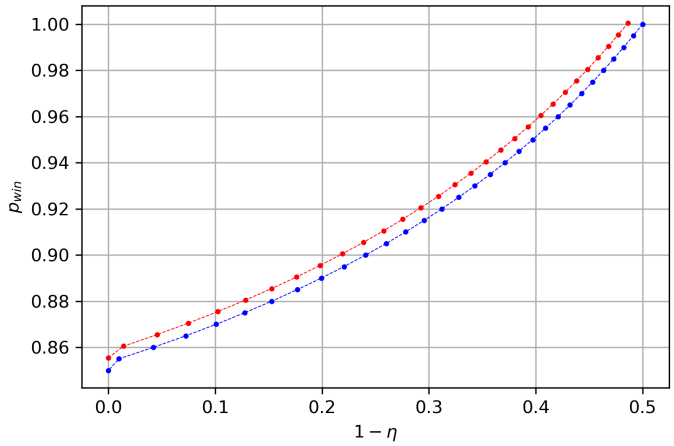


Figure 4.3: Upper bounds of the winning probability given by (3.24) (blue dots), (equivalent representation of the blue pluses in Figure 3.3), which corresponds to a numerical representation of the function $w(\eta)$. Red dots correspond to a numerical representation of the function $\tilde{w}^\epsilon(\eta)$, which is obtained by adding $\epsilon = 0.001$ to the relaxation of (3.24) where the attackers are allowed to make errors with probability ϵ. The continuous interpolation between values is meant for a better viewing of the plot.

Now, we prove that the difference between the probabilities obtained by two quantum states projected into the same space is upper bounded by their trace distance. We then use this result to show that if two quantum states can be used to successfully attack around of the protocol with high probability with the POVMs $\{A_a^{xy}\}$ and $\{B_b^{xy}\}$ for input 0 and 1 of a q–qubit strategy for $\text{QPV}_{\text{BB84}}^{\eta,f}$,

respectively, these two states have to differ by at least a certain amount. These results are formalized in the next proposition and lemma.

4.2.5. Proposition. *Let* $|\psi\rangle$ *and* $|\varphi\rangle$ *be two quantum states of (the same) arbitrary dimension, and let* $\mathcal{D}(|\psi\rangle,|\varphi\rangle)$ *denote their trace distance. Then, for every projector* Π*,*

$$|\mathrm{Tr}[(|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|)\Pi]| \leq \mathcal{D}(|\psi\rangle,|\varphi\rangle). \tag{4.15}$$

Proof:
There exist Q and S positive operators with orthogonal support [NC11, Chapter 9] such that

$$|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| = Q - S, \text{ and } \mathcal{D}(|\psi\rangle,|\varphi\rangle) = \mathrm{Tr}[Q] = \mathrm{Tr}[S]. \tag{4.16}$$

Then,

$$\begin{aligned}\mathrm{Tr}[(|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|\Pi)] = \mathrm{Tr}[(Q-S)\Pi] = \mathrm{Tr}[Q\Pi] - \mathrm{Tr}[S\Pi] \leq \mathrm{Tr}[Q\Pi] \\ \leq \mathrm{Tr}[Q]\|\Pi\|_\infty = \mathcal{D}(|\psi\rangle,|\varphi\rangle),\end{aligned} \tag{4.17}$$

where we used that S is positive definite and $\|\Pi\|_\infty = 1$. □

4.2.6. Lemma. *Let* $\Delta > 0$*, and let* $|\psi\rangle$ *and* $|\varphi\rangle$ *be such that* $p^{1,\eta}_{\psi} \geq \tilde{w}^{\epsilon}(\eta) + \Delta$ *and* $p^{0,\eta}_{\varphi} \geq \tilde{w}^{\epsilon}(\eta) + \Delta$*, which, due to Definition 4.2.4,* $|\psi\rangle \in \mathcal{S}^{\varepsilon}_0$ *and* $|\varphi\rangle \in \mathcal{S}^{\varepsilon}_1$*, for* $\varepsilon = 1 - (\tilde{w}^{\epsilon}(\eta) + \Delta)$*. Then,*

$$\mathcal{D}(|\psi\rangle,|\varphi\rangle) \geq \eta\Delta. \tag{4.18}$$

Notice that the hypothesis of Lemma 4.2.6 implies that $p^{1,\eta}_{\psi}, p^{0,\eta}_{\varphi} \geq \tilde{w}^{\epsilon}(\eta) + \Delta > w(\eta)$ and thus these two states perform better in inputs 1 and 0, respectively, than any state would perform on average on both inputs. The greater is Δ, the better they can perform.

Proof:
Let $\epsilon = \mathcal{D}(|\psi\rangle,|\varphi\rangle)$ and $\psi = |\psi\rangle\langle\psi|$, $\varphi = |\varphi\rangle\langle\varphi|$. Subtracting and adding φ to ψ in Equation (4.11) for $i = 1$,

$$\begin{aligned}\eta p^{1,\eta}_{\psi} &= \max_{\substack{\{A^1_a,B^1_a\}_{a\in\{0,1,\perp\}} \\ \text{with } \mathrm{Tr}[\psi A^1_a B^1_b]=0,\forall a\neq b\in\{0,1,\perp\}, \\ \text{and } \mathrm{Tr}[\psi A^1_\perp B^1_\perp]=1-\eta}} \sum_{a\in\{0,1\}} \mathrm{Tr}\big[(\psi-\varphi+\varphi)V^1_a A^1_a B^1_a\big] \\ &\leq 2\epsilon + \max_{\substack{\{A^1_a,B^1_a\}_{a\in\{0,1,\perp\}} \\ \text{with } \mathrm{Tr}[\psi A^1_a B^1_b]=0,\forall a\neq b\in\{0,1,\perp\}, \\ \text{and } \mathrm{Tr}[\psi A^1_\perp B^1_\perp]=1-\eta}} \sum_{a\in\{0,1\}} \mathrm{Tr}\big[\varphi V^1_a A^1_a B^1_a\big] \\ &\leq 2\epsilon + \max_{\substack{\{A^1_a,B^1_a\}_{a\in\{0,1,\perp\}} \\ \text{with } \mathrm{Tr}[\varphi A^1_a B^1_b]\leq\epsilon,\forall a\neq b\in\{0,1,\perp\}, \\ \text{and } (1-\eta)-\epsilon\leq\mathrm{Tr}[\varphi A^1_\perp B^1_\perp]\leq(1-\eta)+\epsilon}} \sum_{a\in\{0,1\}} \mathrm{Tr}\big[\varphi V^1_a A^1_a B^1_a\big] = 2\epsilon + \eta\tilde{p}^{1,\eta,\epsilon}_{\varphi},\end{aligned} \tag{4.19}$$

where the first bound by 2ϵ comes from (4.15) and we used that, because of (4.15), the condition $\mathrm{Tr}\left[\psi A_a^1 B_b^1\right] = 0, \forall a \neq b \in \{0,1,\perp\}$ implies $\mathrm{Tr}\left[\varphi A_a^1 B_b^1\right] \leq \epsilon, \forall a \neq b \in \{0,1,\perp\}$ and condition $\mathrm{Tr}[\psi A_\perp^1 B_\perp^1] = 1-\eta$ implies $(1-\eta)-\epsilon \leq \mathrm{Tr}[\varphi A_\perp^1 B_\perp^1] \leq (1-\eta)+\epsilon$. Combining (4.19), the hypothesis $p_\psi^{1,\eta} \geq \tilde{w}^\epsilon(\eta) + \Delta$ and Equation (4.14), we have

$$\tilde{p}_\varphi^{0,\eta,\epsilon} \leq \tilde{w}^\epsilon(\eta) - \Delta + \frac{2\epsilon}{\eta}. \tag{4.20}$$

On the other hand, since $\tilde{p}_\varphi^{0,\eta,\epsilon}$ is obtained by relaxing the restrictions of $p_\varphi^{0,\eta}$, we have that $\tilde{p}_\varphi^{0,\eta,\epsilon} \geq p_\varphi^{0,\eta}$ and, by hypothesis, $p_\varphi^{0,\eta} \geq \tilde{w}^\epsilon(\eta) + \Delta$. These, together with (4.20), lead to $\epsilon \geq \eta\Delta$. □

Notice that Lemma 4.2.6 implies that Alice and Bob in some sense have to decide what strategy they follow before they communicate. Consequently, if the dimension of the state they share is small enough, a classical description of the first part of their strategy yields a compression of f. The notion of the following definition captures this classical compression.

4.2.7. Definition. *[BCS22] Let q, κ, $n \in \mathbb{N}$, $\varepsilon > 0$. Then,*

$$g : \{0,1\}^{3\kappa} \to \{0,1\}$$

*is an (ε, q)-*classical rounding *of size κ if for all $f : \{0,1\}^{2n} \to \{0,1\}$, for all states $|\varphi\rangle$ on $2q+1$ qubits, for all $l \in \{1,\ldots,2^{2n}\}$ and for all (ε, l)-perfect q-qubit strategies for $\mathrm{QPV}_{\mathrm{BB84}}^f$, there are functions $f_A : \{0,1\}^n \to \{0,1\}^\kappa$, $f_B : \{0,1\}^n \to \{0,1\}^\kappa$ and $\mu \in \{0,1\}^\kappa$ such that $g(f_A(x), f_B(y), \mu) = f(x,y)$ on at least l pairs (x,y).*

We now demonstrate the existence of an (ε, q)-classical rounding by explicitly constructing one. To this end, we will make use of the following observation. Similarly to Section 4.5.4 in [NC11], notice that any state $|\varphi\rangle$ of $2q+1$ qubits can be decomposed as

$$|\varphi\rangle = \sum_{j=0}^{2^{2q+1}-1} \varphi_j |j\rangle, \tag{4.21}$$

with $\varphi_j \in \mathbb{C}$ for all $j \in [2^{2q+1}]$ and

$$1 = \sum_j |\varphi_j|^2 = \sum_j \mathrm{Re}(\varphi_j)^2 + \mathrm{Im}(\varphi_j)^2. \tag{4.22}$$

The latter corresponds to the condition for a point to be on the unit sphere in $\mathbb{R}^{2\cdot 2^{2q+1}}$, i.e. the unit $(2^{2q+1+1}-1)$-sphere and therefore the set of states can be seen as a unit sphere. Similarly, the set of unitary matrices of dimension d can be seen as the unit $(2d^2-1)$-sphere, since for every $U \in \mathcal{U}(d)$, $UU^\dagger = \mathbb{I}_d$, this will correspond to the unitaries that Alice and Bob apply in the step 2. of the general attack. Then, we will consider a δ-net $\mathcal{N}_S$ in Euclidean norm of the $(2^{2q+1+1}-1)$-sphere, which corresponds to the set of quantum states of $2q+1$ qubits, i.e. the set

of possible states $|\varphi\rangle_{VAB}$ that attackers will start in step 2. of the general attack. Moreover, we will consider δ-nets $\mathcal{N}_A$ in and $\mathcal{N}_B$ in the Schatten ∞-norm of the $(2d^2-1)$-sphere, where $d = 2^q$, which correspond to the set of unitary operators that Alice and Bob apply in step 2. of the general attack, respectively. We will use these δ-nets to approximate the state and unitaries of an arbitrary strategy, and show that they capture the essence of the strategy. We will use the δ-nets to construct the (ε, q)-classical rounding, where ε will depend on δ and the size κ of the rounding will depend on the size of the nets.

4.2.8. Lemma. *(Corollary 4.2.13 in [Ver18]) Let $N \in \mathbb{N}$ and $\delta > 0$. Then, there exists a δ-net, with the Euclidean distance, of the unit sphere in $\mathbb{R}^N$ with cardinality κ at most $\kappa \leq (1+\frac{2}{\delta})^N \leq \left(\frac{3}{\delta}\right)^N$.*

4.2.9. Lemma. *Let $\Delta > 0$, and let $0 \leq \varepsilon \leq \varepsilon_0$, where ε_0 is such that $|\psi_z\rangle \in \mathcal{S}^{\varepsilon}_z$ for $z \in \{0,1\}$ implies $\mathcal{D}(|\psi_0\rangle, |\psi_1\rangle) \geq \eta\Delta$. Then, there exists an (ε, q)-classical rounding of size $\kappa \leq \log(\lceil \frac{4}{2^{\frac{2}{3}}(\eta\Delta+2)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$.*

Proof:
Sketch (see Lemma 4.3.4 for a detailed proof of a generalized version). Consider a δ-net in Euclidean norm for the set of pure state on $2q+1$ qubits, where the net has cardinality at most 2^{κ}. Following the proof of Lemma 4.3.4 analogously, we have that δ is such that $3\delta + 3\delta^2 + \delta^3 < \eta\Delta/2$, which holds for $\delta < (2+\eta\Delta)^{\frac{1}{3}}/2^{\frac{1}{3}} - 1$. By Lemma 4.2.8, we obtain the size $\kappa = \log(\lceil \frac{4}{2^{\frac{2}{3}}(\eta\Delta+2)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$. The remaining part of the proof is analogous to the proof of Lemma 4.3.4. □

4.2.10. Lemma. *Let $\Delta = 0.013$, $\eta \in (0.53, 1]$, $\varepsilon \in [0,1]$ n, k, $q \in \mathbb{N}$, $n \geq 10$. Moreover, fix an (ε, q)-classical rounding g of size κ with $\kappa = \log(\lceil \frac{4}{2^{\frac{2}{3}}(\eta\Delta+2)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$. Let $q \leq \frac{1}{2}n - 5$. Then, a uniformly random $f : \{0,1\}^{2n} \to \{0,1\}$ fulfills the following with probability at least $1 - 2^{-2^n}$: For any $f_A : \{0,1\}^n \to \{0,1\}^{\kappa}$, $f_B : \{0,1\}^n \to \{0,1\}^{\kappa}$, $\mu \in \{0,1\}^{\kappa}$, the equality $g(f_A(x), f_B(y), \mu) = f(x,y)$ holds on less than $3/4$ of all pairs (x,y).*

Proof:
Sketch (see below Lemma 4.2.10 for a detailed proof of the generalized version). We want to estimate the probability that for a randomly chosen f, we can find f_A and f_B such that the corresponding function g is such that $\Pr_{x,y}\{f(x,y) = g(f_A(x), f_B(y), \mu)\} \geq 3/4$. In a similar manner as in (4.46), we have that

$$\Pr[f : \exists f_A, f_B, \mu \text{ s.t. } \Pr_{x,y}\{f(x,y) = g(f_A(x), f_B(y), \mu)\}] \leq 2^{(2^{n+1}+1)k} 2^{2^{2n} h_b(1/4)} 2^{-2^{2n}}, \tag{4.23}$$

where $h_b(\cdot)$ denotes the binary entropy function, see (2.1). If $q \leq n/2 - 5$ and $\kappa = \log(\lceil \frac{4}{2^{\frac{2}{3}}(\eta\Delta+2)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$, with $\Delta = 0.013$, for $\eta \in (0.53, 1]$, the above expression

is strictly upper bounded by 2^{-2^n}. □

Lemma 4.2.10 shows that if the dimension of the initial state that Alice and Bob hold is small enough, any $(\varepsilon, 3/4{\cdot}2^{2n})$-perfect q-qubit strategy needs a number of qubits which is linear in n. This leads to the following theorem:

4.2.11. Theorem. *Consider the most general attack to a round of the* $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ *protocol for a transmission rate* $\eta \in (0.53, 1]$. *Let* $\Delta = 0.013$. *If the attackers respond with probability* η *and control at most* q *qubits at the beginning of the protocol, and* q *is such that*

$$q \leq \frac{n}{2} - 5, \tag{4.24}$$

then, for any q*-qubit strategy for* $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$, *the probability that the attackers answer* Correct *is at most*

$$\Pr[\mathrm{V_{AB}} = \mathrm{C}] \leq \eta\Big(1 - \frac{1}{4}[1 - (\tilde{w}^{\epsilon}(\eta) + \Delta)]\Big). \tag{4.25}$$

The proof of Theorem 4.2.11 is a particular case of the proof of Theorem 4.3.6. See Figure 4.4 for a representation of the bound (4.25). Notice that if $p_{err} < 1 - \frac{1}{4}[1 - (\tilde{w}^{\epsilon}(\eta) + \Delta)]$, then the probability that the attackers answer Correct is strictly below the corresponding probability for an honest prover.

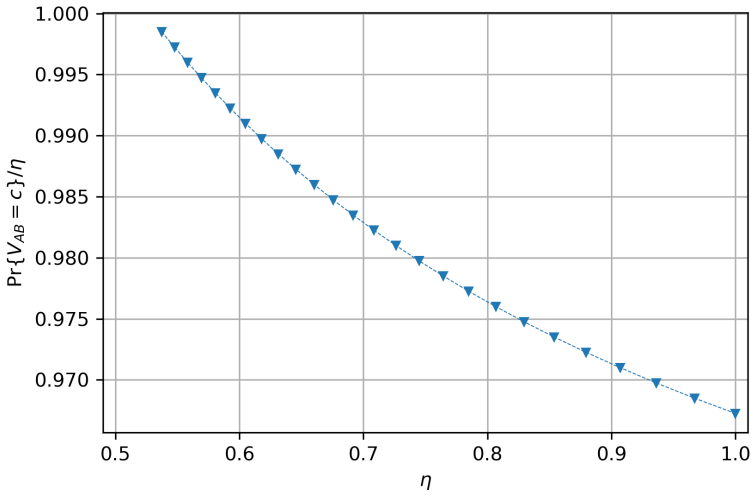


Figure 4.4: Normalized upper bounds (triangles pointing down) given by Theorem 4.2.11 on the probabilities that the attackers are correct given that they answer with probability η.

4.2.2 Sequential repetition of $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$

We will next show that, under the conditions of Theorem 4.2.11, attackers will reproduce a score $\Gamma_r^{ent,att}$ that will fail the $\mathsf{T}^{rf-\mathrm{BB84}}_{\varepsilon_{\mathrm{h}}}$ with exponentially high probability. Let $\mathcal{A} \subseteq \Delta_2$ be the set of probabilities $\mathbf{q} = (q_{\mathrm{C}}, q_{\perp}, q_{\mathrm{I}})$ that the attackers can reproduce, where $q_{\mathrm{I}} \coloneqq q_{\mathrm{W}} + q_{\lightning}$. Notice that since for $\mathbf{q}_1, \mathbf{q}_2 \in \mathcal{A}$, the attackers can play any convex combination of them, the set $\mathcal{A}$ is convex. Let $\Delta = 0.013$ and, for simplicity, denote $\mathfrak{b}_\eta \coloneqq \frac{1}{4}\big(1 - (\tilde{w}^\epsilon(\eta) + \Delta)$. Let $\mathcal{R} \subset \Delta_2$ be the region of the probability simplex defined as $\mathcal{R} \coloneqq \cup_{\eta\in(0.53,1]}\mathcal{R}_\eta \subset \Delta_2$, where the sets $\mathcal{R}_\eta$ are defined as

$$\mathcal{R}_\eta = \Big\{(p_{\mathrm{C}}, p_{\perp}, p_{\mathrm{I}}) \in \Delta_2 \mid p_{\mathrm{C}} > \max\{1 - p_{\perp} + \frac{\mathfrak{b}_\eta(1-2p_{\perp})}{1-2(\eta-\epsilon)}, \frac{\eta-\epsilon-\cos^2(\frac{\pi}{8})-\mathfrak{b}_\eta}{1-(\eta-\epsilon)}p_{\perp} + \cos^2(\frac{\pi}{8})\} \\ \wedge p_{\mathrm{I}} < \min\{\frac{\mathfrak{b}_\eta(1-2p_{\perp})}{2(\eta-\epsilon)-1}, \frac{\mathfrak{b}_\eta - \sin^2(\frac{\pi}{8})}{1-(\eta-\epsilon)}p_{\perp} + \sin^2(\frac{\pi}{8})\}\Big\}. \tag{4.26}$$

4.2.12. Lemma. *Under the conditions of Theorem 4.2.11, any* $\boldsymbol{q}$ *that the attackers can reproduce is such that* $\boldsymbol{q} \notin \mathcal{R}$*, i.e.* $\mathcal{R} \cap \mathcal{A} = \varnothing$*, and thus*

$$\mathcal{A} \subsetneq \mathcal{R}^c. \tag{4.27}$$

Proof:
Let $\mathbf{q} = (q_{\mathrm{C}}, q_{\perp}, q_{\mathrm{I}})$ be the probability distribution corresponding to an attack from Alice and Bob and define $\mathcal{A}$ as the set of all probabilities If they are allowed to answer with probability $\eta \pm \epsilon$, then

$$\mathbf{q} = (q_{\mathrm{C}}, 1 - (\eta + \mu), q_{\mathrm{I}}), \mu \in [-\epsilon, \epsilon]. \tag{4.28}$$

Moreover, by Theorem 4.2.11, if they control at most $q \leq \frac{n}{2} - 5$ qubits at the beginning of the protocol,

$$q_{\mathrm{I}} \geq \mathfrak{b}_\eta, \forall \mu \in [-\epsilon, \epsilon]. \tag{4.29}$$

We define the following region

$$\mathcal{R}^0_\eta = \{(p_{\mathrm{C}}, p_{\perp}, p_{\mathrm{I}}) \in \Delta_2 \mid p_{\perp} \in [1 - (\eta - \epsilon), 1 - (\eta + \epsilon)] \wedge p_{\mathrm{I}} < \mathfrak{b}_\eta\}, \tag{4.30}$$

therefore, by (4.29), $\mathbf{q} \notin \mathcal{R}^0_\eta$, and thus

$$\mathcal{R}^0_\eta \cap \mathcal{A} = \varnothing. \tag{4.31}$$

Notice that the strategies $\mathbf{S}_{\mathrm{TFKW}}$ and $\mathbf{S}_{guess}$, reproduce $\mathbf{q}_{\mathrm{TFKW}} = (\cos^2(\frac{\pi}{8}), 0, 1 - \cos^2(\frac{\pi}{8}))$ and $\mathbf{q}_{guess} = (\frac{1}{2}, \frac{1}{2}, 0)$ and, respectively, and therefore $\mathbf{q}_{\mathrm{TFKW}}, \mathbf{q}_{guess} \in \mathcal{A}$. The attackers can also do the strategies consisting on always responding $\perp$ or always being incorrect (e.g answering inconsistent answers $a \neq b$), which reproduce the probabilities $\mathbf{q} = (0, 1, 0)$ and $\mathbf{q} = (0, 0, 1)$, respectively. Therefore, the convex

hull of these four points is a convex subset of $\mathcal{A}$. Consider the straight line s_1 defined by the two points $\mathbf{q}_{guess}$ and $(\eta-\epsilon-\mathfrak{b}_\eta, 1-(\eta-\epsilon), \mathfrak{b}_\eta) \in \partial\mathcal{R}^0_\eta$, where ∂ denotes the boundary, which is given by

$$s1: \frac{x-\frac{1}{2}}{\eta-\epsilon-\frac{1}{2}-\mathfrak{b}_\eta} = \frac{y-\frac{1}{2}}{\frac{1}{2}-(\eta-\epsilon)} = \frac{z}{\mathfrak{b}_\eta}. \tag{4.32}$$

Consider the set $\mathcal{R}^1_\eta$, defined as the points in Δ_2 that do not belong to $\mathcal{R}^0_\eta$ that are 'below' the straight line s_1 and are such that $p_\perp \leq 1-(\eta+\epsilon)$, formally defined as

$$\mathcal{R}^1_\eta = \left\{(p_{\text{C}}, p_\perp, p_{\text{I}}) \in \Delta_2 \mid p_{\text{C}} > 1-p_\perp + \frac{\mathfrak{b}_\eta(1-2p_\perp)}{1-2(\eta-\epsilon)} \wedge p_{\text{I}} < \frac{\mathfrak{b}_\eta(1-2p_\perp)}{2(\eta-\epsilon)-1}\right\} \setminus \mathcal{R}^0_\eta. \tag{4.33}$$

We will show by contradiction that $\mathcal{R}^1_\eta \cap \mathcal{A} = \varnothing$. Assume that exists $\mathbf{p}_R \in \mathcal{R}^1_\eta \cap \mathcal{A}$. Since $\mathcal{A}$ is a convex set and $\mathbf{q}_{guess} \in \mathcal{A}$, $t\mathbf{p}_R + (1-t)\mathbf{q}_{guess} \in \mathcal{A}$ for all $t \in [0,1]$. By construction of $\mathcal{R}^1_\eta$, $\{t\mathbf{p}_R + (1-t)\mathbf{q}_{guess} \mid t \in [0,1]\} \cap \mathcal{R}^0_\eta \neq \varnothing$, i.e. the straight line connecting $\mathbf{p}_R$ and $\mathbf{q}_{guess}$ intersects $\mathcal{R}^0_\eta$. Then, $\exists t_0 \in [0,1]$ such that $\mathbf{p}_{t_0} := t_0\mathbf{p}_R + (1-t_0)\mathbf{q}_{guess} \in \mathcal{R}^0_\eta \cap \mathcal{A}$. However, by (4.31), $\mathcal{R}^0_\eta \cap \mathcal{A} = \varnothing$. Therefore, $\nexists \mathbf{p}_R \in \mathcal{R}^1_\eta \cap \mathcal{A}$.
Similarly, consider the set $\mathcal{R}^2_\eta$ consisting of the points in Δ_2 that are such that $p_\perp \geq 1-(\eta+\epsilon)$ and that are 'below' the straight line given by the points $\mathbf{q}_{\text{TFKW}}$ and $(\eta-\epsilon-\mathfrak{b}_\eta, 1-(\eta-\epsilon), \mathfrak{b}_\eta)$, formally defined as

$$\mathcal{R}^2_\eta = \left\{(p_{\text{C}}, p_\perp, p_{\text{I}}) \in \Delta_2 \mid p_{\text{C}} > \frac{\eta-\epsilon-\cos^2(\frac{\pi}{8})-\mathfrak{b}_\eta}{1-(\eta-\epsilon)} p_\perp + \cos^2(\frac{\pi}{8})\right\} \wedge p_{\text{I}} < \frac{\mathfrak{b}_\eta - \sin^2(\frac{\pi}{8})}{1-(\eta-\epsilon)} p_\perp + \sin^2(\frac{\pi}{8})\Big\}$$

By an analogous convexity argument with the point $\mathbf{q}_{\text{TFKW}}$, we have that $\mathcal{R}^2_\eta \cap \mathcal{A} = \varnothing$.
Notice that $\mathcal{R}_\eta = \mathcal{R}^0_\eta \cup \mathcal{R}^1_\eta \cup \mathcal{R}^2_\eta$, and therefore, $\mathcal{R}_\eta \cap \mathcal{A} = \varnothing \ \forall \eta \in (0.53, 1]$. As a consequence, $\mathcal{R} \cap \mathcal{A} = \left(\cup_{\eta\in(0.53,1]} \mathcal{R}_\eta\right) \cap \mathcal{A} = \varnothing$ and therefore, $\mathcal{A} \subset \mathcal{R}^c$. □

4.2.13. Theorem. *Let $\varepsilon_h > 0$, and η and p_{err} be such that $\alpha^{ent} > 0$. Then, any sequential strategy that attackers who pre-share $q \leq n/2 - 5$ qubits to break $\text{QPV}^{\eta,f}_{\text{BB84}}$ is such that $\mathbb{E}[\Gamma^{ent,att}_r] \leq 0$ and, moreover, the probability that they are accepted in the $\mathsf{T}^{rf-\text{BB84}}_{\varepsilon_h}$ test is exponentially small:*

$$\mathbb{P}[\Gamma^{ent,att}_r \geq r(\alpha^{ent} - \delta)] \leq e^{-r(\alpha^{ent}-\delta)^2/2}. \tag{4.34}$$

Theorem 4.2.13 shows that there is a way (statistical test) to distinguish an honest prover from attackers with exponentially high probability, i.e. that after r rounds the attackers will be *caught*. The values for which $\alpha^{ent} > 0$ correspond to the points below the straight line in Figure 3.4—the above $\alpha^{ent} - \delta > 0$ corresponds to a shift, where δ can be made small by increasing the number of repetitions.

Proof:
Let $\mathbf{p}_1 = (959/1000, 0, 41/1000)$ and $\mathbf{p}_2 = (27/50, 23/50, 0)$. The line segment given by $\mathbf{p}_1$ and $\mathbf{p}_2$ is a subset of $\mathcal{R}$ and it can be described as the intersection of Δ_2 and the plane $\gamma_{\mathrm{C}} p_{\mathrm{C}} - \gamma_{\perp} p \gamma_{\perp} - \gamma_{\mathrm{I}} p_{\mathrm{I}} = 0$, with the normal vector $\boldsymbol{\gamma} = (\gamma_{\mathrm{C}}, \gamma_{\perp}, \gamma_{\mathrm{I}})$, where $\gamma_{\mathrm{C}} = \frac{943}{\sqrt{488625947}} \simeq 0.04266$, $\gamma_{\perp} = \frac{1107}{\sqrt{488625947}} \simeq 0.050079$ and $\gamma_{\mathrm{C}} = \frac{22057}{\sqrt{488625947}} \simeq 0.99783$. Consider the follow non-empty partition of the simplex Δ_2:

$$\Delta_2^{+} \coloneqq \Delta_2 \cap \{\mathbf{p} \in \Delta_2 \mid \mathbf{p} \cdot \boldsymbol{\gamma} > 0\}, \quad \text{and} \quad \Delta_2^{-} \coloneqq \Delta_2 \cap \{\mathbf{p} \in \Delta_2 \mid \mathbf{p} \cdot \boldsymbol{\gamma} \leq 0\}, \tag{4.35}$$

which is such that $\Delta_2 = \Delta_2^{+} \dot{\bigcup} \Delta_2^{-}$. In particular, $\Delta_2^{+} \subset \mathcal{R}$ and $\mathcal{A} \subset \Delta_2^{-}$. Then we have that for all $\mathbf{q} \in \mathcal{A}$,

$$q_{\mathrm{C}} \gamma_{\mathrm{C}} - q_{\perp} \gamma_{\perp} - q_{\mathrm{I}} \gamma_{\mathrm{I}} \leq 0. \tag{4.36}$$

The above amount corresponds to the expected value of T^{ent} for a strategy $\mathbf{q} \in \mathcal{A}$, and thus we have that for all rounds i, the expected value of the attackers (att) is such that

$$\mathbb{E}_{att}[T_i^{ent}] \leq 0. \tag{4.37}$$

Define $\Gamma_0^{ent,att} = 0$. The process $\Gamma = (\Gamma_r^{ent,att} : r \geq 0)$ is a supermartingale relative to the filtration $\mathcal{F}_r$, where $\mathcal{F}_r = \sigma(T_1^{ent}, ..., T_r^{ent})$, and σ denotes the σ-algebra. In fact,

$$\mathbb{E}[\Gamma_r^{att} \mid \mathcal{F}_{r-1}] = \mathbb{E}[T_r^{ent} \mid \mathcal{F}_{r-1}] + \mathbb{E}[\Gamma_{r-1}^{att} \mid \mathcal{F}_{r-1}] \leq \Gamma_{r-1}^{att}, \tag{4.38}$$

which is the definition of a supermartingale. The first equality is due to the linearity of the conditional expectation and the inequality is due to the fact that $\mathbb{E}[T_r^{ent} \mid \mathcal{F}_{r-1}]$ is independent of $\mathcal{F}_{r-1}$ and thus $\mathbb{E}[T_r^{ent} \mid \mathcal{F}_{r-1}] = \mathbb{E}_{att}[T_r^{ent}] \leq 0$ and Γ_{r-1}^{att} is $\mathcal{F}_{r-1}$-measurable.

An immediate application of Azuma's inequality [Azu67] leads to (4.34).
The proof of Theorem 3.2.11 is analogous to the above case considering the segment line given by the two points $\mathbf{q}_{\mathrm{TKFW}} = (\cos^2 \frac{\pi}{8}, 0, \sin^2 \frac{\pi}{8}, 0)$ and $\mathbf{q}_{guess} = (\frac{1}{2}, \frac{1}{2}, 0, 0)$ and the corresponding partition is such that $\Delta_2^{-} = \mathcal{A}$ and $\Delta_2^{+} = \Delta_2 \setminus \mathcal{A}$. □

4.3 The $\mathrm{QPV}^{\eta,f}_{k_{\theta\varphi}}$ protocol

In Section 4.2 we have shown that $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ is secure against entangled attackers if they hold a bounded number of qubits, but it is currently non-implementable experimentally for relatively long distances due to the fact that it is not secure for $\eta \leq 1/2$. On the other hand, in Section 3.3 we have shown that extending the $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ protocol to k bases allows for more resistance to photon loss. In this section, we use the results from Section 3.3 to prove Lemma 4.3.1. This lemma will form the key tool to re-apply the analysis in [BCS22] to our case, and as a consequence we will show that the $\mathrm{QPV}^{\eta,f}_{k_{\theta\varphi}}$ protocol is secure against

entangled attackers, and more loss-tolerant than $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$. The results in this section are proven for arbitrary k, however they are based on solving the SDP described in (3.48), which needs k to be fixed. Here, we obtain numerical results for the two particular cases $k_{\theta\varphi} = (3,2,2)$ and $k_{\theta\varphi} = (5,3,2)$, but to obtain the results for any $k_{\theta\varphi}$ that would potentially be applied experimentally, one just needs to solve (3.48), and the corresponding relaxation, see below. Moreover, here we solve the semidefinite programs for a complete range of p_{err}, thereby obtaining an exhaustive characterization for the fixed $k_{\theta\varphi}$, but for an experimental implementation it would just be needed to solve the SDPs for the ranges that the experimental set-up requires.

For $n \in \mathbb{N}$, consider a $2n$-bit function $f : \{0,1\}^n \times \{0,1\}^n \to [k]$. *One round of the $k_{\theta\varphi}$-basis lossy-function protocol*, denoted by $\mathrm{QPV}_{k_{\theta\varphi}}^{\eta,f}$, is described as in Definition 4.2.1 changing the range of f. The corresponding general attack is described as in the attack described for $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$, extended by changing the range of the function f, and similarly for the *q-qubit strategy*.

4.3.1 Security of $\mathrm{QPV}_{k_{\theta\varphi}}^{\eta,f}$

With the same reasoning as in Section 4.2, from (3.48) and its corresponding relaxation given by $\langle A_a^z B_b^z \rangle \leq \epsilon$, for all $a \neq b$, we have that there exists functions $w_{k_{\theta\varphi}}(\eta)$ and $\tilde{w}_{k_{\theta\varphi}}^{\epsilon}(\eta)$ such that, for all states $|\psi\rangle$, regardless of their dimension,

$$\frac{1}{k} \sum_{z \in [k]} p_{\psi}^{z,\eta} \leq w_{k_{\theta\varphi}}(\eta), \tag{4.39}$$

and

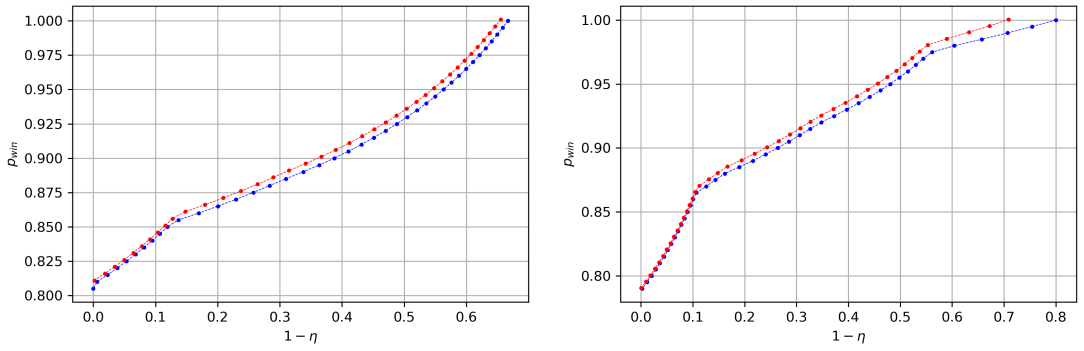
$$\frac{1}{k} \sum_{z \in [k]} \tilde{p}_{\psi}^{z,\eta,\epsilon} \leq \tilde{w}_{k_{\theta\varphi}}^{\epsilon}(\eta), \tag{4.40}$$

that are such that $w_{k_{\theta\varphi}}(\eta) \leq \tilde{w}_{k_{\theta\varphi}}^{\epsilon}(\eta)$. The probabilities $p_{\psi}^{z,\eta}$ and $\tilde{p}_{\psi}^{z,\eta,\epsilon}$ are as in (4.11) and (4.13), respectively, with $z \in [k]$. See Figure 4.5 for a numerical approximation of the functions $w_{k_{\theta\varphi}}(\eta)$ and $\tilde{w}_{k_{\theta\varphi}}^{\epsilon}(\eta)$ for different $k_{\theta\varphi}$, see [EFS] for the code.

Now, we show a lemma that formalizes the idea that if a set of k quantum states can be used to be correct with high probability in an attack of the protocol, then, their average distance is lower bounded by a certain amount. This has the interpretation that these states cannot all be simultaneously arbitrarily close. This means that exists an ε_0 such that for all $\varepsilon \leq \varepsilon_0$, $\bigcap_{z \in [k]} \mathcal{S}_z^{\varepsilon} = \varnothing$, where $\mathcal{S}_z^{\varepsilon}$ is defined as in Definition 4.2.4 with $z \in [k]$.

4.3.1. Lemma. *Let $|\psi_k\rangle$ be such that $p_{\psi_z}^{z,\eta} \geq \tilde{w}_{k_{\theta\varphi}}^{\epsilon}(\eta) + \Delta$, for all $z \in [k]$, for some $\Delta > 0$, which implies that $|\psi_z\rangle \in \mathcal{S}_z^{\varepsilon}$, for $\varepsilon = 1 - (\tilde{w}^{\epsilon}(\eta) + \Delta)$. Then, for all $z' \in [k]$*

$$\mathop{\mathbb{E}}_{z \in [k]} [\mathcal{D}(|\psi_{z'}\rangle, |\psi_z\rangle)] \geq \frac{\eta\Delta}{2}. \tag{4.41}$$



(a) (b)

Figure 4.5: Upper bounds of the winning probability given by (3.48) (blue dots), corresponding to a numerical representation of the function $w_{k_{\theta\varphi}}(\eta)$. Red dots correspond to a numerical representation of the function $\tilde{w}^{\epsilon}_{k_{\theta\varphi}}(\eta)$, which is obtained by adding $\epsilon = 0.001$ to the relaxation of (3.48) where the attackers are allowed to make errors with probability ϵ, for (a) $k_{\theta\varphi} = (3,2,2)$, and (b) $k_{\theta\varphi} = (5,3,2)$. The blue dots in (a) are obtained by the level 2 of the NPA hierarchy, and the rest of the values, via the level '1+AB'. The continuous interpolation between values is meant for a better viewing of the plot.

Proof:
Let $\epsilon_{z'z} = \mathcal{D}(|\psi_{z'}\rangle, |\psi_z\rangle)$ and let $\epsilon = \max_{zz'} \epsilon_{zz'}$. From an analogous application of equation (4.19), we have that for all $z, z' \in [k]$,

$$p^{z,\eta}_{\psi_z} \leq \frac{2}{\eta}\epsilon_{zz'} + \tilde{p}^{z,\eta,\epsilon_{zz'}}_{\psi_{z'}} \leq \frac{2}{\eta}\epsilon_{zz'} + \tilde{p}^{z,\eta,\epsilon}_{\psi_{z'}}, \tag{4.42}$$

where in the second inequality we used that replacing $\epsilon_{zz'}$ by ϵ is a relaxation of the restrictions of the maximization (4.13). Fixing z' and summing over z,

$$\sum_{z\in[k]} p^{z,\eta}_{\psi_z} \leq \frac{2}{\eta}\sum_{z\in[k]} \epsilon_{zz'} + \sum_{z\in[k]} \tilde{p}^{z,\eta,\epsilon}_{\psi_{z'}}. \tag{4.43}$$

By hypothesis, each term in the left-hand side is lower bounded by $\tilde{w}^{\epsilon}_{k_{\theta\varphi}}(\eta) + \Delta$. This, together with (4.40), lead to (4.41). □

Since Lemma 4.3.1 implies that if a set of k states 'performs well' on their respective inputs, their average distance with respect to an arbitrary state is at least a certain amount, meaning that there are at least two states that differ by such an amount, it has as consequence that Alice and Bob in some sense have to decide (at least one) strategy not to follow before they communicate. Consequently, if the dimension of the state they share is small enough, a classical

description of the first part of their strategy yields a compression of f. The notion of the following definition captures this classical compression.

4.3.2. Definition. *Let $q, k, n \in \mathbb{N}$, $\varepsilon > 0$. Then,*

$$g_{k_{\theta\varphi}} : \{0,1\}^{3\kappa} \to 2^{[k]} \setminus [k] \tag{4.44}$$

is an (ε, q)-classical rounding restriction of size κ is for all $f : \{0,1\}^{2n}$, for all states $|\varphi\rangle$ on $2q+1$ qubits, for all $l \in \{1, ..., 2^{2n}\}$ and for all (ε, l)-perfect q-qubit strategies for $\mathrm{QPV}^{\eta,f}_{k_{\theta\varphi}}$, there are functions $f_A : \{0,1\}^n \to \{0,1\}^k$, $f_B : \{0,1\}^n \to \{0,1\}^k$ and $\mu \in \{0,1\}^k$ such that $f(x,y) \in g(f_A(x), f_B(y), \mu)$.

4.3.3. Lemma. *[BCS22] Let $|x\rangle, |y\rangle \in \mathbb{C}^d$, for $d \in \mathbb{N}$, be two unit vectors. Then, $\mathcal{D}(|x\rangle, |y\rangle) \leq \||x\rangle - |y\rangle\|_2$.*

4.3.4. Lemma. *Let $\Delta > 0$, and let $0 \leq \varepsilon \leq \varepsilon_0$, where ε_0 is such that $|\psi_z\rangle \in \mathcal{S}^\varepsilon_z$, for $z \in [k]$, implies $\mathop{\mathbb{E}}_{z\in[k]}[\mathcal{D}(|\psi_{z'}\rangle, |\psi_z\rangle)] \geq \frac{\eta\Delta}{2}$, for every $z' \in [k]$. Then there exists an (ε, q)-classical rounding restriction of size $\kappa = \log(\lceil \frac{4}{2^{\frac{1}{3}}(\eta\Delta+4)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$.*

Proof:
We follow the same techniques as in the proof of Lemma 3.12 in [BCS22]. Let $\delta < \frac{\sqrt[3]{\eta\Delta+4}}{2^{2/3}} - 1$, and consider δ-nets $\mathcal{N}_S$, $\mathcal{N}_A$ and $\mathcal{N}_B$, where the first is for the set of pure states on $2q+1$ qubits in Euclidean norm and the other nets are for the set of unitaries in dimension 2^q in operator norm. They are such that $|\mathcal{N}_S|$, $|\mathcal{N}_A|$, $|\mathcal{N}_B| \leq 2^k$.

Let $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A^{xy}_a\}_a, \{B^{xy}_b\}_b\}_{x,y}$ be an $(\varepsilon, \ell)-$ strategy for $\mathrm{QPV}^{\eta,f}_{k_{\theta\varphi}}$, we define (i) μ as the element in $\mathcal{N}_S$ that is closest to $|\varphi\rangle$ in Euclidean norm, and denote by $|\varphi_\delta\rangle$ the state described by μ, (ii) $f_A(x)$ as the element in $\mathcal{N}_A$ that is closest to U^x in operator norm, and denote by U^x_δ the unitary described by $f_A(x)$, and (iii) $f_B(y)$ as the element in $\mathcal{N}_B$ that is closest to V^y in operator norm, and denote by V^y_δ the unitary described by $f_A(y)$. If the closest element is not unique, make an arbitrary choice. Moreover, we define a function g as $g(x,y,\mu) := \{z \mid U^x_\delta \otimes V^y_\delta |\varphi_\delta\rangle \in \mathcal{S}^\varepsilon_z\}$. We are going to show that g is an (ε, q)-classical rounding restriction.

Let z and z' be such that $\mathcal{D}(|\psi_z\rangle, |\psi_{z'}\rangle) \geq \eta\Delta/2$. Assume $U^x \otimes U^y|\varphi\rangle \in \mathcal{S}^\varepsilon_z$. Then,

$$\begin{aligned}
\mathcal{D}(U^x \otimes V^y|\psi\rangle, U^x_\delta \otimes V^y_\delta|\varphi_\delta\rangle) &\leq \|U^x \otimes V^y|\varphi\rangle - U^x_\delta \otimes V^y_\delta|\varphi\rangle\|_2 \\
&\leq \|(U^x_\delta + U^x - U^x_\delta) \otimes (V^y_\delta + V^y - V^y_\delta)(|\varphi_\delta\rangle + |\varphi\rangle - |\varphi_\delta\rangle) - U^x_\delta \otimes V^y_\delta|\varphi\rangle\|_2 \\
&\leq 3\delta + 3\delta^2 + \delta^3 < \frac{\eta\Delta/2}{2},
\end{aligned} \tag{4.45}$$

where in the first inequality, we used Lemma 4.3.3, in the second, we used the triangle inequality and the inequality $\|X \otimes Y|x\rangle\|_2 \leq \|X\|_\infty \|Y\|_\infty \||x\rangle\|_2$, together

with $\|U^x - U^x_\delta\|_\infty, \|V^y - V^y_\delta\|_\infty, \||\varphi\rangle - |\varphi_\delta\rangle\| \leq \delta$, and, finally, in the last inequality we used that $\delta < \frac{\sqrt[3]{\eta\Delta+4}}{2^{2/3}} - 1$. Thus, $U^x_\delta \otimes V^y_\delta |\varphi\rangle$ is closer to $\mathcal{S}^\varepsilon_z$ than to $\mathcal{S}^\varepsilon_{z'}$.
Consider an (ε, l)-perfect strategy for $\mathrm{QPV}^{\eta,f}_{k_{\theta\varphi}}$ and let (x,y) be such that the attackers are caught with probability at most ε and such that $f(x,y) = z$. In particular, we have that $U^x \otimes V^y|\psi\rangle \in \mathcal{S}^\varepsilon_z$, and because of (4.45), $f(x,y) \in g(f_A(x), f_B(y), \mu)$. Since there are at least l pairs (x,y) satisfying this condition, $f(x,y) \in g(f_A(x), f_B(y), \mu)$ holds on at least l pairs (x,y) and therefore g is an (ε, q)-classical rounding restriction. The size of κ follows from Lemma 4.2.8. □

Given $k_{\theta\varphi}$, we denote by $\eta_{k_{\theta\varphi}}$ the minimum η such that $\tilde{w}^\epsilon_{k_{\theta\varphi}}(\eta) + \Delta \leq 1$, e.g. for $k_{\theta\varphi} = (2,2,1)$, i.e. $\mathrm{QPV}^\eta_{\mathrm{BB84}}$, that corresponds to 0.53. From (4.40) and picking $\Delta = 0.009$, $\eta_{k_{\theta\varphi}} = 0.36$ for $k_{\theta\varphi} = (3,2,2)$ and $\eta_{k_{\theta\varphi}} = 0.34$ for $k_{\theta\varphi} = (5,3,2)$ (by picking a smaller Δ, the latter gets closer to 0.2).

4.3.5. Lemma. *Let* $\Delta = 0.009$, $\eta \in (\eta_{k_{\theta\varphi}}, 1]$, $\varepsilon \in [0,1]$ n, κ, $q \in \mathbb{N}$, $n \geq 10$. *Moreover, fix an* (ε, q)*-classical rounding* g *of size* κ *with* $\kappa \leq \log(\lceil \frac{4}{2^{\frac{1}{3}}(\eta\Delta+4)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$. *Let* $q \leq \frac{1}{2}n - 5$. *Then, a uniformly random* $f : \{0,1\}^{2n} \to \{0,1\}$ *fulfills the following with probability at least* $1 - 2^{-2^n}$*: For any* $f_A : \{0,1\}^n \to \{0,1\}^\kappa$, $f_B : \{0,1\}^n \to \{0,1\}^\kappa$, $\mu \in \{0,1\}^\kappa$, $f(x,y) \in g(f_A(x), f_B(y), \mu)$ *holds on less than* $1 - \beta_{k_{\theta\varphi}}$ *of all pairs* (x,y)*, for certain* $\beta_{k_{\theta\varphi}} > 0$ *(*$\beta_{k_{\theta\varphi}} = 0.15$ *for* $k_{\theta\varphi} = (3,2,2)$ *and* $\beta_{k_{\theta\varphi}} = 0.13$ *for* $k_{\theta\varphi} = (5,3,2)$ *).*

Proof:
For simplicity, denote $\beta_{k_{\theta\varphi}}$ by β. We want to estimate the probability that for a randomly chosen f, we can find f_A and f_B such that the corresponding function g is such that $\mathbb{P}_{x,y}[f(x,y) \in g_{k_{\theta\varphi}(f_A(x), f_B(y), \mu)}] \geq (1-\beta)$.

$$\begin{aligned}
&\mathbb{P}[f : \exists f_A, f_B, \mu \text{ s.t. } \mathbb{P}[x,y : f(x,y) \in g_{k_{\theta\varphi}}(f_A(x), f_B(y), \mu)] \geq (1-\beta)] \\
&= \frac{|\{f : \exists f_A, f_B, \mu \text{s.t. } \mathbb{P}[x,y : f(x,y) \in g_{k_{\theta\varphi}}(f_A(x), f_B(y), \mu)] \geq (1-\beta)\}|}{|\{f : \{0,1\}^{2n} \to [k]\}|} \\
&\leq \frac{|\{f : \exists f_A, f_B, \mu \text{ s.t. } \forall x,y, f(x,y) \in g_{k_{\theta\varphi}}(f_A(x), f_B(y), \mu)\}|}{k^{2^{2n}}} \sum_{i=0}^{\beta 2^{2n}} \binom{2^{2n}}{i} (k-1)^i \\
&\leq \frac{1}{k^{2^{2n}}} 2^{(2^{n+1}+1)\kappa} (k-1)^{2^{2n}} (k-1)^{\beta 2^{2n}} 2^{h_b(\beta) 2^{2n}} \\
&= 2^{(h_b(\beta) - \log k + (1+\beta)\log k - 1)2^{2n} + (2^{n+1}+1)\kappa}.
\end{aligned} \tag{4.46}$$

Where in the first equality we used that f is chosen uniformly at random, in the second step we estimate the numerator by considering a ball in Hamming distance around every function g that cab be expressed suitable by f_A, f_B, μ, and

in the third step we bounded $(k-1)^i$ in the sum by $(k-1)^{\beta 2^{2n}}$ and we used the inequality $\sum_{l=0}^{\beta n}\binom{n}{n} \leq 2^{nh_b(\beta)}$ for $n \in \mathbb{N}$ and $\beta \in (0, 1/2)$ [MS77]. For $k_{\theta\varphi} = (3,2,2)$ and $k_{\theta\varphi} = (5,3,2)$, $\Delta = 0.009$, $\kappa \leq \log(\lceil \frac{4}{2^{\frac{1}{3}}(\eta\Delta+4)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$ for $\eta \in (\eta_{k_{\theta\varphi}}, 1]$ and $q \leq n/2 - 5$, (4.46) is strictly upper bounded by 2^{-2^n}. □

Lemma 4.3.5 has the same interpretation as Lemma 4.3.5. This leads to the next theorem, which provides a lower bound of the probability that attackers pre-sharing entanglement are caught in a round of the $\text{QPV}_{k_{\theta\varphi}}^{\eta,f}$ protocol.

4.3.6. Theorem. *Consider the most general attack a round of the* $\text{QPV}_{k_{\theta\varphi}}^{\eta,f}$ *protocol for a transmission rate* $\eta \in (\eta_{k_{\theta\varphi}}, 1]$ *and prover's error rate* p_{err}. *Let* $\Delta = 0.009$. *If the attackers respond with probability* η *and control at most* q *qubits at the beginning of the protocol, and* q *is such that*

$$q \leq \frac{n}{2} - 5, \tag{4.47}$$

then,

$$\Pr[\text{V}_{\text{AB}} = \text{C}] \leq \eta(1 - \beta_{k_{\theta\varphi}}[1 - (\tilde{w}^{\epsilon}(\eta) + \Delta)]). \tag{4.48}$$

We see then that if $p_{err} < \beta_{k_{\theta\varphi}}[1-(\tilde{w}^{\epsilon}_{k_{\theta\varphi}}(\eta)+\Delta)]$ the $\text{QPV}_{k_{\theta\varphi}}^{\eta,f}$ protocol is secure even in the presence of photon loss (more loss-tolerant than the $\text{QPV}_{\text{BB84}}^{\eta,f}$ protocol) and attackers who pre-share entanglement.

Proof:

Let $0 \leq \varepsilon \leq \varepsilon_0 = 1 - (\tilde{w}^{\epsilon}_{k_{\theta\varphi}}(\eta) + \Delta)$. By Lemma 4.3.4 there exists $g_{k_{\theta\varphi}}$ (ε, q)-classical rounding of size $\kappa \leq \log(\lceil \frac{4}{2^{\frac{1}{3}}(\eta\Delta+4)^{\frac{1}{3}}-2} \rceil) 2^{2q+2}$. Fix $f : \{0,1\}^{2n} \to [k]$ such that $f(x,y) \in g(f_A(x), f_B(y), \mu)$ holds on less than $1 - \beta_{k_{\theta\varphi}}$ of all pairs (x,y), for all f_A, f_B and μ as defined previously. By Lemma 4.3.5, a uniformly random f will have this property with probability at least $1 - 2^{-2^n}$.

On the other hand, assume that there is a $(\varepsilon, (1-\beta_{k_{\theta\varphi}})\cdot 2^{2n})$-perfect q-qubit strategy for $\text{QPV}_{k_{\theta\varphi}}^{\eta,f}$. Then, the corresponding f_A, f_B, μ satisfy $f(x,y) \in g_{k_{\theta\varphi}}(f_A(x), f_B(y), \mu)$ on at least $(1 - \beta_{k_{\theta\varphi}}) \cdot 2^{2n}$ pairs (x,y). This is a contradiction of the choice of f. Therefore, with probability at least $1 - 2^{-2^n}$ the function f is such that there are no $(\varepsilon, (1 - \beta_{k_{\theta\varphi}}) \cdot 2^{2n})$-perfect q-qubit strategies for $\text{QPV}_{k_{\theta\varphi}}^{\eta,f}$. Hence, for every strategy that the attackers can implement, on at least $\beta_{k_{\theta\varphi}}$ of the possible strings (x,y), they will not be correct with probability at least ε. □

The security of the sequential repetition of $\text{QPV}_{k_{\theta\varphi}}^{\eta,f}$ is obtained as in the proof of Theorem 4.2.13 adjusting the parameters accordingly for the particular choice of $k_{\theta\varphi}$.

Chapter 5

A generic framework for loss and constraints

In Chapters 3 and 4, we analyzed quantum correlations in a variation of a class of non-local games called *monogamy-of-entanglement (MoE) games*, adapted to incorporate losses in quantum communication. These games involve two distant parties (Alice and Bob) who prepare a quantum state, send a subsystem to a referee, who then performs a measurement on his register. Previously, we bounded achievable correlations using an ad hoc approach: combining the Navascués–Pironio–Acín (NPA) hierarchy [NPA08], which, via semidefinite programs (SDPs) characterizes correlations achievable by *commuting measurements*—a superset of tensor-product measurements (describing non-local correlations), which coincide with tensor-product measurements in finite dimensions—with additional linear constraints analytically derived for each specific game. While effective, this method requires manual derivation for each game and does not guarantee convergence to the optimal value.

In this chapter, we introduce a more systematic method. We extend the notion of *extended non-local games* [JMRW16], which generalize MoE games, by incorporating experimental constraints such as photon loss and measurement errors. We show that a variation of the hierarchy of SDPs in [JMRW16], which solely requires the game description and its constraints, suffices to obtain upper bounds with guaranteed convergence to the optimal (commuting) value. We demonstrate the effectiveness of our framework by applying it to quantum position verification, recovering and sharpening existing results. For further applications in quantum cryptography, including relativistic bit commitment and quantum key distribution, we refer the reader to [EFS25a].

The results presented in this chapter are based on the following publication:

- *Quantum 9, 1712*, "Lossy-and-Constrained Extended Non-Local Games with Applications to Quantum Cryptography", by Llorenç Escolà-Farràs, and Florian Speelman [EFS25a].

5.1 Introduction

The study of quantum correlations attainable by distant parties, known as non-local correlations, has been a broad and well-studied topic in quantum information theory. They are not only interesting from a fundamental point of view, given that it is well-known that quantum distant parties can attain correlations that classical physics is not able to describe [Bel64], but also lead to many applications such as secure key distribution [ABG+07], certified randomness [PAM+10], reduced communication complexity [BCMdW10], self-testing [MY04, ŠB20], and computation [AB09].

Non-local correlations are often studied in the literature as non-local games, which provide an operational framework for understanding them. Usually, a classical referee sends classical questions to the two distant parties, namely Alice and Bob, who have to respond classical answers. The game is defined according to a predicate that accepts the answers as correct if they fulfill a previously agreed relation with the questions. One of the most well-known examples in the literature is given by the CHSH game [CHSH69].

The usage of semidefinite programming (SDP) techniques to bound correlations of non-local games was initiated by Cleve, Høyer, Toner and Watrous [CHTW04], Wehner [Weh06], and Liang and Doherty [LD07]. Later on, Navascués, Pironio and Acín introduced an infinite hierarchy of conditions, the so-called NPA hierarchy, necessarily satisfied by any set of quantum correlations, each of them testable with SDPs [NPA07], with the subsequent result showing that this hierarchy is complete [NPA08].

Non-local correlations have also been investigated beyond the classical question-and-answer scenario. For example, in a quantum XOR game [RV12], a quantum referee sends quantum questions to Alice and Bob, who respond with classical answers. Another example is given by rank-one quantum games [CJPPG15], where both questions and answers are quantum. In this work, we consider a slightly different scenario. In terms of games, the referee is quantum and performs a measurement on their local register of a tripartite system shared together with the two collaborative parties Alice and Bob. These types of games are known in the literature as extended non-local games, introduced by [JMRW16]. They are a generalization of monogamy-of-entanglement games [TFKW13], where, as described in Chapter 3, the referee, Alice and Bob pre-share a joint quantum state, the referee performs a local measurement on their local register, chosen from a predefined set of measurements, then, the referee announces the chosen measurement, and the task of Alice and Bob is to guess the outcome. These types of games have applications to quantum cryptography tasks, such as quantum position verification and device-independent quantum key distribution [TFKW13], and have been studied in the context of quantum steering [RW17]. Using similar ideas as in [NPA08], it was shown [JMRW16] that there exists a hierarchy of SDPs that bound the optimal winning probability of any given extended non-local

game, and it is such that converges to its optimal (commuting) value.

When analyzing the applications of such games, for example in quantum communication tasks, one has to take into account experimental parameters such as errors and loss of the quantum information, and, as shown in Chapter 3, treating these two separately can give significant improvements in the analysis, where a loss-tolerance of up to 50% is shown for a given protocol with only around 15% error-tolerance [TFKW13], which is impossible if naively treating loss as error. Moreover, besides errors and loss, when executing a protocol it can be the case that certain answers are expected to be observed with a given frequency, for example: a certain number of correct answers; some wrong answers (caused e.g. by errors); some 'empty' answers, if the quantum information got lost when transmitted. Additionally, in some protocols there are answer combinations that are simply inconsistent with the setting, and are never expected to be observed: including such constraints in the analysis of extended non-local games could enable improved bounds in practical applications.

We introduce a modification of extended non-local games, which we call *lossy-and-constrained* extended non-local games, that takes into account errors, loss and the fact that certain answers are expected to be observed with a given frequency. These games are inspired by practical considerations, describing scenarios where honest parties receive quantum states over a lossy channel, and we aim to prevent security issues that can occur because of such transmission loss. We show that similar results as in [JMRW16] can be applied to the *lossy-and-constrained* version, and that there exists a hierarchy of SDPs converging to the optimal (commuting) value that can be attained by the quantum parties Alice and Bob.

We consider different monogamy-of-entanglement and extended non-local games, and we analyze them in their lossy-and-constrained version.

We compute the corresponding semidefinite programs to show a way to verify some previously known results by solving only an SDP. By solely computing the corresponding SDPs, we show a way to verify some previously known results. Moreover, we find new tighter and new tight results for those games. It is worth highlighting that for most of the games that we analyze with loss or constraints, we obtain tight values by using the first level of the hierarchy—showing that the resulting SDPs are numerically solvable in practice and going to higher levels is not required. We created Python codes to compute these values via SDP [EF], using *cvxpy* [AB09]. These programs can be modified and adapted to analyze other games.

Finally, we study applications to quantum position verification (QPV) in the presence of photon loss, showing that (lossy-and-constrained) non-local games can be used to prove security for certain protocols in a simpler way, with a method that can be executed using only the description of the game. Using our analysis, we provide tighter security bounds. For the QPV_{BB84} protocol with loss, we obtain, in an easier way compared to Chapter 3, Theorem 3.2.10, where

it was necessary to prove a relation between certain operator norms and error and then use it in the NPA hierarchy to obtain the values. The advantage is that by considering the corresponding game with loss and constraints, it is enough to have the description to compute the SDP providing the optimal values. We improve the bounds found in Chapter 3 for an extension of $\mathrm{QPV}_{\mathrm{BB84}}$, and we show that they are tight, and we also apply our results to show security of the 2-fold parallel repetition of $\mathrm{QPV}_{\mathrm{BB84}}$ with loss.

5.2 Lossy-and-constrained extended non-local games

Following [JMRW16], we describe extended non-local games. Let $\mathcal{Z}$, $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{V}$, $\mathcal{A}$ and $\mathcal{B}$ be finite non-empty alphabets, let q be a probability distribution over $\mathcal{Z}\times\mathcal{X}\times\mathcal{Y}$, let V_v^z be a square Hermitian matrix of dimension $d\in\mathbb{N}$ for all $(z,v)\in\mathcal{Z}\times\mathcal{V}$ and let $\mathcal{M}:=\{V_v^z\}_{z,v}$. Three parties will play a role in the extended non-local games: a referee, Alice and Bob, whose associated Hilbert spaces will be denoted by $\mathcal{H}_R,\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

5.2.1. Definition. *An* extended non-local game $\mathcal{G}$*, played by a referee* R *and two collaborative parties Alice (*A*) and Bob (*B*), denoted by the tuple*

$$\mathcal{G}=(q,\mathcal{M},W), \tag{5.1}$$

where $W=\{(z,x,y,v,a,b)\mid pred(v,a,b|z,x,y)=1\}$ *(winning set), for a certain predicate function* $pred(v,a,b|z,x,y)\in\{0,1\}$*, is described as follows:*

1. *Alice and Bob prepare a tripartite state* ρ_{RAB} *where the dimension of the register* R *is* d*, i.e. the reduced state* $\rho_R\in\mathcal{S}(\mathcal{H}_R)$*, for* $\mathcal{H}_R\cong\mathbb{C}^d$*.*

2. *They send the register* R *of the tripartite state to the referee. The two parties are no longer allowed to communicate.*

3. *The referee sends questions* $x\in\mathcal{X}$ *and* $y\in\mathcal{Y}$ *to Alice and Bob and picks* $z\in\mathcal{Z}$ *according to the probability distribution* $q(z,x,y)$*. Then, Alice and Bob have to answer* $a\in\mathcal{A}$ *and* $b\in\mathcal{B}$*, respectively. Denote by* $\rho^{x,y}_{R_{a,b}}\in\mathcal{S}(\mathcal{H}_R)$ *the resulting quantum state held by* R *after Alice and Bob send* a *and* b*. The average pay-off for the players is given by*

$$\sum_{z,x,y,v,a,b\in W} q(z,x,y)\mathrm{Tr}\Big[V_v^z\rho^{x,y}_{R_{a,b}}\Big]. \tag{5.2}$$

See Figure 5.1 for a schematic representation of an extended non-local game.

5.2.2. Remark. A monogamy-of-entanglement game G, as introduced in Section 3.2.1, is an extended non-local game $\mathcal{G}$ where $x=y=z$, i.e. all the parties get the same question, drawn uniformly at random, and the winning set is given by $W=\{(x,v,a,b)\mid v=a=b\}$, i.e. they have to guess the measurement outcome of the referee, see Figure 3.2 for a visual illustration.

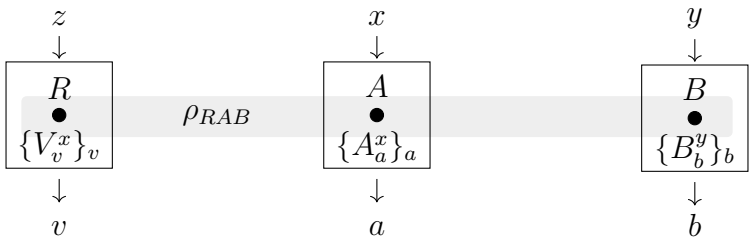


Figure 5.1: Schematic representation of an extended non-local game. The gray-shaded region represents the tripartite quantum state ρ_{RAB} prepared by Alice and Bob and shared amongst the three parties.

In order to play an extended non-local game, the most general thing that Alice and Bob can do using quantum mechanics is to perform POVMs $\{A_a^x\}$ and $\{B_b^y\}$ on their local registers to answer a and b, respectively. Similar as in a monogamy-of-entanglement game (Definition 3.2.4), a *quantum strategy* $\mathbf{S}_Q$ is defined by the tuple $\{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$, and the quantum winning probability of the extended non-local game $\mathcal{G}$ is defined as

$$\omega_Q(\mathcal{G}) \coloneqq \sup \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}\big[(V_v^z \otimes A_a^x \otimes B_b^y)\rho_{RAB}\big], \tag{5.3}$$

where the supremum (sup) is taken over all quantum states ρ_{RAB} and all POVMs $\{A_a^x\}$ and $\{B_b^y\}$ over all possible dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$. All the supremums in this chapter will be taken with respect to the same conditions. A particular case of quantum strategies that will appear in this work are the *unentangled* strategies. These correspond to quantum strategies $\mathbf{S}_Q$ for which Alice and Bob prepare an unentangled initial state, i.e. of the form $\rho_{RAB} = \sum_\lambda p_\lambda \rho_R^\lambda \otimes \rho_A^\lambda \otimes \rho_B^\lambda$, where $p_\lambda \geq 0$ are such that $\sum_\lambda p_\lambda = 1$. Notice that the winning probability of unentangled strategies can be attained by Alice and Bob acting only classically (using shared randomness), since the following holds:

$$\mathrm{Tr}\big[(V_v^z \otimes A_a^x \otimes B_b^y)\rho_{RAB}\big] = \sum_\lambda p_\lambda \mathrm{Tr}\big[V_v^z \rho_R^\lambda\big]\mathrm{Tr}\big[A_a^x \rho_A^\lambda\big]\mathrm{Tr}\big[B_b^y \rho_B^\lambda\big]. \tag{5.4}$$

Therefore, we will refer to unentangled strategies as those where Alice and Bob send a quantum state to the referee but only perform local operations based on shared classical randomness, reducing to $\rho_{RAB} = \rho_R$. Note that, since in this case the winning probability will be given by a convex combination, the optimal values will be obtained by extremal points and thus, by the proper choice of a pure state $|\phi\rangle\langle\phi|_R$, we have that

$$\begin{aligned}\sum_{(z,x,y,v,a,b)\in W} q(z,x,y) \sum_\lambda p_\lambda \mathrm{Tr}\big[V_v^z \rho_R^\lambda\big]\mathrm{Tr}\big[A_a^x \rho_A^\lambda\big]\mathrm{Tr}\big[B_b^y \rho_B^\lambda\big] \\ \leq \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}[V_v^z|\phi\rangle\langle\phi|]p(a|x)p(b|y),\end{aligned}$$

where $p(a|x)$ and $p(b|y)$ are the (classical) probabilities to output a and b, given x and y, respectively. As discussed in Section 3.2.1, for G^{BB84}, it was shown [TFKW13] that $\omega_Q(\mathsf{G}^{BB84}) = \cos^2\left(\frac{\pi}{8}\right)$, which is attained by the unentangled strategy $\{|\phi\rangle\langle\phi|, A_a^x = \delta_{a0},\ B_a^x = \delta_{a0}\}$, where $|\phi\rangle = \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle$.

A broader class of strategies, encompassing quantum strategies as a special case, is given by the so-called *commuting strategies* which consist of POVMs $\{A_a^x\}$ and $\{B_b^y\}$ on Alice's and Bob's joint system $\mathcal{H}_{AB}$ such that $[A_a^x, B_b^y] = 0$, i.e. the POVMs commute, and a joint tripartite state ρ_{RAB}. Here, AB refers to a single composite register on which both measurements act, not two separate subsystems. The respective commuting winning probability of a non-local game $\mathcal{G}$ is defined as

$$\omega_{\text{comm}}(\mathcal{G}) := \sup \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\text{Tr}\left[(V_v^z \otimes A_a^x B_b^y)\rho_{RAB}\right]. \tag{5.5}$$

By extending Alice's and Bob's Hilbert spaces, if necessary, ρ_{RAB} can be taken as a pure state, and $\{A_a^x\}$ and $\{B_b^y\}$ projective measurements. Since the quantum strategies are a subset of the commuting strategies, we have that, for all extended non-local games $\mathcal{G}$,

$$\omega_Q(\mathcal{G}) \leq \omega_{\text{comm}}(\mathcal{G}). \tag{5.6}$$

A particularly interesting case arises when an extended non-local game is sequentially played many times so that one can extract statistics from the answers of the players. Such a case arises, for example, when monogamy-of-entanglement games are used to analyze security of certain quantum protocols [TFKW13], where the two collaborative parties play the role of attackers/dishonest implementers of the protocol who want to emulate the behavior of an honest party towards the referee.

In a realistic implementation of those protocols, the honest party will not perform them with perfect correctness, and one might expect a certain distribution over the possible outcomes. For example, there will be answers that will be wrong with a certain probability due to e.g. experimental measurement errors or noisy quantum channels. However, we can find other types of answers that are wrong and that are simply inconsistent with the behavior of an honest executor of the protocol, for instance if she broadcasts classical information and this information is received differently in different locations. Moreover, in communication tasks, a sizable fraction of qubits get lost and, therefore, we expect a certain ratio of 'empty' answers ($\perp$). Thus, it is natural to ask whether Alice and Bob's winning probability of a certain extended non-local game decreases if they not only have to answer correctly, but they have to emulate the distribution of the other (different) incorrect answers and the transmission rate. In order to analyze these games where Alice and Bob are expected to answer certain answers with a certain probability, we introduce the concept of *lossy-and-constrained* extended non-local games. To clarify these ideas, we now present an example before introducing the formal definitions of constrained and lossy extended non-local games.

5.2.3. Example. Consider the extended non-local game $\mathcal{G}^{BB84}$ (also denoted G^{BB84}), as described in Theorem 3.2.6. Briefly recalling its structure, Alice and Bob send a qubit register to the referee, who measures it in either the computational or Hadamard basis. Their task is to guess the outcome of the referee's measurement. We consider two versions of this game:

1. *Constrained version* (see Section 5.3.1 for further details): This version is motivated by applications to quantum cryptographic protocols, where Alice and Bob model an adversarial implementation attempting to simulate a single honest prover (see Section 5.4). In this context, Alice and Bob are required to coordinate their actions so that they behave as a single entity. A natural constraint to enforce this is to forbid them from providing different answers when they receive the same question. Formally, we impose that for every strategy $\mathbf{S}_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$, the following condition holds:
$$\sum_{x,a,a'\neq b'} q(x)\mathrm{Tr}[(V_a^x \otimes A_{a'}^x \otimes B_{b'}^x)\rho_{RAB}] = 0. \tag{5.7}$$

2. *Lossy version* (previously introduced in Section 3.2.1; see Section 5.3.4 for a generalization and further details): Motivated by losses in quantum communication, assume that Alice and Bob have the option to answer "inconclusive answer" ($\perp$) with probability $1-\eta$. This can be viewed as Alice and Bob claiming at will that the quantum messages have been lost, even if that was not the case. In this scenario, if they have to coordinately mimic a response rate η, this can be done by imposing that for every strategy $\mathbf{S}_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,
$$\sum_x q(x)\mathrm{Tr}[(\mathbb{I}_R \otimes A_\perp^x \otimes B_\perp^y)\rho_{RAB}] = 1-\eta. \tag{5.8}$$

We now formalize these concepts with the following definitions.

5.2.4. Definition. *Let $L \in \mathbb{N}$, for all $\ell \in \{1,\dots,L\}$, let*
$$C = \{\alpha_\ell(v,a,b|z,x,y), c_\ell^0, c_\ell^1\}_{(\ell,z,x,y,v,a,b)}$$
(set of constraints) for $\alpha_\ell : \mathcal{Z}\times\mathcal{X}\times\mathcal{Y}\times\mathcal{V}\times\mathcal{A}\times\mathcal{B} \to \mathbb{R}$ and let $c_\ell^0, c_\ell^1 \in \mathbb{R}$ be such that $c_\ell^0 \le c_\ell^1$. We say that an extended non-local game is constrained*, and we denote it by $\mathcal{G}_C$, if for every strategy $S_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,*
$$c_\ell^0 \le \sum_{z,x,y,v,a,b} \alpha_\ell(v,a,b|z,x,y)\mathrm{Tr}\big[(V_v^z \otimes A_a^x \otimes B_b^y)\rho_{RAB}\big] \le c_\ell^1 \quad \forall \ell \in \{1,\dots,L\}. \tag{5.9}$$

5.2.5. Definition. *We say that an extended non-local game $\mathcal{G}$ is* lossy *with parameter $\eta \in [0,1]$, and we denote it by $\mathcal{G}_\eta$, if the players are allowed to respond $a \in \mathcal{A}\cup\{\perp\}$ and $b \in \mathcal{B}\cup\{\perp\}$ in such a way that for every strategy $S_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$, for $a \in \mathcal{A}\cup\{\perp\}$ and $b \in \mathcal{B}\cup\{\perp\}$,*
$$\sum_{x,y} q(x,y)\mathrm{Tr}[(\mathbb{I}_R \otimes A_\perp^x \otimes B_\perp^y)\rho_{RAB}] = 1-\eta. \tag{5.10}$$

See more examples in Section 5.3. We define a lossy extended non-local game by imposing that the average probability of the answers '$\perp$' is $1-\eta$. We stress that depending on the case to be considered, one can vary the definition and (i) impose that the probability for every input x, y is $1-\eta$, i.e. $\mathrm{Tr}\big[(\mathbb{I}_R \otimes A_\perp^x B_\perp^y)\rho_{RAB}\big] = 1-\eta$ $\forall x, y \in \mathcal{X}\times\mathcal{Y}$ instead of on average, or (ii) impose different loss rates for Alice and Bob, which includes the case where one party answers $\perp$, while the other party does not. Although we stick to the above definition, the results presented in this work still apply if these alternative definitions are considered.

If an extended non-local game $\mathcal{G}$ is both lossy and constrained, we say that it is *lossy-and-constrained*, and we denote it by $\mathcal{G}_{C,\eta}$. The quantum and commuting winning probabilities of $\mathcal{G}_{C,\eta}$ will be denoted by $\omega_Q(\mathcal{G}_{C,\eta})$ and $\omega_{\mathrm{comm}}(\mathcal{G}_{C,\eta})$, respectively.

5.2.1 Convergence of $\omega_{\mathbf{comm}}(\mathcal{G}_{C,\eta})$ via SDPs

In [JMRW16], it was shown that similar ideas as in [NPA08] could be applied to construct a hierarchy of SDPs that upper bound the average winning probability of a given extended non-local game, which converges to its optimal value. Here, we show that when slightly modifying these games, by considering their lossy-and-constrained versions, the results still apply. For completeness, in this section we reproduce the proof in [JMRW16] to show that it applies in our case whenever the games that are considered are modified by their constraints and the loss.

Following Section 3 in [JMRW16], consider the set

$$\Sigma = (\mathcal{X}\times\mathcal{A}) \sqcup (\mathcal{Y}\times\mathcal{B}), \tag{5.11}$$

where $\sqcup$ denoted the disjoint union. The set of strings of length at most k over the alphabet Σ will be denoted by $\Sigma^{\leq k}$, the set of all strings of finite length over Σ will be denoted by Σ^*. Finally, the reverse of a string s will be denoted by s^R, and the empty string will be denoted by ε. For example,

$$\begin{aligned}
&\Sigma^{\leq 0} = \{\varepsilon\},\\
&\Sigma^{\leq 1} = \Sigma^{\leq 0} \cup \{(x,a),(y,b)\}_{(x,a,y,b)\in\mathcal{X}\times\mathcal{A}\times\mathcal{Y}\times\mathcal{B}},\\
&\Sigma^{\leq 2} = \Sigma^{\leq 1} \cup \{(x,a,x',a'),(y,b,y',b'),(x,a,y,b),(y,b,x,a)\}_{(x,x',a,a',y,y',b,b')\in\mathcal{X}^{\times 2}\times\mathcal{A}^{\times 2}\times\mathcal{Y}^{\times 2}\times\mathcal{B}^{\times 2}}.
\end{aligned} \tag{5.12}$$

For later purposes, we will consider the set defined for $k =$ '$1+AB$', which is given by

$$\Sigma^{\leq \text{`}1+AB\text{'}} = \Sigma^{\leq 1} \cup \{(x,a,y,b)\}_{(x,a,y,b)\in\mathcal{X}\times\mathcal{A}\times\mathcal{Y}\times\mathcal{B}} \subset \Sigma^{\leq 2}. \tag{5.13}$$

Consider the equivalence relation $\sim$ on Σ^* defined by:

1. For every $s, t \in \Sigma^*$, and σ in Σ, $s\sigma t \sim s\sigma\sigma t$,
2. For every $s, t \in \Sigma^*$, $\sigma_A \in \mathcal{X}\times\mathcal{A}$, and $\sigma_B \in \mathcal{Y}\times\mathcal{B}$, $s\sigma_A\sigma_B t \sim s\sigma_B\sigma_A t$.

5.2.6. Definition. (Admissible function [JMRW16]). *A function $\phi : \Sigma^* \to \mathbb{C}$ is said to be* admissible *if and only if the following conditions are satisfied:*

1. *For every $s,t \in \Sigma^*$, and every $(x,y) \in \mathcal{X} \times \mathcal{Y}$,*

$$\sum_{a\in\mathcal{A}} \phi(s(x,a)t) = \phi(s,t) = \sum_{b\in\mathcal{B}} \phi(s(y,b)t). \tag{5.14}$$

2. *For every $s,t \in \Sigma^*$, every $(x,y) \in \mathcal{X} \times \mathcal{Y}$, and every $a \neq a' \in \mathcal{A}$, $b \neq b' \in \mathcal{B}$,*

$$\phi(s(x,a)(x,a')t) = 0 = \phi(s(y,b)(y,b')t). \tag{5.15}$$

3. *For every $s,t \in \Sigma^*$ such that $s \sim t$,*

$$\phi(s) = \phi(t). \tag{5.16}$$

A function $\phi : \Sigma^{\leq k} \to \mathbb{C}$ is said to be admissible if and only if (5.14)-(5.16) *hold, given that the arguments' length is such that ϕ is defined.*

We extend the definition of kth order admissible matrices in [JMRW16].

5.2.7. Definition. *For every $1 \leq k \in \mathbb{Z}$, let $M^{(k)}$ be a block matrix of the form*

$$M^{(k)} = \begin{pmatrix} M^{(k)}_{1,1} & \cdots & M^{(k)}_{1,d} \\ \vdots & \ddots & \vdots \\ M^{(k)}_{d,1} & \cdots & M^{(k)}_{d,d} \end{pmatrix} \tag{5.17}$$

where $M^{(k)}_{i,j} : \Sigma^{\leq k} \times \Sigma^{\leq k} \to \mathbb{C}$ for every $i,j \in \{1,\ldots,d\}$. The matrix $M^k(s,t)$ is defined as the matrix with entries $M^{(k)}_{i,j}(s,t)$. We say that $M^{(k)}$ is a lossy-and-extended kth order admissible matrix for $\mathcal{G}_{C,\eta}$ with constraints $C = \{\alpha_\ell(v,a,b|z,x,y), c^0_\ell, c^1_\ell\}_{(\ell,z,x,y,v,a,b)}$, if the following conditions are satisfied:

1. *For every $i,j \in \{1,\ldots,d\}$, there exists an admissible function $\phi_{i,j} : \Sigma^{2k} \to \mathbb{C}$ such that for every $s,t \in \Sigma^{\leq k}$,*

$$M^{(k)}_{i,j}(s,t) = \phi_{i,j}(s^R t). \tag{5.18}$$

2. *The following holds*

$$\mathrm{Tr}\big[M^{(k)}(\varepsilon,\varepsilon)\big] = 1. \tag{5.19}$$

3. *For all $\ell \in \{1,\ldots,L\}$,*

$$c^0_\ell \leq \sum_{z,x,y,v,a,b} \alpha_\ell(v,a,b|z,x,y)\mathrm{Tr}\big[V^z_v M^{(k)}((x,a),(y,b))\big] \leq c^1_\ell, \tag{5.20}$$

and

$$\sum_{x,y} q(x,y)\mathrm{Tr}\big[M^{(k)}((x,\perp),(y,\perp))\big] = 1-\eta. \tag{5.21}$$

4. The matrix $M^{(k)}$ is positive semidefinite.

The definition of a kth order admissible matrix defined in [JMRW16] is the same, except without condition 3.

For a lossy-and-extended kth order admissible matrix for $\mathcal{G}_{C,\eta}$ with constraints $C = \{\alpha_\ell(z,x,y|v,a,b), c_\ell^0, c_\ell^1\}_{(\ell,z,x,y,v,a,b)}$, consider

$$\omega_{admiss}^{(k)}(\mathcal{G}_{C,\eta}) := \sup \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}\big[V_v^z M^{(k)}((x,a),(y,b))\big]. \tag{5.22}$$

Here the supremum is taken over all the strategies that fulfill the constraints given by C and are consistent with η in the sense of (5.10).

5.2.8. Remark. The value $\omega_{admiss}^{(k)}(\mathcal{G}_{C,\eta})$ can be computed by the following SDP:

$$\begin{aligned} &\max \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}\big[V_v^z M^{(k)}((x,a),(y,b))\big] \\ &\text{subject to the linear constraints given by (5.18)-(5.21),} \\ &\text{and } M^{(k)} \succeq 0. \end{aligned} \tag{5.23}$$

Recall that semidefinite programs (SDPs) can be solved in polynomial time to any fixed prescribed precision, see e.g. [LR05, BV04].

5.2.9. Lemma. *For all $k \geq k' \geq 1$,*

$$\omega_{admiss}^{(k)}(\mathcal{G}_{C,\eta}) \geq \omega_{admiss}^{(k')}(\mathcal{G}_{C,\eta}) \geq \omega_{comm}(\mathcal{G}_{C,\eta}). \tag{5.24}$$

Proof:
The function K defined as $K(a,b|x,y) = \mathrm{Tr}_{AB}\big[(\mathbb{I}_R \otimes A_a^x B_b^y)\rho_{RAB}\big]$ is said to be a *commuting measurement assemblage*. Then, (5.3) can be rewritten as

$$\omega_{\mathrm{comm}}(\mathcal{G}) = \sup \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}[V_v^z K(a,b|x,y)]. \tag{5.25}$$

We will show that given a commuting measurement assemblage K, for every integer $k \geq 1$, there exists a lossy-and-extended kth order admissible matrix for $\mathcal{G}_{C,\eta}$ with constraints C.

Consider a commuting strategy $\mathbf{S}_{\mathrm{comm}} = \{|\psi\rangle, A_a^x, B_b^y\}$ for $\mathcal{G}_{C,\eta}$, with $|\psi\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ and A_a^x, B_b^y projective measurements (recall that a strategy can be taken as a pure state and projective measurements). Consider a Schmidt decomposition of $|\psi\rangle$ given by $|\psi\rangle = \sum_{i=1}^d \lambda_i |i\rangle_R |\psi_i\rangle_{AB}$, where $\{|i\rangle\}$ is the standard basis of $\mathcal{H}_R$ and $|\psi_i\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$. Let $|\tilde{\psi}_i\rangle := \lambda_i |\psi_i\rangle$.

Define

$$\Pi_c^z := \begin{cases} A_c^z \text{ if } (c,z) \in \mathcal{A}\times\mathcal{X}, \\ B_c^z \text{ if } (c,z) \in \mathcal{B}\times\mathcal{Y}. \end{cases} \tag{5.26}$$

Consider $M^{(k)}$ defined by

$$M^{(k)}_{i,j}(s,t) = \phi_{i,j}(s^R t) \ \forall i,j \in \{1,\dots,m\}, \tag{5.27}$$

where $\phi_{i,j}$ are defined as

$$\phi_{i,j}((z_1,c_1)\dots(z_l,c_l)) = \langle\tilde{\psi}_j|\Pi^{z_1}_{c_1}\cdots\Pi^{z_l}_{c_l}|\tilde{\psi}_i\rangle. \tag{5.28}$$

The functions $\phi_{i,j}$ fulfill (5.14)-(5.16), and thus they are admissible functions. Notice that

$$\begin{aligned} 1 = \mathrm{Tr}[|\psi\rangle\langle\psi|] = \mathrm{Tr}\left[\sum_{i,j=1}^{d}|i\rangle|\tilde{\psi}_i\rangle\langle\tilde{\psi}_j|\langle j|\right] = \sum_{i,j=1}^{d}\langle i|j\rangle\langle\tilde{\psi}_i|\tilde{\psi}_j\rangle \\ = \sum_{i=1}^{d}\langle\tilde{\psi}_i|\tilde{\psi}_i\rangle = \sum_{i=1}^{d}\phi_{i,i}(\varepsilon,\varepsilon) = \sum_{i=1}^{d}M^{(k)}_{i,i}(\varepsilon,\varepsilon) = \mathrm{Tr}\big[M^k(\varepsilon,\varepsilon)\big], \end{aligned} \tag{5.29}$$

and therefore (5.19) is fulfilled. Moreover, S_{comm} is such that equations (5.20) and (5.21) hold. Finally, since $M^{(k)}$ is a Gram matrix by construction, it is positive semidefinite. Thus, $M^{(k)}$ is a lossy-and-extended kth order admissible matrix for $\mathcal{G}_{C,\eta}$ with constraints C.

It remains to see that $M^{(k)}$ corresponds to K. Since

$$\begin{aligned} K(a,b|x,y) &= \mathrm{Tr}_{AB}\left[(\mathbb{I}_R\otimes A^x_a B^y_b)\sum_{i,j=1}^{d}\lambda_i\lambda_j|j\rangle|\psi_j\rangle\langle\psi_i|\langle i|\right] \\ &= \sum_{k=1}^{\dim\mathcal{H}_A\otimes\mathcal{H}_B}\langle\psi_k|(\mathbb{I}_R\otimes A^x_a B^y_b)\sum_{i,j=1}^{d}\lambda_i\lambda_j|j\rangle|\psi_j\rangle\langle\psi_i|\langle i|)|\psi_k\rangle = \sum_{i,j=1}^{d}|i\rangle\langle j|\lambda_j\langle\psi_j|A^x_a B^y_b|\psi_i\rangle\lambda_i \\ &= \sum_{i,j=1}^{d}|i\rangle\langle j|\langle\tilde{\psi}_j|A^x_a B^y_b|\tilde{\psi}_i\rangle = \sum_{i,j=1}^{d}|i\rangle\langle j|M^{(k)}_{i,j}((x,a),(y,b)), \end{aligned} \tag{5.30}$$

we have that $K(a,b|x,y) = M^{(k)}((x,a),(y,b))$.

Finally, the inequality $\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) \geq \omega^{(k')}_{admiss}$ for $k \geq k'$ comes from the fact that both are obtained with an SDP with the same objective function, but the latter is obtained with more constraints. □

5.2.10. Lemma. *(Lemma 5.2. in [Rus17]). Let $M^{(k)}$ be as in (5.17). Then, for all $i,j \in \{1,\dots,m\}, s,t \in \Sigma^{\leq k}$,*

$$|M^{(k)}_{i,j}(s,t)| \leq 1. \tag{5.31}$$

5.2.11. Lemma. (Banach–Alaoglu theorem for separable spaces [Ala40]). *Let X be a separable normed space. Then, the closed unit ball in X^* is sequentially weak*-compact. That is, for every sequence $\{\mu_n\}_{n\in\mathbb{N}}$ in X^* with $\|\mu_n\| \leq 1 \ \forall n \in \mathbb{N}$, there exists a subsequence $\{\mu_{n_k}\}_{k\in\mathbb{N}}$ such that weak* converges to $\mu \in X^*$: $\lim_{k\to\infty}\mu_{n_k} = \mu$.*

5.2.12. THEOREM. *The following holds*

$$\lim_{k\to\infty} \omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) = \omega_{\text{comm}}(\mathcal{G}_{\mathcal{C},\eta}). \tag{5.32}$$

In summary, for a given game $\mathcal{G}_{\eta,C}$, Lemma 5.2.9 shows us that computing the SDP (5.23) will provide an upper bound to the value $\omega_Q(\mathcal{G}_{\eta,C})$. Moreover, Theorem 5.2.12 tells us that the upper bounds will actually converge to the optimal value of $\omega_{\text{comm}}(\mathcal{G}_{\eta,C})$.

Proof:
From Lemma 5.2.9 we have a non-increasing sequence $\{\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta})\}$ that for every k, $\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) \geq \omega_{\text{comm}}(\mathcal{G}_{\mathcal{C},\eta})$. We will first show the convergence of $\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta})$, and finally that it converges to $\omega_{\text{comm}}(\mathcal{G}_{\mathcal{C},\eta})$.

By Lemma 5.2.10, we have that $|M^{(k)}_{i,j}(s,t)| \leq 1 \ \forall i,j \in \{1,\dots,d\}, s,t \in \Sigma^{\leq k}$. By the Banach-Alaoglu theorem for separable spaces (Lemma 5.2.11), there exists a subsequence $\{M^{(k_l)}_{i,j}(s,t)\}_{l\in\mathbb{N}}$ and $M_{i,j}(s,t)$ such that $\lim_{l\to\infty} = M_{i,j}(s,t)$. Let

$$M = \begin{pmatrix} M_{1,1} & \cdots & M_{1,d} \\ \vdots & \ddots & \vdots \\ M_{d,1} & \cdots & M_{d,d} \end{pmatrix}, \tag{5.33}$$

then, by construction $M^{(k_l)} \to M$. The $M_{i,j}$ are such that

1. For every $i,j \in \{1,\dots,d\}$, there exists an admissible function $\phi_{i,j} : \Sigma^* \to \mathbb{C}$ such that for every $s,t \in \Sigma^{\leq k}$,

$$M^{(k)}_{i,j}(s,t) = \phi_{i,j}(s^R t). \tag{5.34}$$

2. Equation (5.19) holds,

3. For all $\ell \in \{1,\dots,L\}$, equations (5.20), and (5.21) hold.

4. The matrix M is positive semidefinite.

We want to see that M defines a commuting measurement strategy $\mathbf{S}_{\text{comm}} = \{|\psi\rangle, A^x_a, B^y_b\}$. Since M is positive semidefinite, there exists vectors $|\psi_{i,s}\rangle \in \mathcal{H}$ for $i \in \{1,\dots,d\}$ and $s \in \Sigma^*$, for a separable Hilbert space $\mathcal{H}_{AB}$, such that

$$M_{i,j}(s,t) = \langle \psi_{j,s} | \psi_{i,t} \rangle. \tag{5.35}$$

Assume $\mathcal{H}$ is spanned by $\{|\psi_{i,s}\rangle\}$, otherwise let $\mathcal{H} = \text{span}\{|\psi_{i,s}\rangle\}$.

- Consider the state

$$|\psi\rangle = \sum_{j=1}^{d} |j\rangle |\psi_{j,\varepsilon}\rangle \in \mathcal{H}_R \otimes \mathcal{H}, \tag{5.36}$$

which is normalized, since

$$\||\psi\rangle\|^2 = \langle\psi|\psi\rangle = \sum_{j=1}^{d}\langle j|j\rangle\langle\psi_{j,\varepsilon}|\psi_{j,\varepsilon}\rangle = \sum_{j=1}^{d}\langle\psi_{j,\varepsilon}|\psi_{j,\varepsilon}\rangle = \sum_{j=1}^{d} M_{j,j}(\varepsilon,\varepsilon) = 1, \tag{5.37}$$

where we used (5.35) and (5.19).

- For all $(z,c) \in \Sigma$, let Π_c^z be the projection operator onto the following space

$$\text{span}\{|\psi_{j,(z,c)s}\rangle : j \in \{1,\dots,d\}, s \in \Sigma^*\}. \tag{5.38}$$

We want to see that these operators are projective measurements, and that the ones corresponding to Alice commute with the ones corresponding to Bob. Notice that (5.38) is the image of Π_c^z, which we denote by $\text{Im}(\Pi_c^z)$. For all $j \in \{1,\dots,d\}$ and $s \in \Sigma^*$,

$$\begin{aligned}\langle\psi_{j,(z,c)t}|\psi_{j,s}\rangle &= M_{i,j}((z,c)t,s) = \phi_{i,j}(t^R(z,c)s) = \phi_{i,j}(t^R(z,c)(z,c)s)\\ &= M_{i,j}((z,c)t,(z,c)s) = \langle\psi_{j,(z,c)t}|\psi_{i,(z,c)s}\rangle.\end{aligned} \tag{5.39}$$

By linearity, for every $|\varphi_1\rangle \in \text{Im}(\Pi_c^z)$,

$$\langle\varphi_1|\psi_{j,s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle. \tag{5.40}$$

Let $(\Pi_c^z)^\perp$ denote the projection onto $\text{Im}(\Pi_c^z)^\perp$ (orthogonal complement), so that $\Pi_c^z + (\Pi_c^z)^\perp = \mathbb{I}$. Then,

$$\langle\varphi_1|\psi_{j,s}\rangle = \langle\varphi_1|(\Pi_c^z + (\Pi_c^z)^\perp)\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle + \langle\varphi_1|(\Pi_c^z)^\perp|\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle, \tag{5.41}$$

where we used that $(\Pi_c^z)^\perp|\psi_{j,s}\rangle \in \text{Im}(\Pi_c^z)^\perp$ and therefore, $\langle\varphi_1|(\Pi_c^z)^\perp|\psi_{j,s}\rangle = 0$. Using (5.40), we have that

$$\langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle. \tag{5.42}$$

Take an arbitrary $|\varphi\rangle \in \mathcal{H}$, then $|\varphi\rangle = |\varphi_1\rangle + |\varphi_1^\perp\rangle$, for $|\varphi_1\rangle \in \text{Im}(\Pi_c^z)$ and $|\varphi_1^\perp\rangle \in \text{Im}(\Pi_c^z)^\perp$. Then,

$$\langle\varphi|\Pi_c^z|\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle + \langle\varphi_1^\perp|\Pi_c^z|\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle, \tag{5.43}$$

$$\langle\varphi|\psi_{j,(z,c)s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle + \langle\varphi_1^\perp|\psi_{j,(z,c)s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle, \tag{5.44}$$

where we used $\langle\varphi_1^\perp|\Pi_c^z|\psi_{j,s}\rangle = 0$ and $\langle\varphi_1^\perp|\psi_{j,(z,c)s}\rangle = 0$. Then, we have that, because of (5.43), for all $|\varphi\rangle \in \mathcal{H}_{AB}$, and for all $|\psi_{j,s}\rangle$, $\langle\varphi|\Pi_c^z|\psi_{j,s}\rangle = \langle\varphi|\psi_{j,(z,c)s}\rangle$, and therefore,

$$\Pi_c^z|\psi_{j,s}\rangle = |\psi_{j,(z,c)s}\rangle. \tag{5.45}$$

Then, for all $i,j \in \{1,\dots,d\}$, $s,t \in \Sigma^*$, for $(z,c_1),(z,c_2) \in \Sigma$ with $c_1 \neq c_2$,

$$\begin{aligned}\langle\psi_{j,t}|\Pi^z_{c_1}\Pi^z_{c_2}|\psi_{i,s}\rangle &= \langle\psi_{j,(z,c_1)t}|\psi_{i,(z,c_2)s}\rangle = M_{i,j}((z,c_1)t,(z,c_2)t)\\ &= \phi_{i,j}(t^R(z,c_1)(z,c_2)s) = 0.\end{aligned} \tag{5.46}$$

Therefore, we have that

$$\Pi^z_{c_1}\Pi^z_{c_2} = 0. \tag{5.47}$$

Moreover, for all $i,j \in \{1,\dots,d\}$, $s,t \in \Sigma^*, x \in \mathcal{X}$,

$$\sum_{a\in\mathcal{A}}\langle\psi_{i,s}|\Pi^x_a|\psi_{j,t}\rangle = \sum_{a\in\mathcal{A}}\langle\psi_{i,s}|\psi_{j,(x,a)t}\rangle = \sum_{a\in\mathcal{A}}\phi_{i,j}(s^R(x,a)t) = \phi_{i,j}(s^Rt) = \langle\psi_{i,s}|\psi_{j,t}\rangle,$$

and thus, $\sum_{a\in\mathcal{A}}\Pi^x_a = \mathbb{I}$. Analogously, one finds that for all $y \in \mathcal{Y}$, $\sum_{b\in\mathcal{B}}\Pi^y_b = \mathbb{I}$.

For all $i,j \in \{1,\dots,d\}, s,t \in \Sigma^*, x \in \mathcal{X}, y \in \mathcal{Y}, a \in \mathcal{A}, b \in \mathcal{B}$,

$$\begin{aligned}\langle\psi_{i,s}|\Pi^x_a\Pi^y_b|\psi_{j,t}\rangle &= \langle\psi_{i,(x,a)s}|\psi_{j,(y,b)t}\rangle = \phi_{i,j}(s^R(x,a)(y,b)t) = \phi_{i,j}(s^R(y,b)(x,a)t)\\ &= \langle\psi_{i,(y,b)s}|\psi_{j,(x,a)t}\rangle = \langle\psi_{i,s}|\Pi^y_b\Pi^x_a|\psi_{j,t}\rangle,\end{aligned} \tag{5.48}$$

and therefore $[\Pi^x_a,\Pi^y_b] = 0$.

Lastly, we see that, from (5.45),

$$M_{i,j}((x,a),(y,b)) = \langle\psi_{j,(x,a)}|\psi_{i,(y,b)}\rangle = \langle\psi_{j,\varepsilon}|A^x_aB^y_b|\psi_{i,\varepsilon}\rangle, \tag{5.49}$$

and, thus,

$$\begin{aligned}K(a,b\,|\,x,y) &= \mathrm{Tr}_{\mathcal{H}_{AB}}\big[(\mathbb{I}_R\otimes A^x_aB^y_b)|\psi\rangle\langle\psi|\big] = \sum_{l,k}\langle\psi_{l,k}|(\mathbb{I}_R\otimes A^x_aB^y_b)\sum_{i,j}|i\rangle|\psi_{i,\varepsilon}\rangle\langle\psi_{j,\varepsilon}|\langle j||\psi_{l,k}\rangle\\ &= \sum_{i,j}\langle\psi_{j,\varepsilon}|A^x_aB^y_b|\psi_{i,\varepsilon}\rangle|i\rangle\langle j| = \sum_{i,j}M_{i,j}((x,a),(y,b))|i\rangle\langle j| = M((x,a),(y,b)).\end{aligned}$$

□

5.3 Concrete games

In this section, we consider particular extended non-local games, and we analyze lossy and constrained versions of these games, inspired by experimental considerations computing the SDPs that give the values of $\omega^{(k)}_{admiss}$. We show that our results are consistent with previously known results, for some cases with a simpler proof, and we show new results, and tight results in Section 5.3.4. For a reader interested in applications in quantum cryptography, the games analyzed in this section will be used in Section 5.4 to prove security for cryptographic primitives.

5.3.1 Constrained BB84 monogamy-of-entanglement game

We now consider a constrained version of the $\mathcal{G}^{BB84}$ (G^{BB84}) game. Recall that in [TFKW13], it was shown that $\omega_Q(\mathcal{G}^{BB84}) = \cos^2\left(\frac{\pi}{8}\right)$, which is attained by the strategy $\mathbf{S}_{\text{TFKW}} = \{|\phi\rangle\langle\phi|, A_a^x = \delta_{a0}, B_a^x = \delta_{a0}\}$, where $|\phi\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$. In particular, as motivated in Theorem 5.2.3, we consider a constrained version of $\mathcal{G}^{BB84}$ in which Alice and Bob are required to never answer differently—that is, by imposing that the probability that they provide different answers is zero.

There are settings in quantum cryptography, for example in quantum-position verification, where this constraint can be added naturally—see Section 5.4. In this case, the set of constraints C is given by: for every strategy $\mathbf{S}_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,

$$\sum_{x,a,a'\neq b'} q(x)\text{Tr}[(V_a^x \otimes A_{a'}^x \otimes B_{b'}^x)\rho_{RAB}] = 0. \tag{5.50}$$

From Section 5.2.1, we have that

$$\omega_Q(\mathcal{G}_C^{BB84}) \leq \omega_{comm}(\mathcal{G}_C^{BB84}) \leq \omega_{admiss}^{(k=1)}(\mathcal{G}_C^{BB84}). \tag{5.51}$$

Solving the SDP (5.23) to obtain the value of $\omega_{admiss}^{(k=1)}(\mathcal{G}_C^{BB84})$, see code [EF], we find

$$\omega_{admiss}^{(k=1)}(\mathcal{G}_C^{BB84}) = 0.8535533905 \simeq \cos^2\left(\frac{\pi}{8}\right), \tag{5.52}$$

and therefore we see that constraining Alice and Bob by forbidding them to answer inconsistently does not lower their average winning probability. This is not surprising, since in [TFKW13] it was shown that the strategy $\mathbf{S}_{\text{TFKW}}$ gives the optimal value for $\mathcal{G}^{BB84}$. This strategy fulfills the constraints C, and therefore it is also optimal for $\mathcal{G}_C^{BB84}$.

Moreover, we see that for this game giving inconsistent answers precludes attaining the optimal value. For instance, if we impose the constraints C_ε given by

$$\sum_{x,a,a'\neq b'} q(x)\text{Tr}[(V_a^x \otimes A_{a'}^x \otimes B_{b'}^x)\rho_{RAB}] \geq \varepsilon, \tag{5.53}$$

for $\varepsilon \geq 0$, thus imposing that the probability that Alice and Bob answer inconsistently is at least ε, the upper bounds obtained by $\omega_{admiss}^{(k=1)}(\mathcal{G}_{C_\varepsilon}^{BB84})$ for different values of $\varepsilon > 0$ are lower than $\cos^2\left(\frac{\pi}{8}\right)$, see Figure 5.2 (black dots) for $0 \leq \varepsilon \leq 0.25$. This fact is consistent with the rigidity results for the $\mathcal{G}^{BB84}$ game shown in [BC23].

A numerical optimization over states $|\phi\rangle_{VAB}$ of dimension 2^3 with real coefficients, where each register is 2-dimensional (3-qubit states), and 2-dimensional projective measurements for both Alice and Bob, shows that the results obtained with the first level of the hierarchy ($\omega_{admiss}^{(k=1)}(\mathcal{G}_{C_\varepsilon}^{BB84})$) are *tight*, up to numerical precision. See the continuous black line in Figure 5.2 for the values of the numerical optimization, which match the values of $\omega_{admiss}^{(k=1)}(\mathcal{G}_{C_\varepsilon}^{BB84})$ (black dots), and

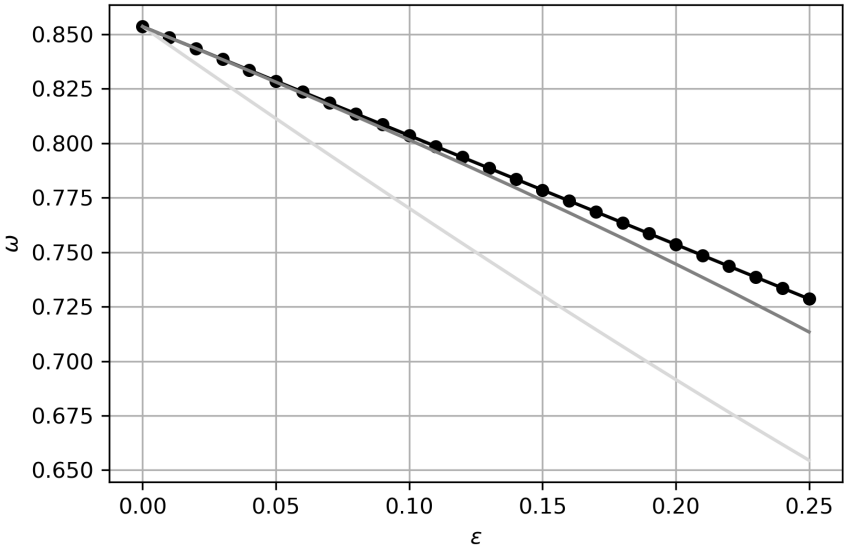


Figure 5.2: Values of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$ (black dots), optimal winning probability using unentangled strategies (light gray continuous line), 2-qubit state (dark gray continuous line) and 3-qubit state (black continuous line) for different values of ε.

see [EF] for the explicit states $|\phi\rangle_{VAB}$ and the 2-dimensional projective measurements $\{A^x_a\}$ and $\{B^y_b\}$ for different values of ε fulfilling the constraint (5.53) and matching the upper bounds $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$.

In addition, the optimal values for $\varepsilon > 0$, unlike for $\varepsilon = 0$ (strategy S^{BB84}_Q), cannot be obtained by unentangled strategies, i.e. by just preparing a single qubit and sending it to the referee. A numerical optimization over unentangled strategies fulfilling the constraint (5.53), see [EF], shows that the optimal values are significantly lower than $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$, see light gray line in Figure 5.2. Numerically optimizing over all states $|\phi\rangle_{VAB}$ of dimension 2^2, with the referee's and Alice's registers being both 2-dimensional and Alice performing projective measurements, shows that the optimal value increases, being *tight* (only) for small values of ε, see the dark gray line in Figure 5.2. Therefore, we see that imposing certain constraints forces Alice and Bob to utilize higher-dimensional quantum systems to achieve the optimal winning probability. We would like to stress that we do not have an understanding of the fundamental reason behind this requirement.

5.3.1. Remark. In order to analyze optimal strategies, if one is able to find an optimal strategy for an extended non-local game (or monogamy-of-entanglement game), one can constrain the game and see if certain restrictions on the strategies affect the optimal winning value. Finding a still-optimal perturbation of an

optimal strategy in such way is a way to exclude possible rigidity results.

5.3.2 Alice guessing game with constraints

We consider a slight variation of the $\mathcal{G}^{BB84}$ monogamy-of-entanglement game where only Alice has to guess the measurement outcome of the referee, described as follows:

$$\mathcal{G}^{\text{A } m \text{ guess}} := \left(q(z) = \frac{1}{|\mathcal{Z}|}, V = \{V_a^z = |v^z\rangle\langle v^z|\}_{z,v}, W = \{(z,v,a,b) \mid a = v\}_{z,v,a,b} \right),$$

with $\mathcal{Z} = \mathcal{V} = \mathcal{A} = \mathcal{B} = \{0,1\}^m$. Then, given any quantum strategy $\mathbf{S}_Q = \{\rho_{RAB}, A_a^z, B_a^z\}_{z,a}$,

$$\omega_Q(\mathcal{G}^{\text{A } m \text{ guess}}) = \frac{1}{2^m} \sum_{z,a} \text{Tr}\left[\left(V_v^z \otimes A_a^z \otimes (\sum_b B_b^z) \right) \rho_{RAB} \right] = \frac{1}{2^m} \sum_{z,a} \text{Tr}[(V_v^z \otimes A_a^z \otimes \mathbb{I}) \rho_{RAB}].$$

Notice that this game can be won with probability 1 if Alice and Bob send to the referee the maximally entangled state $|\Phi^+\rangle_{RA}^{\otimes n}$, Alice performs the same measurement as the referee and Bob answers at random, and thus, we have that

$$\omega_Q(\mathcal{G}^{\text{A } m \text{ guess}}) = 1. \tag{5.54}$$

Now, consider its constrained version given by imposing that Bob also has to guess the referee's measurement outcome up to an error p_{err} per bit, but does not have to coordinate his answers with Alice. This variant is motivated by ideas from device-independent QKD; we refer the reader to [EFS25a] for further details. In such a case, the set of constraints $C_{p_{err}}$ is described as: for every strategy $\mathbf{S}_Q = \{\rho_{RAB}, A_a^z, B_b^z\}_{z,a,b}$,

$$\sum_{z,a} q(z) \text{Tr}[(V_v^z \otimes A_a^z \otimes B_b^z) \rho_{RAB}] \leq p_{err}^{d_H(v,b)} \quad \forall v, b. \tag{5.55}$$

In order to find an upper bound on the winning probability, we find the values of $\omega_{admiss}^{(k=1)}(\mathcal{G}_C^{\text{A } m \text{ guess}})$ for $m = 1, 2$ computing the corresponding SDPs, see Figure 5.3 for their values. Notice that we obtain tight bounds for $p_{err} = 0$ and $p_{err} \geq \frac{1}{2}$, since for $p_{err} = 0$, i.e. if Bob's outcome has to perfectly match the referee's outcome, the optimal values are upper bounded by 0.5 and 0.25, for $m = 1$ and $m = 2$, respectively, which can be obtained by the strategy where Alice and Bob send $|\Phi^+\rangle_{RB}^{\otimes n}$, Bob measures V_b^z and Alice and makes the random guess $a = 0 \ldots 0$, which will be correct with probability $\frac{1}{2^m}$. On the other hand, if $p_{err} \geq \frac{1}{2}$, Bob can answer randomly and Alice can share $|\Phi^+\rangle_{RA}^{\otimes m}$ with the referee and perform the same measurement, in which case Alice's outcomes will be perfectly correlated with the referee's outcomes.

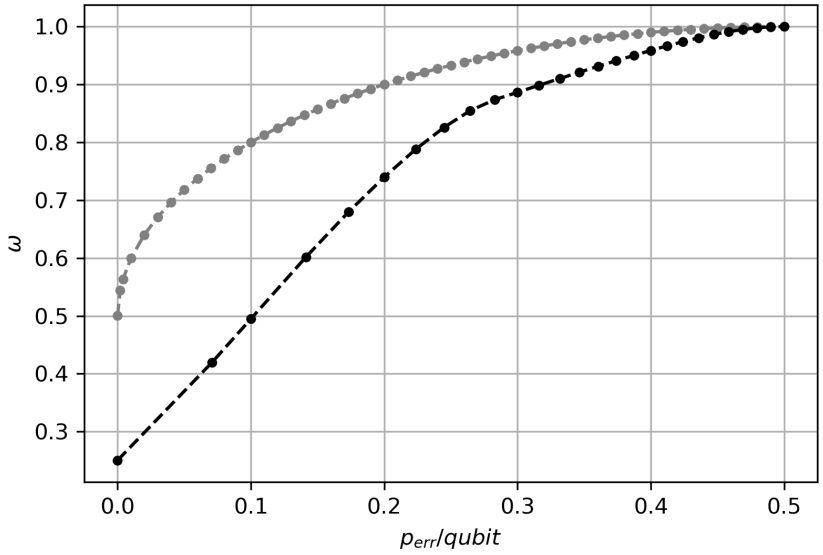


Figure 5.3: Upper bounds for $\omega_Q(\mathcal{G}^{\text{A } m \text{ guess}}_{C_{perr}})$ obtained from solving the SDP giving the value of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{\text{A } m \text{ guess}}_{C})$ for $m = 1$ (in grey) and $m = 2$ (in black).

5.3.3 Local guessing game

Let $m \in \mathbb{N}$, and consider the extended non-local game where Alice and Bob receive input $x \in \{0,1\}$ and the referee chooses $z \in \{0,1\}^m$, all uniformly at random. The referee's measurements (on a system of n qubits) are $V^z_v = |v^{z_1}_1\rangle\langle v^{z_1}_1| \otimes \ldots \otimes |v^{z_m}_m\rangle\langle v^{z_m}_m|$, for $v \in \{0,1\}^m$. Alice and Bob have to answer $a, b \in \{0,1\}^m$, and they win the game if and only if both answers are the same and, for every i such that $z_i = x$, then $a_i = b_i = v_i$, i.e. whenever R measures qubit i in basis x, Alice and Bob have to guess correctly the measurement outcome. This game will be denoted by $\mathcal{G}^{m-\text{local guessing}}$, and, in the above notation,

$$\mathcal{G}^{m-\text{local guessing}} := \left(q(z,x,y) = \frac{\delta_{x,y}}{2}\frac{1}{2^n}, V = \{V^z_v\}_{z,v}, W\right), \tag{5.56}$$

where $W = \{(z,x,v,a,b) \mid a = b \text{ and } \forall i \text{ s.t. } z_i = x, a_i = v_i\}$.

5.3.2. Proposition. *The optimal average winning probability of $\mathcal{G}^{m-\text{local guessing}}$ for $m = 1$ is given by $\omega_Q(\mathcal{G}^{1-\text{local guessing}}) = \frac{1+\cos^2\left(\frac{\pi}{8}\right)}{2}$. Moreover, this value is attained by the strategy $\mathbf{S}_{\text{TFWK}}$.*

Proof:
The strategy $\mathbf{S}_{\text{TFWK}}$ is such that its winning average probability is $\frac{1+\cos^2\left(\frac{\pi}{8}\right)}{2}$. On the other hand, consider an arbitrary strategy $\mathbf{S}_Q = \{\rho_{RAB}, A^x_a, B^x_b\}$, then

$$\begin{aligned}
\omega_Q(\mathcal{G}^{1-\text{local guessing}}, \mathbf{S}_Q) &= \frac{1}{2^2} \sum_{(z,x,v,a,b)\in W} \mathrm{Tr}[(V_v^z \otimes A_a^x \otimes B_b^x)\rho_{RAB}] \\
&= \frac{1}{2^2} \sum_{x,v,a} \mathrm{Tr}\big[(V_v^x \otimes A_a^{1-x} \otimes B_a^{1-x})\rho_{RAB}\big] + \frac{1}{2^2} \sum_{x,a} \mathrm{Tr}[(V_a^x \otimes A_a^x \otimes B_a^x)\rho_{RAB}] \\
&= \frac{1}{2^2} \sum_{x,v} \mathrm{Tr}\left[\Big(V_v^x \otimes \big(\sum_a A_a^{1-x} \otimes B_a^{1-x}\big)\Big)\rho_{RAB}\right] + \frac{1}{2^2} \sum_{x,a} \mathrm{Tr}[(V_a^x \otimes A_a^x \otimes B_a^x)\rho_{RAB}] \\
&\leq \frac{1}{2^2} \mathrm{Tr}\left[\left(\sum_{x,v} V_v^x\right)\rho_{RAB}\right] + \frac{1}{2}\omega(\mathcal{G}^{BB84}) = \frac{1}{2^2}\mathrm{Tr}[2\rho_{RAB}] + \frac{1}{2}\omega(\mathcal{G}^{BB84}) = \frac{1+\cos^2\left(\frac{\pi}{8}\right)}{2},
\end{aligned}$$

where we split the first sum in $x = z$ and $x \neq z$, then we used $\sum_a A_a^{1-x} \otimes B_a^{1-x} \leq \mathbb{I}$ and that $\frac{1}{2}\sum_{x,a} \mathrm{Tr}[(V_a^x \otimes A_a^x \otimes B_a^x)\rho_{RAB}] \leq \omega_Q(\mathcal{G}^{BB84})$, and finally, that $\sum_{x,v} V_v^x = 2\mathbb{I}$ and $\mathrm{Tr}[\rho_{RAB}] = 1$.

□

The m-fold parallel repetition of the strategy $\mathbf{S}_{tfwk}$, denoted by $(\mathbf{S}_{tfwk})^{\times m}$ does not provide the optimal value for $\mathcal{G}^{m-\text{local guessing}}$ for all m. To see this, notice that on the one hand, this strategy has average winning probability

$$\omega(\mathcal{G}^{m-\text{local guessing}}, (\mathbf{S}_{\text{TFWK}})^{\times m}) = \left(\frac{1}{4}\Big(3 + \frac{1}{\sqrt{2}}\Big)\right)^m. \tag{5.57}$$

On the other hand, consider the strategy $\mathbf{S}_{m-0} = \{|0\rangle^{\otimes m}, A_a^x = \delta_{a,0\ldots0}, B_b^y = \delta_{b,0\ldots0}\}$. This strategy is such that

$$\omega(\mathcal{G}^{m-\text{local guessing}}, \mathbf{S}_{m-0}) = \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^m. \tag{5.58}$$

To see this, let $\mathcal{T}_{xz} \coloneqq \{i \mid z_i = x\}$, let $t = |T_{xz}|$, denote by $\mathcal{T}_{xz}^c$ its complement, and, abusing of notation, we will write $\sum_{v\in\mathcal{T}_{xy}}$ for a bit string $v \in \{0,1\}$ to sum the indices i of v such that $i \in \mathcal{T}_{xz}$. Then,

$$\begin{aligned}
\omega(\mathcal{G}^{m-\text{local guessing}}, \mathbf{S}_{m-0}) &= \frac{1}{2^{m+1}} \sum_{(z,x,v,a,b)\in W} \mathrm{Tr}[(|0\rangle\langle 0|)^{\otimes m}|v^z\rangle\langle v^z|\delta_{a,0}] \\
&= \frac{1}{2^{m+1}} \sum_{z,x} \mathrm{Tr}\left[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}| \otimes |0_{\mathcal{T}_{xz}^c}\rangle\langle 0_{\mathcal{T}_{xz}^c}|)(|0^{x\ldots x}_{\mathcal{T}_{xz}}\rangle\langle 0^{x\ldots x}_{\mathcal{T}_{xz}}| \otimes \sum_{v\in\mathcal{T}_{xz}^c} |v^{1-x\ldots1-x}_{\mathcal{T}_{xz}^c}\rangle\langle v^{1-x\ldots1-x}_{\mathcal{T}_{xz}^c}|)\right] \\
&= \frac{1}{2^{m+1}} \sum_{z,x} \mathrm{Tr}\big[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0^{x\ldots x}_{\mathcal{T}_{xz}}\rangle\langle 0^{x\ldots x}_{\mathcal{T}_{xz}}| \otimes |0_{\mathcal{T}_{xz}^c}\rangle\langle 0_{\mathcal{T}_{xz}^c}|\mathbb{I}\big] \\
&= \frac{1}{2^{m+1}}\left(\sum_{z,x-0} \mathrm{Tr}[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|] + \sum_{z,x=1} \mathrm{Tr}\big[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0^{1\ldots1}_{\mathcal{T}_{xz}}\rangle\langle 0^{1\ldots1}_{\mathcal{T}_{xz}}|\big]\right) \\
&= \frac{1}{2^{m+1}}\left(\sum_z 1 + \sum_{t=0}^m \binom{m}{t} 2^{-t}\right) = \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^m,
\end{aligned} \tag{5.59}$$

where we used that $\mathrm{Tr}\big[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0^{1,..1}_{\overline{\mathcal{T}}_{xz}}\rangle\langle 0^{1,..1}_{\overline{\mathcal{T}}_{xz}}|\big] = |\langle 0_{\mathcal{T}_{xz}}|0^{1,..1}_{\overline{\mathcal{T}}_{xz}}\rangle| = 2^{-t}$. Similarly, one can see (5.57).

We see that for $m \geq 8$, the strategy $\mathbf{S}_{m-0}$ outperforms $(\mathbf{S}_{\mathrm{TFWK}})^{\times m}$. Not only this, but winning probability of the former strategy decays exponentially in m, whereas $\mathbf{S}_{m-0}$ has a winning probability of at least $\frac{1}{2}$. Therefore, we can conclude that

$$\omega_Q(\mathcal{G}^{m-\text{local guessing}}) \geq \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^m. \tag{5.60}$$

In [PGK18] an upper bound was shown that can be directly transformed in an upper bound for $\mathcal{G}^{m-\text{local guessing}}$, which we state in the below proposition:

5.3.3. Proposition. *([PGK18]) For every $m \in \mathbb{N}$, the following bound holds*

$$\omega_Q(\mathcal{G}^{m-local\ guessing}) \leq \frac{1}{2} + \frac{1}{2}\left(\frac{1+1/\sqrt{2}}{2}\right)^m. \tag{5.61}$$

In order to verify tightness of (5.61), we compute the SDPs providing the values of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{n-\text{local guessing}})$ for $m = 1, 2, 3, 4, 5$, see Figure 5.4. We see that using SDPs, we obtain tighter upper bounds for the above-mentioned values of m.

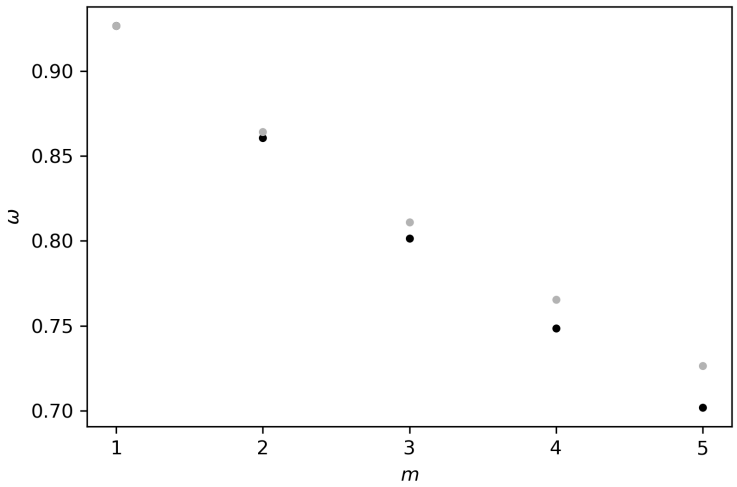


Figure 5.4: Upper bounds in Proposition 5.3.3, given by (5.61), (gray dots) and upper bounds obtained by $\omega^{(k=1)}_{admiss}(\mathcal{G}^{n-\text{local guessing}})$ (black dots).

5.3.4 Lossy monogamy-of-entanglement games

Consider the lossy-and-constrained version of $\mathcal{G}^{BB84}$, denoted by $\mathcal{G}^{BB84}_{C,\eta}$, where the set of constraints C is given as in the previous case by imposing that Alice

and Bob never answer differently, i.e. imposing that their probability of answering different is 0. In this case, the set of constraints C is given by: for every strategy $\mathbf{S}_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,

$$\sum_{x,a,a'\neq b'} q(x)\mathrm{Tr}[(V_a^x \otimes A_{a'}^x \otimes B_{b'}^x)\rho_{RAB}] = 0. \tag{5.62}$$

In Chapter 3, tight results for the optimal winning probability of this lossy-and-constrained game are provided by an *ad hoc* method combining the '1 + AB' level of the NPA hierarchy [NPA08] with extra linear constraints derived from bounding operator norms.

Solving the SDP (5.23) for k = '1 + AB' in the game $\mathcal{G}_{C,\eta}^{BB84}$ (see code [EF]) confirms the results presented in Chapter 3—and does so without requiring intermediate analytical steps such as the proof of Proposition 3.2.8. In particular, it confirms Theorem 3.2.10, which shows that the optimal value is achieved by the strategy given by a convex combination of $\mathbf{S}_{\text{TFWK}}$ and $\mathbf{S}_{guess}$, which is the strategy where Alice and Bob make the guess $x = 0$ for the referee's measurement, and they answer 0 if the guess was right, and they answer $\perp$ if their guess was wrong. See Figure 5.5 for a plot of the results (this plot is equivalent to Figure 3.3). We see that level 1, $\omega_{admiss}^{(k=1)}$, provides a good approximation, whereas level 1 in Section 4.2, see Figure 3.3, is far from the optimal value. The main advantage is that it is enough to have the description of the game to find the value and there is no need to derive extra linear constraints. Moreover, we know that $\omega_{admiss}^{(k)}$ will converge to the true value, whereas it was not necessarily the case in the *ad hoc* method in Chapter 3. This becomes more clear in the following case.

Consider the extended non-local game $\mathcal{G}^{3-bases}$ described by

$$\mathcal{G}^{3-bases} := \left(q(x) = \frac{1}{|\mathcal{X}|}, V = \{V_a^x = |a_x\rangle\langle a_x|\}_{x,a}, W = \{(x,v,a,b) \mid v = a = b\}_{x,v,a,b}\right), \tag{5.63}$$

with $\mathcal{X} = \{0,1,2\}$ and $\mathcal{A} = \{0,1\}$, where $|a_0\rangle = |a\rangle$, $|a_1\rangle = H|a\rangle$, and $|a_2\rangle = |i\rangle$ if $a = 0$ and $|a_2\rangle = |-i\rangle$ if $a = 1$. This game is similar to $\mathcal{G}^{BB84}$ but the referee, instead of measuring his local register in either the computational or the Hadamard basis, can also measure in the basis $\{|\pm i\rangle\}$. The lossy-and-constrained version of this game, $\mathcal{G}_{C,\eta}^{3-bases}$, where C is given by forbidding different answers from Alice and Bob, is analyzed in Section 3.3 with the *ad hoc* method providing upper bounds on $\omega_Q(\mathcal{G}_\eta^{3-bases})$ for $\forall \eta \in [0,1]$, see Figure 3.5. Nevertheless, in Section 3.3, it was left open whether those bounds were tight. Here, we show that solving the SDPs for $\omega_{\text{admiss}}^{(k)}(\mathcal{G}_{C,\eta}^{3\text{-bases}})$ yields improved upper bounds (see Figure 5.6). In addition, we will see that these bounds are indeed tight. Moreover, we computed the values for $\omega_{admiss}^{k=1}(\mathcal{G}_\eta^{3-bases})$, i.e. without the constraint of imposing same answers for Alice and Bob, and we obtained the same value. In search of optimal strategies for every η, this fact leads us to think of strategies that always coordinate the answers of Alice and Bob, consisting on preparing a concrete qubit and pre-agreeing a fix answer regardless the question they receive.

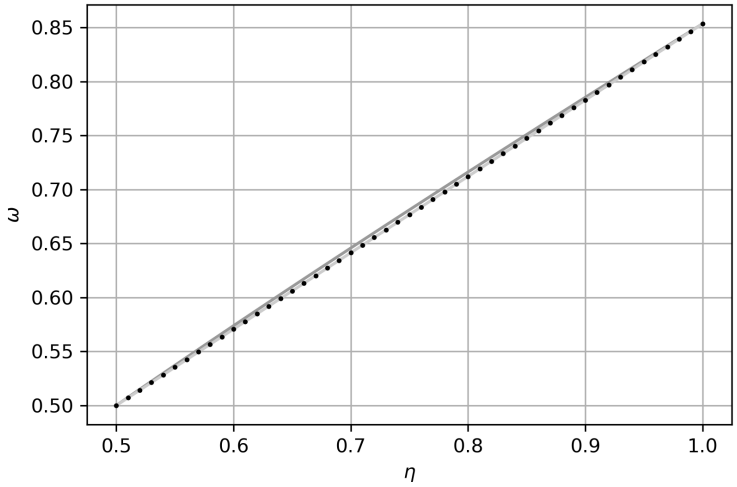


Figure 5.5: Solutions of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C,\eta})$ and $\omega^{(k=\text{`}1+AB\text{'})}_{admiss}(\mathcal{G}^{BB84}_{C,\eta})$, represented by dark gray continuous line and black dots, respectively, together with the winning probability of the strategy given by the convex combination of the strategies $\mathbf{S}_{\text{TFWK}}$ and $\mathbf{S}_{guess}$, represented by a light gray continuous line.

Consider the strategies

$$S_Q^{3-guess} = \{|0\rangle\langle 0|, A_a^0 = \delta_{a0}, A_a^1 = A_a^2 = \delta_{a\perp}, B_a^0 = \delta_{a0}, B_a^1 = B_a^2 = \delta_{a\perp}\}, \tag{5.64}$$

which consists on guessing $x = 0$ and answering $\perp$ (photon loss) if the guess was wrong,

$$S_Q^{3-BB84} = \{|\phi\rangle\langle\phi|, A_a^0 = A_a^1 = \delta_{a0}, A_a^2 = \delta_{a\perp}, B_a^0 = B_a^1 = \delta_{a0}, B_a^2 = \delta_{a\perp}\}, \tag{5.65}$$

where $|\phi\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$, consisting on using $\mathbf{S}_{\text{TFWK}}$ if $x \in \{0,1\}$ and claiming photon loss if $x = 2$, and

$$S_Q^{3-bases} = \{|\phi_3\rangle\langle\phi_3|, A_a^x = \delta_{a0}, B_a^x = \delta_{a0}\}, \tag{5.66}$$

where $|\phi_3\rangle = \cos\Big(\frac{\tan^{-1}(\sqrt{2})}{2}\Big)|0\rangle + e^{i\frac{\pi}{4}}\sin\Big(\frac{\tan^{-1}(\sqrt{2})}{2}\Big)|1\rangle$. Notice that $|\phi_3\rangle$ is the state that has simultaneous maximum overlap with $|0\rangle, |+\rangle$ and $|i\rangle$, i.e.

$$\max_{|\varphi\rangle}\Big\{|\langle 0|\varphi\rangle|^2 + |\langle +|\varphi\rangle|^2 + |\langle i|\varphi\rangle|^2\Big\} = |\langle 0|\phi_3\rangle|^2 + |\langle +|\phi_3\rangle|^2 + |\langle i|\phi_3\rangle|^2. \tag{5.67}$$

5.3.4. Result. *The strategy $\mathcal{S}_Q^{3\eta}$ consisting of Alice and Bob playing:*

- *the convex combination of $S_Q^{3-guess}$ and S_Q^{3-BB84}, for $\eta \in [\frac{1}{3}, \frac{2}{3})$,*
- *the convex combination of S_Q^{3-BB84} and $S_Q^{3-bases}$, for $\eta \in [\frac{2}{3}, 1]$*

is optimal for $\mathcal{G}_\eta^{3-bases}$ *with*

$$\omega_Q(\mathcal{G}_\eta^{3-bases}) = \begin{cases} \frac{1}{3} + \frac{1}{\sqrt{2}}(\eta - \frac{1}{3}) \text{ if } \eta \in [\frac{1}{3}, \frac{2}{3}), \\ \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}}\right) + \frac{1-\sqrt{2}+\sqrt{3}}{2}\eta \text{ if } \eta \in [\frac{2}{3}, 1]. \end{cases} \tag{5.68}$$

The strategy $\mathcal{S}_Q^{3\eta}$ matches the upper bound obtained by the SDP giving the value of $\omega_{admiss}^{(k)}(\mathcal{G}_\eta^{3-bases})$, where k = '1 + AB' for $\eta \in [\frac{1}{3}, \frac{2}{3})$ and $k = 1$ for $\eta \in [\frac{2}{3}, 1]$. We want to highlight that $k = 1$ for $\eta \in [\frac{1}{3}, \frac{2}{3})$ has solutions that are almost equal for k = '1 + AB' and just diverge in the third decimal. Notice that $\mathcal{S}_Q^{3\eta}$ slightly outperforms the strategy given by the convex combination of $S_Q^{3-guess}$ and $S_Q^{3-bases}$, see blue line in Figure 5.6.

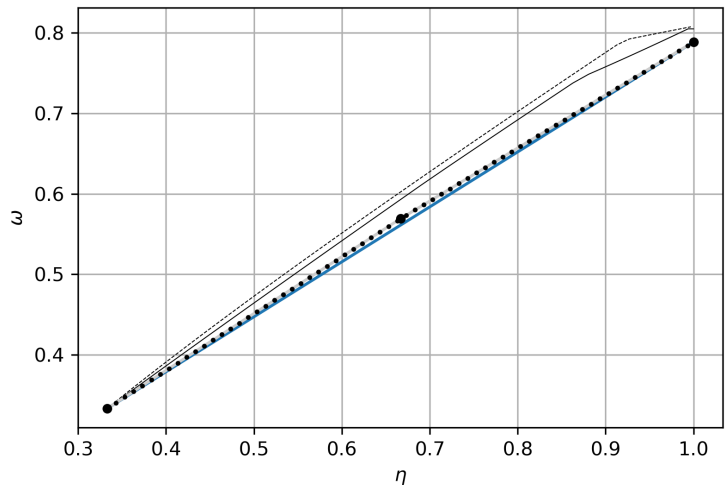


Figure 5.6: The dotted and continuous lines correspond to the upper bounds obtained in Section 3.3 (see Figure 3.5) with the *ad hoc* method using the 1st and 2nd levels of the NPA hierarchy, respectively. The black dots correspond to the values of $\omega_{admiss}^{(k)}(\mathcal{G}_\eta^{3-bases})$, where k = '1 + AB' for $\eta \in [\frac{1}{3}, \frac{2}{3})$ and $k = 1$ for $\eta \in [\frac{2}{3}, 1]$, the gray line correspond to the winning values of the strategy $\mathcal{S}_Q^{3\eta}$, the blue line corresponds to the winning value of the strategy given by the convex combination of $S_Q^{3-guess}$ and $S_Q^{3-bases}$, and the big black dots correspond to the winning probabilities of the strategies $S_Q^{3-guess}$, S_Q^{3-BB84} and $S_Q^{3-bases}$, respectively.

Unlike for $\mathcal{G}_\eta^{BB84}$, the optimal strategy for $\mathcal{G}_\eta^{3-bases}$ for every η is not just given by simply playing the optimal strategy (for $\eta = 1$) with a certain frequency and combining it with the guessing strategy, claiming photon loss enough times to be consistent with η. This is summarized in the below observation:

5.3.5. Remark. The optimal winning probability of a lossy extended non-local game is not always given by the convex combination of the optimal strategy for $\eta = 1$ and the guessing attack.

5.4 Application to quantum position verification

As explained in Chapter 3, in [BCF+14], it was proven that QPV_{BB84} is secure in the No Pre-shared entanglement model, that is, if the attackers do not pre-share entanglement prior to the execution of the protocol. They did so by upper bounding the probability that both Alice and Bob can guess the outcome of V_0's measurement (which they use to answer in the last step of the attack). In [TFKW13], it was shown that security of QPV_{BB84} can be reduced to the $\mathcal{G}^{BB84}$ game. In an experimental implementation, one might expect the prover to answer incorrectly with a certain probability. However, since P broadcasts classical information, it is not expected that she ever sends different answers (*inconsistent answers*) to the two verifiers. Therefore, if in any round the verifiers receive an inconsistent answer, they can abort the entire protocol since they have observed something that will never happen in an honest execution of the protocol. Thus, it is natural to study security adding related constraints to the attackers, which might lower their probability to win the extended non-local game, and thereby provide a tighter bound on the best attack of the protocol. A natural constraint to $\mathcal{G}^{BB84}$ would be to forbid inconsistent answers, i.e. to impose the set of constraints C for every strategy $\mathbf{S}_Q = \{\rho_{RAB}, A_a^z, B_a^z\}_{z,a}$ given by

$$\sum_{x,a,a'\neq b'} q(x)\text{Tr}[(V_a^x \otimes A_{a'}^x \otimes B_{b'}^x)\rho_{RAB}] = 0. \tag{5.69}$$

This corresponds to the constrained $\mathcal{G}^{BB84}$ game analyzed in Section 5.3.1, showing that unentangled attackers cannot win it with probability greater than $\cos^2(\frac{\pi}{8})$, corresponding to the optimal winning probability without constraining the game.

As introduced in Chapter 1 and analyzed in Chapters 3 and 4, in a practical application, not only errors arise, but also a sizable fraction sent from the verifiers to the prover is lost. In the case of QPV_{BB84}, if the transmission rate from the channel connecting V_0 and P is η, the prover is expected to answer either 0, 1 or that she did not receive the qubit (with probability $1-\eta$). The lossy version of QPV_{BB84}, denoted by $\text{QPV}_{\text{BB84}}^{\eta}$ is described in Definition 3.2.1. In Chapter 3, we showed that the security of $\text{QPV}_{\text{BB84}}^{\eta}$ could be reduced to the lossy monogamy-of-entanglement game, in particular, this corresponds to a lossy-and-constrained extended non-local game $\mathcal{G}_{C,\eta}^{BB84}$, which we analyzed in Section 5.3.4, with $\omega_Q(\mathcal{G}_{C,\eta}^{BB84}) = \frac{1}{\sqrt{2}}\eta + \sin^2\left(\frac{\pi}{8}\right)$. We therefore see that for an honest prover without error, the protocol remains secure for $\eta > \frac{1}{2}$, since the honest prover will answer correctly with probability η and $\eta > \frac{1}{\sqrt{2}}\eta + \sin^2\left(\frac{\pi}{8}\right)$ for all $\eta > \frac{1}{2}$. Moreover,

for a given η, the protocol tolerates a total error p_{err} as long as

$$\eta(1-p_{err}) > \frac{1}{\sqrt{2}}\eta + \sin^2\left(\frac{\pi}{8}\right). \tag{5.70}$$

Since the results are tight, the above inequality provides the optimal relation with the error. We saw that using our new methodology introduced in this chapter, the results of Section 4.2 are verified in a simplified way, since there it was necessary to derive inequalities using the norms of the verifier's measurements but just the description of the protocol.

The application of Section 5.3.4 in QPV not only verifies in a different way previously known results but improves some, providing tight results. Consider the extension of QPV_{BB84}, originally introduced in [KMS11], consisting on V_0 sending a uniformly random state from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ and V_0 sending in which basis to measure (Hadamard, computational or $\{|\pm i\rangle\}$), see Section 3.3. The security of this protocol in the No-PE model can be reduced to the winning probability of the extended non-local game $\mathcal{G}^{3-bases}$, as shown in Section 3.3. We analyzed this game in Section 5.3.4, and it has optimal value $\frac{1}{2} + \frac{\sqrt{3}}{6}$, therefore, attackers can spoof the verifiers with at most a probability $\frac{1}{2} + \frac{\sqrt{3}}{6} \simeq 0.788675$ per round. In addition, if loss is considered, security reduced to the winning probability of $\mathcal{G}^{3-bases}_{C,\eta}$ where the set of constraints is such that different answers are forbidden, whose optimal winning probability is given in Theorem 5.3.4. Notice that we have that $\omega_Q(\mathcal{G}^{3-bases}_{C,\eta}) = \omega_Q(\mathcal{G}^{3-bases}_{\eta})$, since the optimal strategy given in Theorem 5.3.4 is such that C is fulfilled. Then, for an error-free prover, one expects correct answers with probability η and the protocol is secure for $\eta > \frac{1}{3}$, since for this range, $\eta > \omega_Q(\mathcal{G}^{3-bases}_{C,\eta})$. Then, given a transmission rate η, the tight relation with the error p_{err} is given by:

(i) if $\eta \in [\frac{1}{3}, \frac{2}{3})$, then $\eta(1-p_{err}) > \frac{1}{3} + \frac{1}{\sqrt{2}}(\eta - \frac{1}{3})$,

(ii) if $\eta \in [\frac{2}{3}, 1]$, then $\eta(1-p_{err}) > \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}}\right) + \frac{1-\sqrt{2}+\sqrt{3}}{2}\eta$.

Security for 2-fold parallel repetition of $\text{QPV}^{\eta}_{\text{BB84}}$

The security of the m-fold parallel repetition of $\text{QPV}^{\eta}_{\text{BB84}}$, given that the attackers do not pre-share entanglement, can be reduced to the m-fold parallel repetition of the lossy extended non-local game $\mathcal{G}^{BB84\times n}_{\eta}$, with $\mathcal{Z} = \{0,1\}^m$, and $\mathcal{A} = \mathcal{B} = \{0,1,\perp\}^m$.

In this section, we analyze the case $m = 2$ and we show security for the 2-fold parallel repetition of $\text{QPV}^{\eta}_{\text{BB84}}$, given that the attackers do not pre-share entanglement. Imposing the same loss rate for both qubits, i.e.

$$\sum_{z_1 z_2} q(z_1 z_2)\text{Tr}[(\mathbb{I}_R \otimes \mathbb{I}_R \otimes A^{z_1 z_2}_{\perp\perp} B^{z_1 z_2}_{\perp\perp})\rho_{RAB}] = (1-\eta)^2, \tag{5.71}$$

$$\sum_{z_1 z_2} q(z_1 z_2)\mathrm{Tr}\Big[(\mathbb{I}_R \otimes \mathbb{I}_R \otimes A^{z_1 z_2}_{a_0 \perp} B^{z_1 z_2}_{a'_0 \perp})\rho_{RAB}\Big] = \frac{1}{2}\eta(1-\eta), \quad \forall a_0, a'_0 \in \{0,1\}, \tag{5.72}$$

$$\sum_{z_1 z_2} q(z_1 z_2)\mathrm{Tr}\Big[(\mathbb{I}_R \otimes \mathbb{I}_R \otimes A^{z_1 z_2}_{\perp a_1} B^{z_1 z_2}_{\perp a'_1})\rho_{RAB}\Big] = \frac{1}{2}\eta(1-\eta), \quad a_1, a'_1 \in \{0,1\}, \tag{5.73}$$

we obtain an upper bound solving the SDP that gives the value $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84\times 2}_{\eta})$. The obtained values, see [EF] for the code, are plotted in Figure 5.7, together with the winning value of the parallel repetition of the optimal strategy for $\mathcal{G}^{BB84}_{\eta}$. We see that the upper bounds are slightly grater than the values corresponding to the parallel repetition of the optimal strategy, and thus it remains open if strong parallel repetition holds when there is loss.

An error-free honest prover will answer correctly with probability η^2, which is strictly larger than the upper bounds found for $\omega_Q(\mathcal{G}^{BB84\times 2}_{\eta})$, for all $\eta > \frac{1}{2}$. In addition, if the total error of the prover is p_{err}, we have security for 2-fold parallel repetition as long as the probability of answering correctly, given by $\eta^2(1-p_{err})$, is such that

$$\eta^2(1-p_{err}) > \omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84\times 2}_{\eta}). \tag{5.74}$$

Security for the m-fold parallel repetition for a given m can be computed analogously. Since our techniques do run into a practical limit when increasing m, we leave the open problem to create a more efficient program that computes the parallel repetition faster.

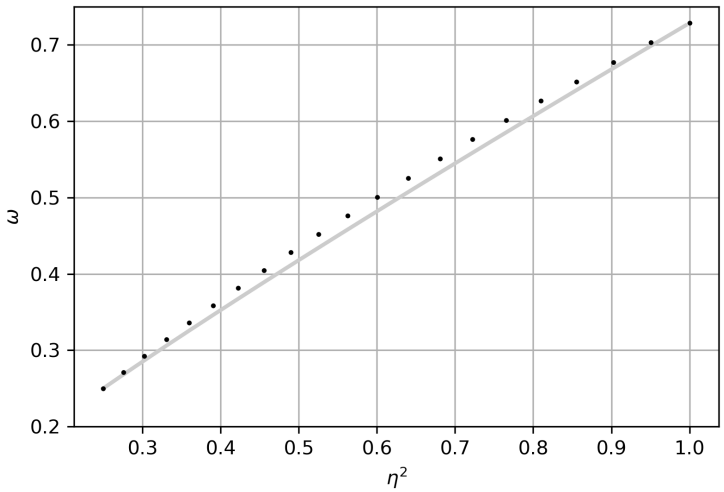


Figure 5.7: Values of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84\times 2}_{\eta})$ (black dots) and winning values for the parallel repetition of the optimal strategy for $\mathcal{G}^{BB84}_{\eta}$ (gray continuous line).

Chapter 6

Parallel repetition of local simultaneous state discrimination

In the previous chapters, we analyzed monogamy-of-entanglement (MoE) games and their generalization, extended non-local games. In those settings, two distant players, Alice and Bob, prepare a joint state, send one share to a quantum referee, the referee performs a measurement chosen from a publicly known set and announces his choice, and the players return answers that must satisfy a known predicate, for instance, guessing the referee's outcome in a MoE game.

This chapter inverts the picture. We consider games in which the referee prepares a tripartite state—specifically a classical-quantum-quantum state—keeps the classical register, and distributes the two quantum subsystems to Alice and Bob. Then, the referee performs a projective measurement on his register. The players, acting locally, must identify the outcome, i.e. determine which bipartite state they share. Such task is called the local simultaneous state-discrimination (LSSD) game, first introduced in [MOST24].

In this chapter, we first characterize optimal strategies using classical resources for a broad class of LSSD games. We then focus on a representative member of this class: the binary-symmetric-channel (BSC) game, parameterized by an error probability α. For this game, we analyze its parallel repetition and provide the exact winning probabilities attainable with classical, quantum, and no-signaling resources. Interestingly, for most values of α, the success probability attainable with classical strategies already equals that of their—ostensibly stronger—quantum and no-signaling counterparts.

The results presented in this chapter are based on the following publication:

- *Quantum 9, 1706* , "Parallel repetition of local simultaneous state discrimination", by Llorenç Escolà-Farràs, Jaròn Has, Maris Ozols, Christian Schaffner, and Mehrdad Tahmasbi [EFHO+25].

6.1 Introduction

The task of distinguishing between different statistical hypotheses is of fundamental importance in information processing and cryptography [Bla74, Mau00, PPV10]. A rich and extensive literature exists on this fundamental problem under the name of hypothesis testing or state discrimination[Hel69, Was04, BK15]. In quantum cryptography and quantum information theory, a natural extension of this task is to distinguish *quantum states*. In the context of non-local games, the state discrimination problem arises in a multi-player setting. In these scenarios, it is interesting to study how non-local resources such as shared randomness, quantum entanglement or no-signaling correlations can help the players to succeed in the state discrimination task. The authors of [BDF+99, CLMO13] have studied the scenario where local operation and classical communication are allowed between two parties, showing that entanglement can help the players.

The authors of [MOST24] studied another variant of distributed state discrimination in which multiple parties cannot communicate and have to estimate the state locally and simultaneously, hence calling the problem *local simultaneous state discrimination* (LSSD). LSSD problems naturally arise in the context of uncloneable cryptography [BL20, MST21, AKL+22, CLLZ21], where classical data is encoded into a quantum state such that an adversary cannot copy it. In such scenarios, successfully copying translates into successfully distinguishing quantum states. LSSD can be formulated in the following way: a referee selects a bipartite state and sends one register to Alice and the other register to Bob, who have to guess which global state they received. LSSD problems are closely related to monogamy-of-entanglement (MoE) games [TFKW13], where, as introduced in Chapter 3, two parties prepare a tripartite state and perform a measurement to guess the outcome of a measurement performed by a third party. Analyzing optimal performance of MoE games has proven useful in establishing the security of uncloneable cryptographic schemes [BL20], semi device-independent quantum key distribution [TFKW13], and quantum position verification [TFKW13].

Depending on the resources shared between the players of an LSSD game, one can consider various strategies. The authors of [MOST24] showed that even when the state has a classical description, quantum entanglement could enhance the probability of simultaneous state discrimination, and the more powerful resource of no-signaling correlations could enhance it even further. As [MOST24] have shown that finding the optimal strategy for three-party LSSD is NP-hard, it is likely to be challenging to study LSSDs in general. One could, however, characterize the optimal probability of winning and optimal strategies for LSSDs with some specific structure. One natural structure of interest is when an LSSD problem consists of several independent and identical LSSDs, and the parties have to win all these games at once in parallel. Parallel repetition appears often in the structure of cryptographic protocols.

In this chapter, we first outline the general framework of local simultaneous

state-discrimination (LSSD) games and then focus on the subclass in which every bipartite state prepared by the referee admits a classical description. For two distinct structural subclasses within this family, we characterize (i) the optimal winning probabilities when Alice and Bob use *classical* resources in one case, and (ii) structural properties of optimal no-signaling strategies under arbitrary parallel repetition in the other. We then zoom in on the *binary-symmetric-channel* (BSC) game [MOST24], which exemplifies both of these structural properties: the referee encodes a single bit into two noisy copies, corrupted independently with probability α, and Alice and Bob must recover the original bit simultaneously. We analyze its 2- and 3-fold parallel repetition for every possible error α. We use (i) to obtain the optimal classical winning probability, and then, providing *analytical* solutions of primal and dual linear programs, we give the corresponding optimal no-signaling probabilities, utilizing (ii). For the two-parallel repetition, we show that, using the Navascués-Pironio-Acín (NPA) hierarchy [NPA08], via solving semidefinite programs, the numerical results match the analytical optimal classical winning probability, and thus indicating that quantum resources offer no advantage in this case.

The results reveal a striking pattern. For the 2-fold parallel repetition of the BSC game, for all α we observe *no quantum advantage*: the best quantum strategy achieves precisely the classical success probability. Moreover, for almost every α even no-signaling correlations fail to outperform classical ones, highlighting a narrow gap between classical, quantum, and supra-quantum resources in this setting.

6.2 Local simultaneous state discrimination

Now, we define the local simultaneous state discrimination (LSSD) task, originally introduced in [MOST24]. In particular, we discuss strategies with classical, quantum and no-signaling resources for LSSD, and show that the optimal classical success probability can be attained by a symmetric strategy if certain conditions are fulfilled.

Let $\mathcal{V}$, $\mathcal{X}$ and $\mathcal{Y}$ be finite non-empty alphabets, and let p be a probability distribution over $\mathcal{V}$. Three parties will play a role in the extended non-local games: a referee, Alice and Bob, whose associated Hilbert spaces will be denoted by $\mathcal{H}_R, \mathcal{H}_A$ and $\mathcal{H}_B$, with dimensions $|\mathcal{V}|$, $|\mathcal{X}|$, and $|\mathcal{Y}|$, respectively. Let $\{|v\rangle\}_{v\in\mathcal{V}}$ an orthonormal basis of $\mathcal{H}_R$.

6.2.1. Definition. *Let $\{\rho^v_{AB}\}_{v\in\mathcal{V}}$ a set of publicly known quantum states on a finite dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. A* local simultaneous state discrimination *(LSSD) game* $\mathbf{G}$*, played by a referee R and two collaborative parties, Alice and Bob, denoted by the tuple*

$$\mathbf{G} = (p, \{\rho^v_{AB}\}_{v\in\mathcal{V}}), \tag{6.1}$$

is described as follows:

1. *The referee prepares the classical-quantum-quantum (cqq) state*

$$\rho_{RAB} = \sum_{v \in \mathcal{V}} p(v) |v\rangle\langle v|_R \otimes \rho^v_{AB}, \tag{6.2}$$

   and sends registers A and B of ρ_{AB} to Alice and Bob, respectively. The two parties are no longer allowed to communicate.

2. *The referee performs a projective measurement on his local register in the basis $\{|v\rangle\}_{v \in \mathcal{V}}$, obtaining the outcome v.*

3. *The task for Alice and Bob is to guess v, i.e. they output $a, b \in \mathcal{V}$, and they win if and only if $a = b = v$.*

See Figure 6.1 for a schematic representation of a generic LSSD game. See Figure 5.1 in Chapter 5 for a visual comparison between LSSD games and extended non-local games. In essence, the key difference lies in which party prepares the quantum state: in LSSD games, the referee prepares and distributes it to the players, while in extended non-local games, the players prepare the state and the referee sends classical questions.

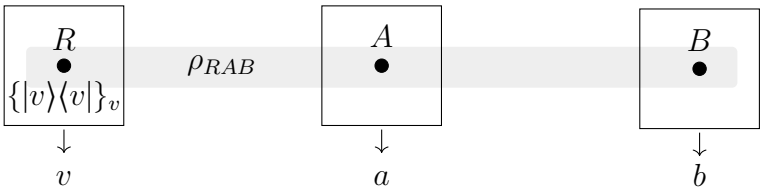


Figure 6.1: Schematic representation of a local simultaneous state discrimination game. The gray-shaded region represents the tripartite quantum state ρ_{RAB} prepared by the referee and shared amongst the three parties.

Note that an LSSD game can equivalently be described as follows: the referee samples $v \in \mathcal{V}$ according to the distribution p, prepares the corresponding state ρ^v_{AB}, and sends the A and B registers to Alice and Bob, respectively—who must then guess the value of v.

In this chapter, we analyze LSSD games in which the quantum states $\{\rho^v_{AB}\}_{v \in \mathcal{V}}$ from Definition 6.2.1 are *classical*, i.e. of the form

$$\rho^v_{AB} = \sum_{x,y} q(x, y|v) |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B, \tag{6.3}$$

where $\{|x\rangle\}_{x \in \mathcal{X}}$ and $\{|y\rangle\}_{y \in \mathcal{Y}}$ are orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, and q is a probability distribution over $\mathcal{V} \times \mathcal{X} \times \mathcal{Y}$, i.e. it satisfies $q(v, x, y) \geq 0$ and

$\sum_{x,y} q(v,x,y) = 1$ for all $v \in \mathcal{V}$. We refer to this class of games as *classical* LSSD games.

Throughout this chapter, for clarity, we use subscripts to indicate the marginal probabilities of a distribution—for example, for a probability distribution $q(v,x,y)$ as above, $q_A(x|v)$ denotes the marginal probability for register A conditioned on v. When the context is clear, we omit the subscript for brevity.

6.2.2. Remark. Note that a classical LSSD game $\mathbf{G}$ can equivalently be described by random variables V, X, and Y , taking values in finite sets taking values in the sets $\mathcal{V}, \mathcal{X}$ and $\mathcal{Y}$, respectively, distributed according to q over their Cartesian product. In this formulation, the referee samples a triple $(v,x,y) \in \mathcal{V} \times \mathcal{X} \times \mathcal{Y}$ according to q, sends x and y to Alice and Bob, respectively, and the two players must guess the value of v. That is,

$$\mathbf{G} = \big(V, X, Y, q\big). \tag{6.4}$$

Next, we will see how to evaluate the performance of Alice and Bob when they play a classical LSSD game, i.e. their winning probability, depending on the resources that they have access to. In a classical LSSD game, Alice and Bob receive inputs x, and y, and they have to produce outputs a, and b, respectively. First, we consider the abstract case where they each have access to a 'black box' that takes input x (y) and produces output a (b), and we will consider probability distributions $Q_{AB}(a,b|x,y)$ that these boxes will reproduce. The set $\mathbf{Q} = \{Q_{AB}(a,b|x,y)\}_{x,y,a,b}$ is known in the literature as a *behavior* [BCP+14]. We will analyze the cases where the boxes correspond to classical, quantum, and no-signaling resources (behaviors).

6.2.1 Classical resources

A behavior $\mathbf{Q} = \{Q_{AB}(a,b|x,y)\}_{x,y,a,b}$ is said to be classical [BCP+14] if

$$Q_{AB}(a,b|x,y) = \int_\Lambda \mathrm{d}\lambda \mu(\lambda) Q_A(a|x,\lambda) Q_B(b|y,\lambda), \quad \forall x,y,a,b \tag{6.5}$$

where λ take values in a space Λ according to the probability density $\mu(\lambda)$. The parameter λ, also known as a local hidden variable, has the interpretation of shared randomness, which can be thought of some shared classical random variable that Alice and Bob share, and they use both the input that they received and λ to output a and b, respectively. Then, given a classical LSSD game $\mathbf{G}$, we say that $\mathbf{S}_\mathrm{c} = \{Q_A(a|x,\lambda) Q_B(b|y,\lambda)\}_{x,y,a,b,\lambda}$ is a *classical strategy* for $\mathbf{G}$, and the corresponding winning probability is

$$\omega_\mathrm{c}(\mathbf{G}, \mathbf{S}_\mathrm{c}) = \sum_{v,x,y} q(v,x,y) \int_\Lambda \mathrm{d}\lambda \mu(\lambda) Q_A(a|x,\lambda) Q_B(b|y,\lambda). \tag{6.6}$$

The optimal winning probability can now be obtained by maximizing over all classical correlations of the form (6.5). However, note that the maximum of $\omega_{\mathrm{c}}(\mathbf{G}, \mathbf{S}_{\mathrm{c}})$ over all classical strategies is always achieved by extremal points—namely, by deterministic strategies. These strategies can be described by functions $h_A : \mathcal{X} \to \mathcal{V}$ and $h_B : \mathcal{Y} \to \mathcal{V}$, which uniquely determine the output based on the input each party receives. Then, the optimal (classical) winning probability of a classical LSSD game $\mathbf{G}$ is given by

$$\omega_{\mathrm{c}}(\mathbf{G}) = \sup_{\mathbf{S}_{\mathrm{c}}} \omega_{\mathrm{c}}(\mathbf{G}, \mathbf{S}_{\mathrm{c}}) = \max_{h_A, h_B} \sum_{v,x,y} q(v,x,y) \mathbf{1}_v(h_A(x)) \mathbf{1}_v(h_B(y)), \tag{6.7}$$

where $\mathbf{1}_{\cdot}(*)$ is the indicator function.

Notice that, given a classical LSSD game $\mathbf{G}$, the optimal classical winning probability in (6.7) can be computed by brute force. However, as the sizes of $\mathcal{V}$, $\mathcal{X}$, and $\mathcal{Y}$ increase, the number of deterministic strategies grows, making the optimization task computationally harder. To address this, we now introduce a type of strategies, which we call symmetric, in which Alice and Bob behave identically, and we will later show that such strategies are optimal for all classical LSSD games of a certain form.

6.2.2 Quantum resources

In order to play a classical LSSD game $\mathbf{G} = \big(\{q(v,x,y)\}_{v,x,y}\big)$, the most general thing that Alice and Bo can do using quantum mechanics is to prepare a joint quantum state $\sigma_{A'B'}$ on a Hilbert space $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, where Alice holds register A', and Bob, register B'. In order to obtain classical answers a and b, the most general procedure is to perform POVMs $\{A_a^x\}_a$ and $\{B_b^y\}_b$ on their respective local registers. Then, the probabilities that they obtain are given by

$$Q_{AB}(a,b|x,y) = \mathrm{Tr}\big[\sigma_{A'B'}(A_a^x \otimes B_b^y)\big] \quad \forall x,y,a,b. \tag{6.8}$$

The tuple $\mathbf{S}_{\mathrm{q}} := \{\sigma_{A'B'}, A_a^x, B_b^y\}$ will be called a strategy for $\mathbf{G}$, and the corresponding winning probability is given by

$$\omega_{\mathrm{q}}(\mathbf{G}, \mathbf{S}_{\mathrm{q}}) = \sum_{v,x,y} q(v,x,y) \mathrm{Tr}[\sigma_{A'B'}(A_v^x \otimes B_v^y)], \tag{6.9}$$

and the (optimal) winning probability of $\mathbf{G}$ is the supremum over all possible strategies (over all possible dimensions):

$$\omega_{\mathrm{q}}(\mathbf{G}) = \sup_{\mathbf{S}_{\mathrm{q}}} \omega_{\mathrm{q}}(\mathbf{G}, \mathbf{S}_{\mathrm{q}}). \tag{6.10}$$

6.2.3 No-signaling resources

A behavior $\mathbf{Q} = \{Q_{AB}(a,b|x,y)\}_{x,y,a,b}$ is said to be no-signaling [BCP+14], if it satisfies the following:

$$\begin{aligned} \sum_b Q_{AB}(a,b|x,y) &= \sum_b Q_{AB}(a,b|x,y') \ \forall a,x,y,y', \text{ and} \\ \sum_a Q_{AB}(a,b|x,y) &= \sum_a Q_{AB}(a,b|x,y') \ \forall b,y,x,x'. \end{aligned} \tag{6.11}$$

Note that classical and quantum correlations (behaviors) have a clear physical interpretation—namely, they can, in principle, be implemented in a laboratory. In contrast, no-signaling correlations are primarily a mathematical construct without physical realization. Nevertheless, they serve as a powerful analytical tool, for instance, to upper bound the strength of quantum correlations in a more tractable way (see below). The constraints in (6.11) express the requirement that the correlations cannot be influenced by the other party's choice of measurement. This captures the principle that no information can be transmitted instantaneously, thereby preserving consistency with the relativistic constraint that nothing can travel faster than the speed of light. As a result, any physically realizable behavior must, in particular, satisfy the no-signaling conditions.

Given a classical LSSD game $\mathbf{G}$, we say that $\mathbf{S}_{\text{ns}} = \{Q_{AB}(a,b|x,y)\}_{x,y,a,b}$ is a *no-signaling strategy* for $\mathbf{G}$, where (6.11) are fulfilled, and the corresponding winning probability is

$$\omega_{\text{ns}}(\mathbf{G},\mathbf{S}_{\text{ns}}) = \sum_{v,x,y} q(v,x,y) Q_{AB}(a,b|x,y), \tag{6.12}$$

and the (optimal) winning probability of $\mathbf{G}$ is the supremum over all possible no-signaling strategies:

$$\omega_{\text{ns}}(\mathbf{G}) = \sup_{\mathbf{S}_{\text{ns}}} \omega_{\text{ns}}(\mathbf{G},\mathbf{S}_{\text{ns}}). \tag{6.13}$$

The set of classical correlations (behaviors) is a subset of the set of quantum correlations, and the latter is a subset of the set of no-signaling correlations, see [BCP+14] for more details. Therefore, we have that, for every classical LSSD game $\mathbf{G}$,

$$\omega_{\text{c}}(\mathbf{G}) \leq \omega_{\text{q}}(\mathbf{G}) \leq \omega_{\text{ns}}(\mathbf{G}). \tag{6.14}$$

Note that the winning probability for a given no-signaling strategy (6.13) is a linear function in the values $Q_{AB}(a,b|x,y)$. This, together with the fact that the set of no-signaling correlations forms a convex polytope, see e.g. [BCP+14], implies that we can use linear programming to find the optimal no-signaling winning probability of an LSSD game. This last fact is what Majenz et al. used to prove that there exists no probability distribution q with binary v, x and y, such that the corresponding LSSD game can be won with higher probability using no-signaling strategies [MOST24, Proposition 3.3]. They showed that none of the

no-signaling correlations at the extreme points of the no-signaling polytope could ever perform better than the simple classical strategy of outputting the most likely value for v.

6.3 Structured classical LSSD games

In this section we identify two families of classical LSSD games that share useful structural properties. For each family we will establish general results on the optimal winning probabilities achievable with (i) classical strategies and (ii) the more powerful no-signaling correlations. A concrete example that belongs to both families—the binary-symmetric-channel game—will be examined in detail later, in Section 6.4.

6.3.1. Definition. *A classical LSSD game* $\mathbf{G} = \{q(v,x,y)\}_{v,x,y}$ *is called* product-symmetric *if it satisfies the following conditions:*

(i) The marginal distribution over $\mathcal{V}$ *is uniform, i.e.* $\sum_{x,y} q(v,x,y) = \frac{1}{|\mathcal{V}|}$, $\forall v$.

(ii) The conditional distribution $q(x,y|v)$ *factorizes as* $q_A(x|v)q_B(y|v)$.

(iii) The marginals satisfy $q_A(\cdot|v) = q_B(\cdot|v)$.

We now introduce a type of classical strategies that will be relevant for the product-symmetric classical LSSD games.

6.3.2. Definition. *A classical strategy* $\mathbf{S}_c$ *is said to be* symmetric *if Alice and Bob apply the same local function, i.e. if* $h_A = h_B$. *In this case, we will write* $\mathbf{S}_c = \{h_A, h_A\}$.

6.3.3. Theorem. *For every product-symmetric classical LSSD game* $\mathbf{G}$*, its optimal classical winning probability* $\omega_c(\mathbf{G})$ *is attained by a deterministic symmetric strategy. That is,*

$$\omega_c(\mathbf{G}) = \max_{h_A:\mathcal{X}\to\mathcal{V}} \omega_c(\mathbf{G}, \{h_A, h_A\}). \tag{6.15}$$

Proof:
Let $h_A : \mathcal{X} \to \mathcal{V}$ and $h_B : \mathcal{Y} \to \mathcal{V}$ define a deterministic strategy. We will see that either Alice and Bob both performing h_A or both performing h_B can only increase the winning probability. Let $\mathbf{S}_c = \{h_A, h_B\}$ be the strategy described by h_A and h_B, then

$$\begin{aligned}
\omega_c(\mathbf{G}, \mathbf{S}_c) &= \sum_{v,x,y} q(v,x,y)\delta[h_A(x) = h_B(y) = v] \\
&= \frac{1}{|\mathcal{V}|} \sum_{v,x,y} q_{AB}(x,y|v)\delta[h_A(x) = h_B(y) = v] \\
&= \frac{1}{|\mathcal{V}|} \sum_v \left(\sum_x q_A(x|v)\delta[h_A(x) = v] \right) \left(\sum_{x'} q_A(x'|v)\delta[h_B(x') = v] \right),
\end{aligned} \tag{6.16}$$

where in the first equality we used assumptions (i) and (ii) of Theorem 6.3.3, and in the last inequality, we used hypothesis (iii). Now, let

$$\alpha_v \coloneqq \sum_x q_A(x|v)\delta[h_A(x) = v] \quad \text{and} \quad \beta_v \coloneqq \sum_{x'} q_A(x'|v)\delta[h_B(x') = v], \tag{6.17}$$

and consider the column vectors $\boldsymbol{\alpha} = (\alpha_{v_1}, \ldots, \alpha_{v_{|\mathcal{V}|}})^\mathsf{T}$ and $\boldsymbol{\beta} = (\beta_{v_1}, \ldots, \beta_{v_{|\mathcal{V}|}})^\mathsf{T}$, then, we have that

$$\omega_{\mathrm{c}}(\mathbf{G}, \mathbf{S}_{\mathrm{c}}) = \frac{1}{|\mathcal{V}|}\sum_v \alpha_v\beta_v = \frac{1}{|\mathcal{V}|}\langle\boldsymbol{\alpha}, \boldsymbol{\beta}\rangle. \tag{6.18}$$

Then, using the Cauchy–Schwarz inequality,

$$\begin{aligned}\omega_{\mathrm{c}}(\mathbf{G}, \mathbf{S}_{\mathrm{c}}) &= \frac{1}{|\mathcal{V}|}\sqrt{|\langle\boldsymbol{\alpha}, \boldsymbol{\beta}\rangle|^2} \leq \frac{1}{|\mathcal{V}|}\sqrt{\langle\boldsymbol{\alpha}, \boldsymbol{\alpha}\rangle\langle\boldsymbol{\beta}, \boldsymbol{\beta}\rangle} \\ &\leq \frac{1}{|\mathcal{V}|}\max_{\alpha,\beta}\{\langle\boldsymbol{\alpha}, \boldsymbol{\alpha}\rangle, \langle\boldsymbol{\beta}, \boldsymbol{\beta}\rangle\} = \max\{\omega_{\mathrm{c}}(\mathbf{G}, \mathbf{S}_{\mathrm{c}}^A), \omega_{\mathrm{c}}(\mathbf{G}, \mathbf{S}_{\mathrm{c}}^B)\},\end{aligned} \tag{6.19}$$

where $\mathbf{S}_{\mathrm{c}}^A = \{h_A, h_A\}$ and $\mathbf{S}_{\mathrm{c}}^B = \{h_B, h_B\}$. Therefore, the optimal value $\omega_{\mathrm{c}}(\mathbf{G})$ will be attained by the maximum over symmetric strategies, in particular, by a symmetric strategy: $\omega_{\mathrm{c}}(\mathbf{G}) = \max_{h_A:\mathcal{X}\to\mathcal{V}} \omega_{\mathrm{c}}(\mathbf{G}, \{h_A, h_A\})$. □

We now define a similar concept to product-symmetric LSSD games.

6.3.4. Definition. *A classical LSSD game $\mathbf{G} = \{q(v, x, y)\}_{v,x,y}$, with $\mathcal{X} = \mathcal{Y}$, is called* channel *LSSD game if it satisfies the following conditions:*

(i) The marginal distribution over $\mathcal{V}$ is uniform, i.e. $\sum_{x,y} q(v, x, y) = \frac{1}{|\mathcal{V}|}\ \forall v$.

(ii) The joint distribution $q(v, x, y)$ factorizes as $q_V(v)q_A(x|v)q_B(y|v)$.

(iii) The marginals satisfy $q_A(\cdot|v) = q_B(\cdot|v)$.

Condition (ii) makes explicit that, conditional on the referee's choice v, the pair (x, y) arises from two independent uses of the *same* classical channel $q_A(\cdot|v) = q_B(\cdot|v)$; this motivates the term "channel LSSD game."

Given a channel LSSD game $\mathbf{G}$, we show a statement regarding its m-fold parallel repetition, denoted by $\mathbf{G}^{\times m}$. To this end, for a permutation $\sigma \in S_m$ and a sequence $x^m \in \mathcal{X}^m$, we denote by $\sigma(x^m) \in \mathcal{X}^m$ the sequence obtained from x^m by permuting its entries according to σ.

6.3.5. Lemma. *Let $\mathbf{G}$ be a channel LSSD game. Then, there exists an optimal no-signaling strategy Q for its n-fold parallel repetition $\mathbf{G}^{\times n}$ such that*

$$\forall\sigma \in S_m: \quad Q(\sigma(a^m), \sigma(b^m)|\sigma(x^m), \sigma(x^m)) = Q(a^m, b^m|x^m, y^m). \tag{6.20}$$

Proof:
Let Q be an optimal strategy for $\mathbf{G}^{\times n}$, and $\sigma \in S_m$. The strategy Q_σ defined by $Q_\sigma(a^m, b^m|x^m, y^m) = Q(\sigma(a^m), \sigma(b^m)|\sigma(x^m), \sigma(y^m))$ has the same winning probability as Q, since the n-fold probability distribution is invariant under permutations: $q^{\times n}(v^n, x^m, y^m) = q^{\times n}(\sigma(v^n), \sigma(x^m), \sigma(y^m))$. We define

$$\hat{Q} := \frac{1}{m!} \sum_{\sigma \in S_m} Q_\sigma.$$

The strategy $\hat{Q}$ satisfies (6.20): for any $\tau \in S_m$,

$$\begin{aligned}
\hat{Q}(\tau(a^m), \tau(b^m)|\tau(x^m), \tau(y^m)) &= \frac{1}{m!} \sum_{\sigma \in S_m} Q_\sigma(\tau(a^m), \tau(b^m)|\tau(x^m), \tau(y^m)) \\
&= \frac{1}{m!} \sum_{\sigma \in S_m} Q(\sigma(\tau(a^m)), \sigma(\tau(b^m))|\sigma(\tau(x^m)), \sigma(\tau(y^m))) \\
&= \frac{1}{m!} \sum_{\pi \in S_m} Q(\pi(a^m), \pi(b^m)|\pi(x^m), \pi(y^m)) \\
&= \frac{1}{m!} \sum_{\pi \in S_m} Q_\pi(a^m, b^m|x^m, y^m) = \hat{Q}(a^m, b^m|x^m, y^m).
\end{aligned}$$

Finally, by linearity of the winning probability, $\hat{Q}$ also achieves the same winning probability as Q, which means that it is optimal. □

6.4 The binary-symmetric-channel game

In this section, we will analyze a representative of both product-symmetric and channel games: the BSC game. A binary symmetric channel (BSC) with error $\alpha \in [0, 1/2]$ is a channel with a single bit of input that transmits the bit without error with probability $1 - \alpha$ and flips it with probability α, see Figure 6.2. In this section, we study a particular LSSD problem: the binary-symmetric-channel game, originally introduced in [MOST24, Example 1], where a referee sends a bit to Alice and Bob over two identical and independent binary symmetric channels, both with error probability α, see Definition 6.4.1 for a formal definition. In [MOST24], an explicit optimal classical strategy for this game is shown and its corresponding optimal winning probability for every α is obtained. Moreover, the authors show that the winning probability cannot be improved by any quantum nor no-signaling strategy. In addition, they show that if two copies of the game are played in parallel for $\alpha = 1 - \frac{1}{\sqrt{2}}$, there is an explicit optimal classical strategy that performs better than repeating the optimal classical strategy for a single copy of the game twice and, as a consequence, quantum and no-signaling optimal strategies must perform better than repeating the respective optimal strategies for a single copy of the game.

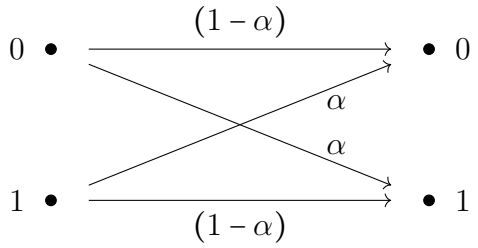


Figure 6.2: Schematic representation of a binary symmetric channel with error probability α.

In Section 6.4.1, we study the parallel repetition of the BSC game and, for the case of two copies, we provide the optimal classical, quantum and no-signaling values, showing that for most α the three values coincide (and in most of the cases the optimal values are obtained just by repeating the optimal strategy for a single copy of the BSC game). Nevertheless, for certain values of α, the classical and quantum values coincide but there is a no-signaling advantage. In Section 6.4.2, we provide the optimal no-signaling winning probabilities for the three-fold parallel repetition of the BSC game.

6.4.1. Definition (Example 1 in [MOST24]). *Let $\mathcal{V} = \mathcal{X} = \mathcal{Y} = \{0,1\}$, $\alpha \in [0,1/2]$, and let N_A and N_B be independent random variables taking values in $\{0,1\}$ with $\Pr[N_A = 1] = \Pr[N_B = 1] = \alpha$. The* binary-symmetric-channel *(BSC) game $\mathbf{G}_{\alpha-BCS} = (V, X, Y, q^\alpha)$ is the classical LSSD game described by the random variables V, uniformly distributed over $\mathcal{V}$, and $X := V \oplus N_A$ and $Y := V \oplus N_B$. This fully specifies the joint distribution q^α over $\mathcal{V} \times \mathcal{X} \times \mathcal{Y}$.*

6.4.2. Proposition (Example 1 in [MOST24]). *For every $\alpha \in [0,1/2]$, the optimal classical, quantum and no-signaling winning probabilities for the $\mathbf{G}_{\alpha-BCS}$ game are equal and given by*

$$\omega_{\mathrm{c}}(\mathbf{G}_{\alpha-BCS}) = \omega_{\mathrm{q}}(\mathbf{G}_{\alpha-BCS}) = \omega_{\mathrm{ns}}(\mathbf{G}_{\alpha-BCS}) = \begin{cases} (1-\alpha)^2 & \text{if } \alpha \in [0, 1-\frac{1}{\sqrt{2}}], \\ \frac{1}{2} & \text{if } \alpha \in (1-\frac{1}{\sqrt{2}}, \frac{1}{2}]. \end{cases} \tag{6.21}$$

The optimal winning probability for $\alpha \in [0, 1-1/\sqrt{2}]$ is achieved by the strategy where Alice and Bob output the input they received. The intuition behind this strategy is that for 'small' α, the bits they receive most likely have not been flipped. Notice that if Alice and Bob were playing this game without having to coordinate their answers, such a strategy would be optimal for all α. In fact, the optimal strategy for 'high'-noise BSC channels, $\alpha \in (1-1/\sqrt{2}, 1/2]$, is achieved by both parties outputting some previously agreed bit.

6.4.1 Two-fold parallel repetition of the BSC game

Let (V', X', Y') be an independent copy of (V, X, Y), as described in Definition 6.4.1. The two-fold parallel repetition of the $\mathbf{G}_{\alpha\text{–BCS}}$ game, denoted by $\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}$, consists of simultaneously guessing (V, V') from (X, X') and (X, X'). This game is described by the probability distribution $q^\alpha \otimes q^\alpha$. According to [MOST24], the optimal classical winning probability for the two-fold parallel repetition of the BSC game for $\alpha = 1 - \frac{1}{\sqrt{2}}$ is

$$\omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) = \frac{1}{4}(1-\alpha^2)^2 + \frac{1}{4}(1-\alpha)^4. \tag{6.22}$$

Hence, for $\alpha = 1 - \frac{1}{\sqrt{2}}$, $\omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) > \omega_{\mathrm{c}}(\mathbf{G}_{\alpha\text{–BCS}})^2$ and, from (6.14) and (6.21), we also have

$$\omega_{\mathrm{q}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) > \omega_{\mathrm{q}}(\mathbf{G}_{\alpha\text{–BCS}})^2, \qquad \omega_{\mathrm{ns}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) > \omega_{\mathrm{ns}}(\mathbf{G}_{\alpha\text{–BCS}})^2. \tag{6.23}$$

Here we study the full range of α (namely, $\alpha \in [0, 1/2]$). In the following theorem, we provide the optimal classical and no-signaling winning probabilities for the two-fold parallel repetition of the BSC game, graphically represented in Figure 6.3. The theorem shows that for most values of α, the classical and no-signaling optimal success probabilities coincide (and therefore so does the quantum value).

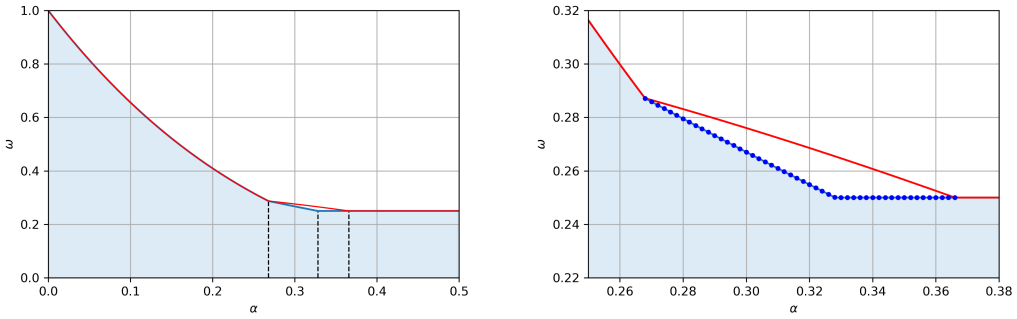
6.4.3. Theorem. *Let $\alpha_0 < 1$ be the real solution of $(1-\alpha^2)^2 + (1-\alpha)^4 = 1$, i.e. $\alpha_0 \simeq 0.32814$, and let $I_1 = [0, 2-\sqrt{3}]$, $I_2 = (2-\sqrt{3}, \alpha_0]$, $I_3 = (\alpha_0, \frac{\sqrt{3}-1}{2}]$ and $I_4 = (\frac{\sqrt{3}-1}{2}, \frac{1}{2}]$. Then, for the two-fold parallel repetition of the BSC game, $\mathbf{G}^{\times 2}_{\alpha\text{–}BCS}$, we have*

$$\omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha\text{–}BCS}) = \begin{cases} (1-\alpha)^4 & \text{if } \alpha \in I_1, \\ \frac{1}{4}(1-\alpha^2)^2 + \frac{1}{4}(1-\alpha)^4 & \text{if } \alpha \in I_2, \\ \frac{1}{4} & \text{if } \alpha \in I_3 \cup I_4, \end{cases} \tag{6.24}$$

and

$$\omega_{\mathrm{ns}}(\mathbf{G}^{\times 2}_{\alpha\text{–}BCS}) = \begin{cases} (1-\alpha)^4 & \text{if } \alpha \in I_1, \\ \frac{(1-\alpha^2)^2}{3} & \text{if } \alpha \in I_2 \cup I_3, \\ \frac{1}{4} & \text{if } \alpha \in I_4. \end{cases} \tag{6.25}$$

Proof:
Since the BSC game fulfills the conditions of Theorem 6.3.3, a symmetric strategy will provide the optimal classical value. We determine ω_{c} by considering all deterministic classical strategies. For each strategy, we compute the winning probability as a function of α. Then we obtain the analytical value (6.24) by taking the maximum and applying the `PiecewiseExpand` command in *Mathematica*. For more details on this derivation, see the *Mathematica* file "`BSC classical strategy n=2.nb`" in [HEFO24].



(a) (b)

Figure 6.3: (a) Optimal classical (blue) and no-signaling (red) winning probabilities for the two-fold parallel repetition of the BSC game. The light blue area represents the values below the optimal classical winning probability. (b) Closeup of (a) with an additional numerical upper bound on the optimal quantum winning probability (blue dots) from the level '$1+AB$' of the NPA hierarchy for the values of α where the classical and no-signaling values differ. The numerical quantum upper bound is in excellent agreement with the classical value, suggesting its optimality (see Theorem 6.4.4).

The optimal no-signaling value can be found via a linear program, i.e. a maximization of a linear function subject to linear constraints. For completeness, we recall the primal and dual formulations introduced in Chapter 2. In *Mathematica*, the standard form to represent a linear program that optimizes over $x \in \mathbb{R}^n$ is

$$\begin{aligned} \textit{Primal problem:} \qquad & \text{minimize: } \langle c, x\rangle = \sum_{i=1}^{n} c_i x_i \\ & \text{subject to: } Ax + b \geq 0, \\ & \qquad\qquad A_{\text{eq}} x + b_{\text{eq}} = 0, \end{aligned} \tag{6.26}$$

where $x, c \in \mathbb{R}^n$, $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$, $A_{\text{eq}} \in \mathbb{R}^{k\times n}$, $b_{\text{eq}} \in \mathbb{R}^k$ (see `LinearOptimization` for more details). Its dual, which optimizes over $\lambda \in \mathbb{R}^m$ and $\nu \in \mathbb{R}^k$, is given by

$$\begin{aligned} \textit{Dual problem:} \qquad & \text{maximize: } -\left(\langle b, \lambda\rangle + \langle b_{\text{eq}}, \nu\rangle\right) = -\sum_{i=1}^{m} b_i \lambda_i - \sum_{i=1}^{k} b_{\text{eq},i} \nu_i \\ & \text{subject to: } A^{\mathsf{T}}\lambda + A_{\text{eq}}^{\mathsf{T}}\nu - c = 0, \\ & \qquad\qquad \lambda \geq 0. \end{aligned} \tag{6.27}$$

A common technique in linear programming is to use one of the two problems to obtain a bound on the other. In the above formulation, any feasible solution to the dual problem (6.27) provides a lower bound on the optimal solution of the primal problem (6.26). The optimal value of both problems can be determined

by finding feasible primal and dual solutions that have the same value. Then, as a consequence of strong duality, both solutions must be optimal.

Since the original linear program for computing ω_{ns} for the BSC game is quite large, see (6.11), and (6.12), we first simplify it by reducing the number of parameters. We do this by imposing the following symmetries on Alice's and Bob's no-signaling strategy Q:[1]

1. By Lemma 6.3.5, there is an optimal no-signaling strategy that is invariant under any permutation of the instances of the game, i.e. $Q(\sigma(a), \sigma(b)|\sigma(x), \sigma(y)) = Q(a, b|x, y)$, for any permutation σ of positions within a string.

2. Since the BSC game is symmetric under exchanging Alice and Bob, we can also exchange Alice's and Bob's strategies, i.e. $Q(b, a|y, x) = Q(a, b|x, y)$.

3. Since the BSC game is symmetric under negating any subset of input and output bits, we can do the same to Alice's and Bob's strategy, i.e. $Q(a \oplus s, b \oplus s|x \oplus s, y \oplus s) = Q(a, b|x, y)$ for any bit string s.

After performing the above symmetry reductions, we need to find feasible primal and dual solutions of equal value. These solutions should be α-dependent, i.e. work not just for a single value of α but for whole intervals of α. We found such solutions with the help of *Mathematica*, and we have provided them in the format of (6.26) and (6.27) in the notebook "`BSC no-signaling strategy n=2.nb`" [HEFO24]. The primal and dual objective values of these solutions match and agree with (6.25) in each of the intervals $I_1, \ldots, I_4$ (occasionally we could not obtain a single α-dependent solution for a whole interval, in which case we broke it into smaller subintervals).

While it is easy to solve the linear program for any particular value of α, obtaining continuous α-dependent solutions is nontrivial—it requires interpolating from a small number of solutions, or often even a single solution. We used a combination of the following numerical tricks to cover all cases in (6.25) (often obtaining the same solution with different methods):

- *Rational multiples of* π: We chose a rational number r so that $\alpha = r\pi$ lies in a given interval I_i. Using `LinearOptimization` we then find a symbolic solution that is polynomial in π.[2] Substituting back $\pi = \alpha/r$ gives us an exact polynomial α-dependent solution. This strategy unfortunately did not work for 3 repetitions of the game since the linear program was too large.

[1] Here we consider only two parallel repetitions of the BSC game. But the same symmetry reductions can be performed for any number of repetitions (see Theorem 6.4.5).

[2] This works since on the one hand *Mathematica* treats π symbolically, on the other hand, it can compare π to any other number by calculating its numerical value to arbitrary accuracy. It is also important that *Mathematica* can manipulate rational numbers symbolically.

- *Rational solutions*: We choose a sequence of equally spaced rational values of α and find exact rational solutions for these values by using `LinearOptimization`. We then interpolate between them by using `FindSequenceFunction`. This method generally requires some fiddling with the chosen sequence since nearby values of α can lead to completely different and unrelated solutions.

- *Algebraic solutions*: We choose an algebraic α from the given interval I_i and find a numerical solution for this α to extremely high accuracy (300 digits). Then we use `RootApproximant` to turn this numerical solution into exact algebraic numbers. Reconstructing the minimal polynomial for each of these numbers gives us an interpolated α-dependent solution that is polynomial. This trick effectively interpolates from a single algebraic point.

Checking the primal and dual constraints of the resulting interpolated solution gives us constraints on α that capture the interval in which this solution holds.

It is important to note that, irrespective of how convoluted the above numerical methods are, once an exact α-dependent solution is found, it can be easily verified that it satisfies all constraints and gives equal primal and dual values, hence implying optimality. For more details, see "`BSC no-signaling strategy n=2.nb`" in [HEFO24]. □

Notice that, unlike a single copy of the BSC game, the optimal winning probabilities have different behaviors split into three different intervals. We see that

$$\omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) = \omega_{\mathrm{ns}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) = \omega_{\mathrm{c}}(\mathbf{G}_{\alpha\text{–BCS}})^2 \ \ \forall \alpha \in I_1 \cup I_4, \tag{6.28}$$

and therefore, due to (6.14), the quantum value is the same value as the classical. Analogously to the single copy of the BSC game, for 'small' α, $\alpha \in I_1$, an optimal classical and no-signaling strategy is given by Alice and Bob outputting their input. The intuition behind it is that, due to 'low' noise, every bit has low probability of being flipped, $(1-\alpha)$, and thus the winning probability using this strategy is $(1-\alpha)^4$. On the other hand, an optimal classical and no-signaling strategy for a 'high' noisy channel, $\alpha \in I_3 \cup I_4$ and $\alpha \in I_4$, respectively, is that both Alice and Bob output some previously agreed bit string. This leads to the conclusion that the corresponding optimal winning probabilities for these values of α can be achieved by just repeating the optimal classical and no-signaling strategies mentioned above for a single copy of the BSC game. Nevertheless, this is not always the case, since

$$\omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) < \omega_{\mathrm{ns}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}}) \quad \forall \alpha \in I_2 \cup I_3. \tag{6.29}$$

An optimal classical strategy for $\alpha \in I_2$ is given by Alice and Bob both outputting 00 if their input contains a 0 and outputting 11, otherwise, which gives an optimal

winning probability of $\frac{1}{4}(1-\alpha^2)^2+\frac{1}{4}(1-\alpha)^4$, which was already given in [MOST24] for $\alpha = 1-\frac{1}{\sqrt{2}}$. An optimal no-signaling strategy for $\alpha \in I_2 \cup I_3$ is given by

$$Q_{AB}(a,b|x,y) = \begin{cases} \frac{1}{3} & \text{if } (a=b \text{ or } a\oplus y = 11 = b\oplus x) \text{ and } (a\oplus ax \neq 11 \neq b\oplus y), \\ 0 & \text{otherwise.} \end{cases}$$

This strategy has winning probability $(1-\alpha^2)^2/3$. More specifically, for $\alpha \in I_2$ and for $\alpha \in I_2 \cup I_3$ there exist classical and no-signaling strategies, respectively, that perform better than repeating the optimal strategy, i.e.

$$\begin{aligned} \omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha-\mathrm{BCS}}) &> \omega_{\mathrm{c}}(\mathbf{G}_{\alpha-\mathrm{BCS}})^2 \qquad \forall \alpha \in I_2, \\ \omega_{\mathrm{ns}}(\mathbf{G}^{\times 2}_{\alpha-\mathrm{BCS}}) &> \omega_{\mathrm{ns}}(\mathbf{G}_{\alpha-\mathrm{BCS}})^2 \qquad \forall \alpha \in I_2 \cup I_3. \end{aligned} \tag{6.30}$$

We are left with characterizing the value $\omega_{\mathrm{q}}(\mathbf{G}^{\times 2}_{\alpha-\mathrm{BCS}})$ for $\alpha \in I_2 \cup I_3$. From (6.29), the optimal quantum value for $\alpha \in I_2 \cup I_3$ has to be in between the two values. Based on strong numerical evidence (see Figure 6.3), in Theorem 6.4.4 below we conjecture that there is no quantum advantage with respect to the optimal classical strategy for any α.

Unlike the set of classical and the set of no-signaling correlations, the set of quantum correlations of the form (6.8), $\mathcal{Q}$, has uncountably many extremal points, see e.g. [BCP+14], making the optimization problem a tough task. As introduced in Section 2.4, in [NPA08], Navascués, Pironio and Acín (NPA) introduced an infinite hierarchy of conditions necessarily satisfied by any set of quantum correlations with the property that each of them can be tested using semidefinite programming (SDP) and thus they can be used to exclude non-quantum correlations, see Section 2.4. In short, as stated in Chapter 3, the authors introduced a recursive way to construct subsets $\mathcal{Q}_\ell \supset \mathcal{Q}_{\ell+1} \supset \mathcal{Q}$ for all $\ell \in \mathbb{N}$, such that each of them can be tested using semidefinite programming and are such that $\cap_{\ell\in\mathbb{N}}\mathcal{Q}_\ell = \mathcal{Q}_{co}$, where $\mathcal{Q}_{co} \supset \mathcal{Q}$ is the set of probabilities as described in Section 6.2.2 but instead of Alice and Bob performing measurements in a tensor product, they perform measurements which commute in a joint Hilbert space. For finite dimensional Hilbert spaces, both sets are equivalent.

By using an intermediate level between the first and the second levels of the NPA hierarchy, the so-called level "$1+AB$" (see "`NPA_hierarchy_BSC_Game.py`" [HEFO24] for the numerical code), as used in Chapter 3, we find that for $\alpha \in I_2$, $\omega_{\mathrm{q}}(\mathbf{G}^{\times 2}_{\alpha-\mathrm{BCS}})$ is upper bounded by $\omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha-\mathrm{BCS}})$, see Figure 6.3 (b). Therefore, this shows that the values coincide in the interval I_2. The reason to restrict ourselves to the level "$1+AB$" is that it requires less computational resources than computing the level 2 and it already provides tight bounds. Based on the fact that the numerical upper bounds on the quantum value obtained by solving the semidefinite programs match the (analytical) lower bounds given by the classical values, we state the following conjecture.

6.4.4. Result. *There is no quantum advantage over the best classical strategy for the two-fold parallel repetition of the BSC game $\mathbf{G}^{\times 2}_{\alpha-BCS}$ for any value of α.*

6.4.2 Three-fold parallel repetition of the BSC game

Consider the three-fold parallel repetition of the BSC game, denoted by $\mathbf{G}^{\times 3}_{\alpha-\mathrm{BCS}}$. In the following theorem, we provide the optimal classical and no-signaling winning probabilities, and we will see that for a vast range of values of α they coincide and therefore so does the quantum winning probability.

6.4.5. THEOREM. *Let α_1 be the root of the polynomial $2(1-\alpha)^4(1+2\alpha)-1$ taking the value $\alpha_1 \simeq 0.358121$, $\alpha_2 = \frac{1}{8}(3-\sqrt{7}+\sqrt{2(32-11\sqrt{7})})$ and $\alpha_3 = 2^{-\frac{2}{3}}(4-\sqrt{14})^{\frac{1}{3}}$. Then, for three copies of the BSC game,*

$$\omega_{\mathrm{c}}(\mathbf{G}^{\times 3}_{\alpha-BCS}) = \begin{cases} (1-\alpha)^6 & \text{if } \alpha \in [0, \frac{1}{4}], \\ \frac{1}{4}(1-\alpha)^4(1+2\alpha) & \text{if } \alpha \in (\frac{1}{4}, \alpha_1], \\ \frac{1}{8} & \text{if } \alpha \in (\alpha_1, \frac{1}{2}], \end{cases} \tag{6.31}$$

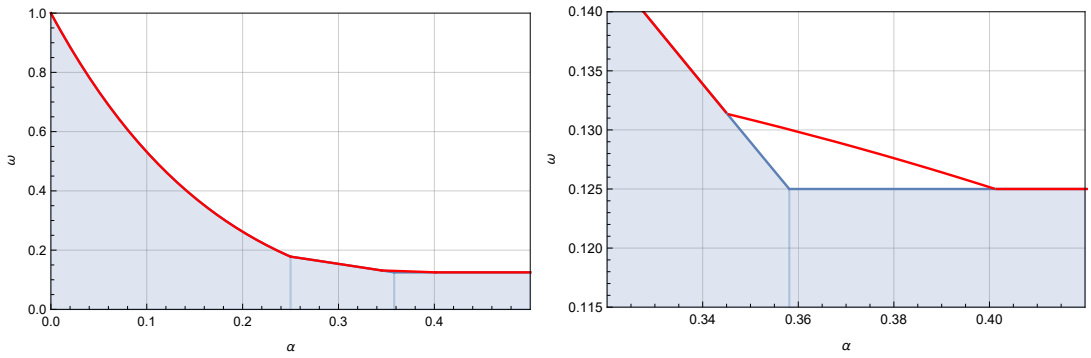
$$\omega_{\mathrm{ns}}(\mathbf{G}^{\times 3}_{\alpha-BCS}) = \begin{cases} (1-\alpha)^6 & \text{if } \alpha \in [0, \frac{1}{4}] =: J_1, \\ \frac{1}{4}(1-\alpha)^4(1+2\alpha)^2 & \text{if } \alpha \in (\frac{1}{4}, \alpha_2] =: J_2, \\ \frac{1}{7}(1-\alpha^3)^2 & \text{if } \alpha \in [\alpha_2, \alpha_3] =: J_3, \\ \frac{1}{8} & \text{if } \alpha \in [\alpha_3, \frac{1}{2}] =: J_4. \end{cases} \tag{6.32}$$

Proof:
The proof is analogous to the proof of Theorem 6.4.3 for two parallel repetitions. In "`BSC classical strategy n=3.nb`" [HEFO24] we perform an optimized search over all symmetric classical strategies leading to (6.31). In "`BSC no-signaling strategy n=3.nb`" [HEFO24] we provide explicit analytic α-dependent solutions for the primal and dual linear programs for the no-signaling value. Both solutions have identical objective value that agrees with (6.32). □

See Figure 6.4 for a graphical representation of the optimal values from Theorem 6.4.5. For 'low' noise, $\alpha \in J_1$, the optimal value is achieved by the classical strategy where Alice and Bob simply output the received bit—i.e. they repeat three times the optimal classical strategy for a single instance of the game. On the other side, for 'high' noise, $\alpha \in J_4$, the optimal value is attained by the classical strategy where Alice and Bob output a pre-agreed bit, which is also obtained by repeating the optimal strategy for a single copy. Therefore,

$$\omega_{\mathrm{c}}(\mathbf{G}^{\times 3}_{\alpha-\mathrm{BCS}}) = \omega_{\mathrm{ns}}(\mathbf{G}^{\times 3}_{\alpha-\mathrm{BCS}}) = \omega_{\mathrm{c}}(\mathbf{G}^{\times 3}_{\alpha-\mathrm{BCS}})^3, \ \forall \alpha \in J_1 \cup J_4. \tag{6.33}$$

For $\alpha \in J_2$, the no-signaling optimal value can be attained by the deterministic strategy consisting on Alice and Bob outputting 111 if they receive an input with more zeros than ones and outputting 000 otherwise. For this interval, the optimal



(a) (b)

Figure 6.4: (a) Optimal classical (blue) and no-signaling (red) winning probabilities for the three-fold parallel repetition of the BSC game, $\mathbf{G}^{\times 3}_{\alpha\text{–BCS}}$. The blue area represents the values below the optimal classical winning probabilities. (b) Zoom in of (a) for the values of α around 0.37 where the classical and no-signaling values differ.

strategy for three copies is better than any combination of optimal two and one copies of the BSC game, i.e.

$$\begin{aligned}&\omega_{\mathrm{c}}(\mathbf{G}^{\times 3}_{\alpha\text{–BCS}}) = \omega_{\mathrm{ns}}(\mathbf{G}^{\times 3}_{\alpha\text{–BCS}}) > \omega_{\mathrm{ns}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}})\omega_{\mathrm{ns}}(\mathbf{G}_{\alpha\text{–BCS}})\\ &\geq \omega_{\mathrm{c}}(\mathbf{G}^{\times 2}_{\alpha\text{–BCS}})\omega_{\mathrm{c}}(\mathbf{G}_{\alpha\text{–BCS}}) > \omega_{\mathrm{ns}}(\mathbf{G}_{\alpha\text{–BCS}})^3, \ \ \forall \alpha \in J_2.\end{aligned} \tag{6.34}$$

For $\alpha \in J_3$ the following no-signaling strategy achieves the optimal value

$$Q_{AB}(a,b|x,y) = \begin{cases} \frac{1}{7} & \text{if } (a = b \text{ or } x \oplus y = 111 = b \oplus x) \text{ and } (a \oplus x \neq 111 \neq b \oplus y), \\ 0 & \text{otherwise.} \end{cases} \tag{6.35}$$

Chapter 7

Parallel repetition of the routing protocol

In this chapter, we turn from the non-local games of the previous chapters—where distant players coordinated *classical* answers—to a setting in which their output must itself be a *quantum state*. We introduce and analyze the *quantum cloning game*: $\hbar$ spatially separated players receive the same classical question that designates one of them, and the chosen player must end the round sharing a maximally entangled EPR pair with a quantum referee. We first determine the optimal success probability for arbitrary quantum strategies. Then, for the relevant case of two players (Alice and Bob) we further show that this success probability decays exponentially when the game is repeated m times in parallel.

The quantum cloning game then becomes the central tool for our study of the *routing quantum position-verification (QPV) protocol* in the *No Pre-shared Entanglement* model. In the routing protocol, the prover must return a qubit to one of two verifiers, with the choice dictated by classical information. Leveraging the cloning-game bound, we give a tight attack on a single round of the protocol. More importantly, we prove that when the protocol is executed in parallel—so that the verifiers interact with the prover only once—its soundness decreases exponentially as a function of the number of repetitions, provided the adversaries possess no prior entanglement.

The results presented in this chapter are based on the following paper:

- "A quantum cloning game with applications to quantum position verification", by Léo Colisson Palais, Llorenç Escolà-Farràs, and Florian Speelman, accepted for publication in the proceedings of *TQC 2025* [EFHO+25].

7.1 Introduction

Non-local correlations are a core theme throughout this thesis. They have become a central topic in quantum information science, both from a foundational perspective [BCP+14] and in applications to cryptography and computation [ABG+07, PAM+10, BCMdW10, MY04, ŠB20, AB09].

A convenient operational language for analyzing them is that of *non-local games*, in which a referee exchanges questions and answers with non-communicating players and decides, according to a public rule, whether they win or lose. A vast literature in non-local games covers the scenario where a classical referee sends questions to non-communicating collaborative parties, and their task is to produce answers according to a certain publicly-known predicate, where the questions and answers are all *classical*. The best-known non-local game is the CHSH game [CHSH69]. Non-locality has also been investigated in terms of supersets of non-local games, called *monogamy-of-entanglement (MoE) games* [TFKW13], see Chapter 3, where a quantum referee sends the same classical question to the players and the parties have to guess the (classical) outcome of a referee's quantum measurement (depending on the question). MoE games have been used to provide security proofs for the quantum cryptographic primitives device-independent quantum key distribution [BB84] and quantum position verification [KMS11]. Such games were later generalized under the name of *extended non-local games* [JMRW16], see Chapter 5.

In this chapter, we adopt a different viewpoint. We ask what changes when the referee expects the player's answer to be a *quantum state*. We introduce the concept of the *quantum cloning game*, played by k distant parties and a quantum referee. The referee publicly announces a party, i.e. sends the same classical question to all the players, and the chosen party has to end up with the maximally entangled (EPR) state with the referee. At the beginning of the game, the players are allowed to share any quantum state with the referee. In this work, we show that the optimal winning probability for players using any quantum resources is given by $\frac{1}{2} + \frac{1}{2k}$, converging to $\frac{1}{2}$ for a large number of players. We analyze the game when it is played m times in parallel, showing an exponential decay in m of the optimal winning probability. Additionally, the quantum cloning game can be generalized to any arbitrary quantum state instead of an EPR state, and we provide its optimal winning probability.

We show that these results have applications in quantum position verification (QPV). In this chapter, we consider the *routing* QPV protocol [KMS11], which has an appealing simple form: the prover has to return a received qubit to one of the verifiers, where the choice of verifier is a function of the classical information sent by the verifiers [KMS11]. Besides the theoretical interest of this protocol, it is also an appealing candidate for free-space quantum position verification, when the quantum messages can travel with the vacuum speed of light, since the hardware of the prover could hypothetically be as sim-

ple as a mirror or an optical switch. Despite theoretical work on this protocol [BFSS13, CM23, BCS22, ABM+24, ACCM24], there were gaps left in our understanding relative to measurement-based QPV protocol variants: namely the security of parallel repetition of this protocol against unentangled attackers and attackers who pre-share a linear (in the security parameter) amount of entangled qubits, and its security in the random-oracle model against arbitrary adversaries. As an application of the quantum cloning game, we show the security of the routing protocol in these scenarios.

7.2 $\hbar$-party quantum cloning game

In the following definition, we introduce the quantum cloning game.

7.2.1. Definition. *The $\hbar$-party* quantum cloning game*, shortly denoted by* $\mathrm{QCG}_\hbar$*, played by a referee R, who has the associated Hilbert space $\mathcal{H}_R = \mathbb{C}^2$, and $\hbar$ collaborative distant parties $P_1, \ldots, P_{\hbar-1}$, referred to as the players, is described as follows:*

1. *The parties prepare a joint quantum state ρ of arbitrary dimension between themselves and the referee.*

2. *The players send a qubit register of ρ to the referee and hold local (arbitrary dimensional) registers of the state. The players are no longer allowed to communicate.*

3. *The referee sends $z \in [\hbar]$, drawn uniformly at random, to all the collaborative parties.*

4. *The players win the game if and only if the party P_z (holding a qubit register P_z) ends up sharing the maximally entangled state with the referee, i.e. if a projection onto $|\Phi^+\rangle_{RP_z}$ yields the correct outcome.*

See Figure 7.1 for a schematic representation of the $\mathrm{QCG}_\hbar$. Intuitively, in such a game, the referee publicly announces which party has to create an entangled state with him. This setup is structurally similar to monogamy-of-entanglement (MoE) games (see Figure 3.2); however, instead of responding with a classical answer as in MoE games, the selected party must output a quantum state.

A strategy for the $\mathrm{QCG}_\hbar$ game is the tuple $\mathbf{S} = \{\rho, \mathcal{E}^z_{P_iE_i\to P_i}\}_{i,z}$, with $\rho \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_{P_0E_0} \otimes \cdots \otimes \mathcal{H}_{P_{\hbar-1}E_{\hbar-1}})$, where, for $i \in [\hbar]$, registers P_i are of the same dimension as $\mathcal{H}_R$ and E_i are auxiliary systems of arbitrary dimension that each party possess, and completely positive trace-preserving (CPTP) maps $\{\mathcal{E}^z_{P_iE_i\to P_i}\}_{i,z}$, where the subscript $P_iE_i \to P_i$ indicates that the map has input and output registers P_iE_i

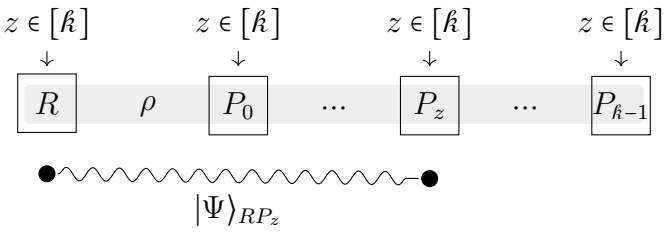


Figure 7.1: Schematic representation of the $\hbar$-party quantum cloning game, where $|\Psi\rangle_{RP_z} = |\Phi^+\rangle_{RP_z}$, where the gray-shaded region represents the shared state ρ. If $|\Psi\rangle_{RP_z}$ is arbitrary, this represents a Ψ-QCG$_\hbar$.

and P_i, respectively, i.e. $\mathcal{E}^z_{P_iE_i\to P_i} : \mathcal{B}(\mathcal{H}_{P_iE_i}) \to \mathcal{B}(\mathcal{H}_{P_i})$. The winning probability of such a game, given the strategy $\mathbf{S}$, is provided by

$$\omega(\mathrm{QCG}_\hbar, \mathbf{S}) = \frac{1}{\hbar} \sum_{z\in[\hbar]} \mathrm{Tr}\left[|\Phi^+\rangle\langle\Phi^+|_{RP_z} \mathrm{Tr}_{P_0\ldots\not{P}_z\ldots P_{\hbar-1}} \left[\mathbb{I}_R \bigotimes_{i\in[\hbar]} \mathcal{E}^z_{P_iE_i\to P_i}(\rho) \right] \right], \tag{7.1}$$

where used the notation $P_0 \ldots \not{P}_z \ldots P_{\hbar-1}$ to denote $P_0 \ldots P_{z-1}P_{z+1} \ldots P_{\hbar-1}$. Due to the Stinespring dilation of quantum channels, we may, without loss of generality, restrict our attention to strategies defined by unitary operations $\{U^z_{P_iE_i}\}_{i,z}$ acting on the registers indicated in the subscripts, in place of the original CPTP maps.

The optimal winning probability of such games is given by

$$\omega(\mathrm{QCG}_\hbar) = \sup_{\mathbf{S}} \omega(\mathrm{QCG}_\hbar, \mathbf{S}), \tag{7.2}$$

where the supremum is taken over all the possible strategies over all possible Hilbert spaces. The following theorem gives the optimal winning probability of this game for every number of parties $\hbar$.

7.2.2. Theorem. *For every $\hbar \in \mathbb{N}$, the optimal winning probability of the* QCG$_\hbar$ *is given by*

$$\omega(\mathrm{QCG}_\hbar) = \frac{1}{2} + \frac{1}{2\hbar}. \tag{7.3}$$

Intuitively, this game cannot be perfectly won since, otherwise, it would be possible to have maximal entanglement between the referee and each of the parties, and this is not possible since entanglement is *monogamous* [CKW00]. In the proof, see below, the key part is to show that the optimal winning probability is attainable by the actions of the players being *independent* of z, intuitively, each party acts as if they were chosen to reproduce the maximally entangled state with the referee. In addition, in the proof, we show that the optimal value can be attained by preparing an initial state ρ where, locally, each of the parties holds a qubit and no further actions taken by the players, i.e. their local actions are

described by the identity channel ($\mathbb{I}_{P_i}$). We then specify a strategy by providing a quantum state, since any local actions are independent of z, they can be absorbed in the quantum state. More precisely, the optimal winning probability for the $\mathrm{QCG}_\hbar$ can be attained by the strategy given by the (pure) quantum state

$$|\varphi\rangle = \sqrt{\frac{2}{\hbar(\hbar+1)}} \sum_{z\in[\hbar]} |\Phi^+\rangle_{RP_z} |0\rangle_{P_0\ldots \not{P}_z \ldots P_{\hbar-1}}. \tag{7.4}$$

Note that other natural multi-party entangled states that have been widely studied in the literature, such as the GHZ state ([GHZ89]) $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and the W state ([DVC00]) $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$, and their respective generalizations to arbitrary dimensions, as well as the strategy of 'guessing' which party has to reproduce the quantum state, e.g. guessing $z = 0$, given by preparing the state $|\Phi^+\rangle_{VP_0}|0\rangle_{P_1}\ldots|0\rangle_{\hbar-1}$, provide significantly suboptimal winning probabilities. For 2 players, $\omega(\mathrm{QCG}_2) = \frac{3}{4}$, and

$$\omega(\mathrm{QCG}_\hbar) \xrightarrow{\hbar\to\infty} \frac{1}{2}, \tag{7.5}$$

which converges to the value attained by the strategy given by preparing the state $|0\rangle_R|0\rangle_{P_0}\ldots|0\rangle_{P_{\hbar-1}}$, showing that when $\hbar$ increases even unentangled states allow for a near-optimal winning probability.

Proof:
Let $\mathbf{S} = \{\rho, U^z_{P_iE_i}\}_{i,z}$ be a strategy for $\mathrm{QCG}_\hbar$, where $\rho \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_{P_0E_0} \otimes \ldots \otimes \mathcal{H}_{P_{\hbar-1}E_{\hbar-1}})$, where, for $i \in [\hbar]$, registers P_i are of the same dimension as $\mathcal{H}_R$ and E_i are auxiliary systems of arbitrary dimension that each party possesses, and unitary transformations $U = \{U^z_{P_iE_i}\}_{i,z}$, acting on the registers in the subscripts. Recall that, as argued above, we do not lose generality by considering unitaries instead of quantum channels. Let d be the dimension of the above (total) Hilbert space, which we denote by $\mathcal{H}_d$. Then, the winning probability of the $\mathrm{QCG}_\hbar$, given the strategy $\mathbf{S}$ on a d-dimensional Hilbert space, is provided by

$$\begin{aligned}
&\omega(\mathrm{QCG}_\hbar, \mathbf{S}, d) \\
&= \frac{1}{\hbar} \sum_{z\in[\hbar]} \mathrm{Tr}\left[\left(|\Phi^+\rangle\langle\Phi^+|_{RP_z} \otimes \mathbb{I}_{E_z} \bigotimes_{i\neq z\in[\hbar]} \mathbb{I}_{P_iE_i}\right)\left(\left(\mathbb{I}_R \otimes_i U^z_{P_iE_i}\right)\rho\left(\mathbb{I}_R \otimes_i U^z_{P_iE_i}\right)^\dagger\right)\right] \\
&= \frac{1}{\hbar} \sum_{z\in[\hbar]} \mathrm{Tr}\left[\left(\mathbb{I}_R \otimes_i U^{z\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_z} \otimes \mathbb{I}_{E_z} \bigotimes_{i\neq z\in[\hbar]} \mathbb{I}_{P_iE_i}\right)\left(\mathbb{I}_R \otimes_i U^z_{P_iE_i}\right)\rho\right],
\end{aligned}$$

where in the last equation we used cyclicity of the trace. For a specific choice of unitary transformations $U = \{U^z_{P_iE_i}\}_{i,z}$, the optimal winning probability is given

by

$$
\begin{aligned}
&\omega^*(\mathrm{QCG}_{\hbar}, U, d)\\
&= \sup_{\rho\in\mathcal{S}(\mathcal{H}_d)} \frac{1}{\hbar}\sum_{z\in[\hbar]} \mathrm{Tr}\left[\left(\mathbb{I}_R\otimes_i U^{z\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z}\bigotimes_{i\neq z\in[\hbar]}\mathbb{I}_{P_iE_i}\right)\left(\mathbb{I}_R\otimes_i U^{z}_{P_iE_i}\right)\rho\right]\\
&= \frac{1}{\hbar}\Big\| \sum_{z\in[\hbar]} \left(\mathbb{I}_R\otimes_i U^{z\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z}\bigotimes_{i\neq z\in[\hbar]}\mathbb{I}_{P_iE_i}\right)\left(\mathbb{I}_R\otimes_i U^{z}_{P_iE_i}\right)\Big\|\\
&= \frac{1}{\hbar}\Big\| \sum_{z\in[\hbar]} \left(\left(\mathbb{I}_R\otimes U^{z\dagger}_{P_zE_z}\right)(|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z})\left(\mathbb{I}_R\otimes U^{z}_{P_zE_z}\right)\right)\bigotimes_{i\neq z\in[\hbar]} U^{z\dagger}_{P_iE_i}\bigotimes_{i\neq z\in[\hbar]}\mathbb{I}_{P_iE_i}\bigotimes_{i\neq z\in[\hbar]} U^{z}_{P_iE_i}\Big\|\\
&= \frac{1}{\hbar}\Big\| \sum_{z\in[\hbar]} \left(\left(\mathbb{I}_R\otimes U^{z\dagger}_{P_zE_z}\right)(|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z})\left(\mathbb{I}_R\otimes U^{z}_{P_zE_z}\right)\right)\bigotimes_{i\neq z\in[\hbar]} U^{z\dagger}_{P_iE_i}U^{z}_{P_iE_i}\Big\|,
\end{aligned}
$$

Notice that, since $\{U^z_{P_iE_i}\}_{i,z}$ are unitary matrices, $U^{z\dagger}_{P_iE_i}U^z_{P_iE_i} = \mathbb{I}_{P_iE_i}$, moreover, $\mathbb{I}_{P_iE_i} = U^{i\dagger}_{P_iE_i}U^i_{P_iE_i}$, then we can use $U^{z\dagger}_{P_iE_i}U^z_{P_iE_i} = U^{i\dagger}_{P_iE_i}U^i_{P_iE_i}$, and therefore

$$
\begin{aligned}
&\omega^*(\mathrm{QCG}_{\hbar}, U, d)\\
&\quad= \frac{1}{\hbar}\Big\| \sum_{z\in[\hbar]} \left(\left(\mathbb{I}_R\otimes U^{z\dagger}_{P_zE_z}\right)(|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z})\left(\mathbb{I}_R\otimes U^{z\dagger}_{P_zE_z}\right)\right)\bigotimes_{i\neq z\in[\hbar]} U^{i\dagger}_{P_iE_i}U^{i}_{P_iE_i}\Big\|\\
&\quad= \frac{1}{\hbar}\Big\| \sum_{z\in[\hbar]} \left(\mathbb{I}_R\bigotimes_{i\neq\epsilon[\hbar]} U^{i\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z}\bigotimes_{i\neq z\in[\hbar]}\mathbb{I}_{P_iE_i}\right)\left(\mathbb{I}_R\bigotimes_{i\epsilon[\hbar]} U^{i}_{P_iE_i}\right)\Big\|\\
&\quad= \frac{1}{\hbar}\Big\| \left(\mathbb{I}_R\bigotimes_{i\neq\epsilon[\hbar]} U^{i\dagger}_{P_iE_i}\right)\left(\sum_{z\in[\hbar]}|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z}\bigotimes_{i\neq z\in[\hbar]}\mathbb{I}_{P_iE_i}\right)\left(\mathbb{I}_R\bigotimes_{i\epsilon[\hbar]} U^{i}_{P_iE_i}\right)\Big\|\\
&\quad= \frac{1}{\hbar}\Big\| \sum_{z\in[\hbar]}|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z}\bigotimes_{i\neq z\in[\hbar]}\mathbb{I}_{P_iE_i}\Big\|\\
&\quad= \sup_{\rho\in\mathcal{S}(\mathcal{H}_d)} \frac{1}{\hbar}\sum_{z\in[\hbar]} \mathrm{Tr}\left[\left(|\Phi^+\rangle\langle\Phi^+|_{RP_z}\otimes\mathbb{I}_{E_z}\bigotimes_{i\neq z\in[\hbar]}\mathbb{I}_{P_iE_i}\right)\rho\right] = \omega^*(\mathrm{QCG}_{\hbar}, d)
\end{aligned}
\tag{7.6}
$$

where in the fourth equality we used that the Schatten ∞-norm is unitarily invariant, i.e. $\|V * W\| = \| * \|$ for unitary matrices V and W, and $\omega^*(\mathrm{QCG}_{\hbar}, d)$ denotes the optimal winning probability if the dimension of the total initial Hilbert space is d. Equation (7.6) shows that, given a Hilbert space $\mathcal{H}_R\otimes\mathcal{H}_{P_0E_0}\otimes\ldots\otimes\mathcal{H}_{P_{\hbar-1}E_{\hbar-1}}$, the optimal winning probability can be attained by an optimal quantum state independently of the actions of the players after knowing z, i.e. the optimal winning probability is independent of $\{U^z_{P_iE_i}\}_z$ and they can apply $\{\mathbb{I}^z_{P_iE_i}\}_z$. We are going to see that, actually, the optimal winning probability can be attained by each of the parties possessing a qubit (2-dimensional Hilbert space), i.e. by the total

Hilbert space being $\mathcal{H}_{2^\hbar} = \bigotimes_{i\in[\hbar]} \mathbb{C}^2$. From (7.6),

$$\begin{aligned}\omega(\mathrm{QCG}_\hbar) &= \sup_{d\in\mathbb{N}} \omega^*(\mathrm{QCG}_\hbar, d) = \sup_{d\in\mathbb{N}} \frac{1}{\hbar} \Big\| \Bigg(\sum_{z\in[\hbar]} |\Phi^+\rangle\langle\Phi^+|_{RP_z} \otimes \mathbb{I}_{P_0\ldots \not{P}_z \ldots P_{\hbar-1}} \Bigg) \bigotimes_{i\in[\hbar]} \mathbb{I}_{E_i} \Big\| \\ &= \sup_{d\in\mathbb{N}} \frac{1}{\hbar} \Big\| \sum_{z\in[\hbar]} |\Phi^+\rangle\langle\Phi^+|_{RP_z} \otimes \mathbb{I}_{P_0\ldots \not{P}_z \ldots P_{\hbar-1}} \Big\| \Big\| \bigotimes_{i\in[\hbar]} \mathbb{I}_{E_i} \Big\| \\ &= \sup_{d\in\mathbb{N}} \frac{1}{\hbar} \Big\| \sum_{z\in[\hbar]} |\Phi^+\rangle\langle\Phi^+|_{RP_z} \otimes \mathbb{I}_{P_0\ldots \not{P}_z \ldots P_{\hbar-1}} \Big\| \\ &= \sup_{\rho\in\mathcal{S}(\mathcal{H}_{2^\hbar})} \frac{1}{\hbar} \sum_{z\in[\hbar]} \mathrm{Tr}\Big[\big(|\Phi^+\rangle\langle\Phi^+|_{RP_z} \otimes \mathbb{I}_{P_0\ldots \not{P}_z \ldots P_{\hbar-1}} \big) \rho \Big], \end{aligned} \tag{7.7}$$

where, in the arguments of the supremums, the dependence on d is implicit in the auxiliary spaces, which, together with the registers P_i and V, fully describe the total Hilbert space, and thus its dimension.

In order to provide the explicit value for the optimal winning probability, we have that, from (7.7),

$$\omega(\mathrm{QCG}_\hbar) = \frac{1}{\hbar} \Big\| \sum_{z\in[\hbar]} |\Phi^+\rangle\langle\Phi^+|_{RP_z} \otimes \mathbb{I}_{P_0\ldots \not{P}_z \ldots P_{\hbar-1}} \Big\| = \frac{1}{2} + \frac{1}{2k}, \tag{7.8}$$

where the last equation is obtained by direct computation. □

7.2.1 Quantum cloning game with any target state

The concept of $\mathrm{QCG}_\hbar$ can be generalized to the case where, instead of the parties having to reproduce EPR pairs with the referee, the state that has to be reproduced is an arbitrary-fixed state, i.e. the referee's Hilbert space $\mathcal{H}_R$ is now of arbitrary dimension, and on input z the party P_z has to generate a given state $|\Psi\rangle_{RP_z}$. Here, the dimension of the registers P_i is the same for all $i \in [\hbar]$. We will refer to such a game as a $\hbar$-party *quantum cloning game with target state* $|\Psi\rangle$, in short denoted by Ψ-$\mathrm{QCG}_\hbar$, see Figure 7.1. Notice that this game becomes trivial if the target state $|\Psi\rangle_{RP}$ is a tensor product state. In the following theorem, we provide the optimal winning probability for any Ψ-$\mathrm{QCG}_\hbar$ for every number of parties $\hbar$ and for any target state $|\Psi\rangle$.

7.2.3. Theorem. *The optimal winning probability for every* Ψ-$\mathrm{QCG}_\hbar$ is given by

$$\omega(\Psi\text{-}\mathrm{QCG}_\hbar) = \frac{1}{\hbar} \Big\| \sum_{z\in[\hbar]} |\Psi\rangle\langle\Psi|_{RP_z} \otimes \mathbb{I}_{P_0\ldots \not{P}_z \ldots P_{\hbar-1}} \Big\|. \tag{7.9}$$

Along the lines of the proof of Theorem 7.2.2, the key idea relies on showing that the optimal winning probability can be attained by the actions of the players being independent on z.

Proof:
The result follows from the proof of Theorem 7.2.2 by repeating the same steps, replacing $|\Phi^+\rangle_{VP_z}$ by $|\Psi\rangle_{VP_z}$, and from (7.7), we obtain (7.9). □

7.3 Parallel repetition of $\mathrm{QCG}_{\not k}$

A case of particular interest is given when $\mathrm{QCG}_{\not k}$ is played m times in parallel, denoted by $\mathrm{QCG}_{\not k}^{\times m}$. Specifically, we will analyze QCG_2 where now the two collaborative parties, who we rename as Alice and Bob, will receive $z = z_0 \dots z_{m-1} \in \{0,1\}^m$. We denote by $R_0 \dots R_{m-1}$, $A_0 \dots A_{m-1}$ and $B_0 \dots B_{m-1}$ the final (qubit) registers of the referee, Alice and Bob, respectively. The players win if at the end of the game Alice is able to create the maximally entangled state with the referee in all her registers such that $z_i = 0$, and analogously for Bob in all his registers such that $z_i = 1$. See Figure 7.2 for a schematic representation.

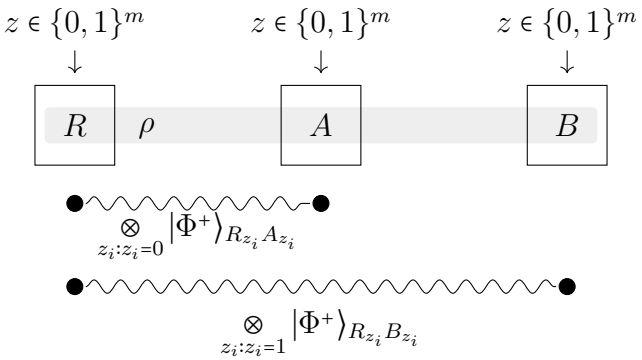


Figure 7.2: Schematic representation of the n-fold parallel repetition of the 2-party quantum cloning game. The gray-shaded region represents the tripartie state ρ that Alice and Bob prepare.

Similarly as before, at the beginning of the game the three parties are allowed to share any arbitrary quantum state $\rho_{RA_0 \dots A_{m-1} E_A B_0 \dots B_{m-1} E_B}$ and, upon receiving the classical information, Alice and Bob can apply CPTP maps $\{\mathcal{E}^z_{A_0 \dots A_{m-1} E_A \to A_0 \dots A_{m-1}}\}_z$ and $\{\mathcal{E}^z_{B_0 \dots B_{m-1} E_B \to B_0 \dots B_{m-1}}\}_z$, where E_A and E_B are arbitrary auxiliary systems that Alice and Bob possess, respectively. As argued in Section 5.4, we do not lose generality if we consider strategies of the form $\mathbf{S} = \{\rho, K^z_{A_0 \dots A_{m-1} E_A}, L^z_{B_0 \dots B_{m-1} E_B}\}$ (if necessary, enlarging the dimensions of the auxiliary systems E_A and E_A), where K^z and L^z are unitary transformations for all $z \in \{0,1\}^m$. In the following

theorem, we state that the optimal winning probability decays exponentially with the number of parallel repetitions m.

7.3.1. Theorem. *The optimal winning probability for m parallel repetitions of the* $\mathrm{QCG}_2^{\times m}$ *is such that*

$$\left(\frac{3}{4}\right)^m \leq \omega(\mathrm{QCG}_2^{\times m}) \leq \left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^m. \tag{7.10}$$

The key idea of the proof relies on combining ideas used in the proof of Theorem 7.2.3 together with Proposition 4.3 in [Sch07], which was also used in [TFKW13] to prove parallel repetition for monogamy-of-entanglement games. Theorem 7.3.1 is a particular case of its error-robust version, Proposition 7.3.2, see proof below.

We now consider the non-ideal case where there is a parameter error $p_{err} < 1/2$ when playing $\mathrm{QCG}_2^{\times m}$, capturing the fraction of rounds in which the check fails. That is, let $v \in \{0,1\}^m$ with $v_i = 0$ if the projective measurement by the referee in yields to the correct outcome in the for z_i, and $v_i = 1$, otherwise, for all $i \in \{1,\dots,m\}$, we then say that the players win the game with error at most p_{err} if $w_H(v) \leq mp_{\mathrm{err}}$, where $w_H(v)$ denotes the Hamming weight of v. This is captured by the referee performing the measurement $\{N_v^z\}_{v\in\{0,1\}^m}$, where

$$N_v^z := \bigotimes_{i\in[m]} N_{v_i}^{z_i}, \tag{7.11}$$

with

$$N_{v_i}^{z_i} := \begin{cases} |\Phi^+\rangle\langle\Phi^+|_{R_{z_i}Q_{z_i}}, & \text{if } v_i = 0, \\ \mathbb{I} - |\Phi^+\rangle\langle\Phi^+|_{R_{z_i}Q_{z_i}}, & \text{if } v_i = 1, \end{cases} \tag{7.12}$$

where $Q_{z_i} = A_i$ if $z_i = 0$ and $Q_{z_i} = B_i$ if $z_i = 1$.
Then, given a strategy $\mathbf{S} = \{\rho, K^z, L^z\}_z$, the corresponding winning probability is given by

$$\omega(\mathrm{QCG}_2^{\times m}, \mathbf{S}, p_{err}) = \frac{1}{2^m} \sum_{\substack{z \\ v: w_H(v)\leq mp_{err}}} \mathrm{Tr}\big[(N_v^z \otimes \mathbb{I})(K^z \otimes L^z)\rho(K^z \otimes L^z)^\dagger\big], \tag{7.13}$$

where the identity $\mathbb{I}$ applies to all the remaining registers. We provide a robust formulation of the parallel repetition theorem for $\mathrm{QCG}_2^{\times m}$:

7.3.2. Proposition. *Let* $\mathrm{QCG}_2^{\times m}$ *be played with an error parameter $p_{err} < 1/2$. Then, its optimal winning probability is such that*

$$\omega(\mathrm{QCG}_2^{\times m}) \leq \left(2^{p_{err}+h_b(p_{err})}\Big(\frac{1}{2}+\frac{1}{2\sqrt{2}}\Big)\right)^m, \tag{7.14}$$

where $h_b(\cdot)$ denotes the binary entropy.

The above bound is exponentially decaying for an error up to 3.0%. In order to prove Proposition 7.3.2, we need the following definition and lemmas:

7.3.3. Definition. *Let $N \in \mathbb{N}$. Two permutations $\pi, \pi' : [N] \to [N]$ are said to be* orthogonal *if $\pi(i) \neq \pi'(i)$ for all $i \in [N]$.*

7.3.4. Lemma. (Lemma 2 in [TFKW13]) *Let $\Pi^1, \dots, \Pi^N$ be projectors acting on a Hilbert space $\mathcal{H}$. Let $\{\pi_k\}_{k\in[N]}$ be a set of mutually orthogonal permutations. Then,*

$$\left\| \sum_{i\in[N]} \Pi^i \right\| \leq \sum_{k\in[N]} \max_{i\in[N]} \left\| \Pi^i \Pi^{\pi_k(i)} \right\|. \tag{7.15}$$

7.3.5. Lemma. *(Lemma 1 in [TFKW13]) Let $A, B, L \in \mathcal{B}(\mathcal{H})$ such that $AA^\dagger \geq B^\dagger B$. Then it holds that $\|AL\| \geq \|BL\|$.*

Proof:
A strategy $\mathbf{S}$ for the m-parallel repetition of QCG_2 (with error p_{err}) is described by a quantum state $\rho \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_{A_0\dots A_{m-1}E_A} \otimes \mathcal{H}_{B_0\dots B_{m-1}E_B})$, where, for $i \in [m]$, registers A_i and B_i are of the same dimension as $\mathcal{H}_R$ and E_A and E_B are auxiliary systems of arbitrary dimension that each party possess, and unitary transformations $\{U^z_{A_0\dots A_{m-1}E_A}\}_z$ and $\{V^z_{B_0\dots B_{m-1}E_B}\}_z$, acting on the registers in the subscripts (due to the Stinespring dilation of the quantum channels, we restrict our attention to unitary transformations). For $z = z_0 \dots z_{m-1} \in \{0,1\}^m$, let $Q_{z_i} = A_i$ if $z_i = 0$ and $Q_{z_i} = B_i$ if $z_i = 1$, and we use the shorthand notation $R = R_0 \dots R_{m-1}$, $A = A_0 \dots A_{m-1}$ and $B = B_0 \dots B_{m-1}$. Then, the winning probability of this game, given the strategy $\mathbf{S}$, is given by

$$\begin{aligned}\omega(\mathrm{QCG}_2^{\times m}, \mathbf{S}, p_{err}) &= \frac{1}{2^m} \sum_{\substack{z \\ v: w_H(v) \leq m p_{err}}} \mathrm{Tr}\big[(N_a^z \otimes \mathbb{I})(K^z \otimes L^z)|\psi\rangle\langle\psi|(K^z \otimes L^z)^\dagger\big], \\ &\leq \frac{1}{2^m} \Big\| \sum_{\substack{z \\ v: w_H(v) \leq m p_{err}}} (K^z \otimes L^z)^\dagger (N_v^z \otimes \mathbb{I})(K^z \otimes L^z) \Big\|.\end{aligned} \tag{7.16}$$

Let

$$\tilde{N}_v^z := (K^z \otimes L^z)^\dagger (N_v^z \otimes \mathbb{I})(K^z \otimes L^z), \tag{7.17}$$

then,

$$\omega(\mathrm{QCG}_2^{\times m}, \mathbf{S}, p_{err}) \leq \frac{1}{2^m} \Big\| \sum_{\substack{z \\ v: w_H(v) \leq m p_{err}}} \tilde{N}_v^z \Big\| \leq \frac{1}{2^m} \sum_{v: w_H(v) \leq m p_{err}} \sum_{k\in[2^m]} \max_{z,z'} \|\tilde{N}_v^z \tilde{N}_v^{z'}\|, \tag{7.18}$$

where we used Lemma 7.3.4, and $z' = \pi_k(z)$, for $\{\pi_k\}_k$ being a set of mutually orthogonal permutations. Fix z and z', and let $\mathcal{T}$ be the set of indices where z and

z' differ, i.e. $\mathcal{T} = \{i \mid z_i \neq z'_i\}$, and let $t = |\mathcal{T}|$. Let $\mathcal{T}_A = \{i \in \mathcal{T} \mid z_i = 0\}$, denote $t_A := |\mathcal{T}_A|$, and, without loss of generality, assume $t_A \geq t/2$. Let $\mathcal{T}_A^0 = \{i \in \mathcal{T}_A \mid a_i = 0\}$, and $t_A^0 := |\mathcal{T}_A^0|$, then we have that

$$
\begin{aligned}
&\tilde{N}_v^z \preceq \tilde{N}_{v_A}^z := \\
&(\mathbb{I}_V \otimes K^{z\dagger} \otimes L^{z\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iQ_{z_i}} \otimes \mathbb{I}_{Q_{1-z_i}}\right) \otimes \left(\bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iQ_{z_i}Q_{1-z_i}}\right) \otimes \mathbb{I}_{E_AE_B}\right)(\mathbb{I}_V \otimes K^z \otimes L^z) \\
&= (\mathbb{I}_V \otimes K^{z\dagger} \otimes L^{z\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iA_iE_A}\right) \otimes \mathbb{I}_{BE_B}\right)(\mathbb{I}_V \otimes K^z \otimes L^z) \\
&= (\mathbb{I}_V \otimes K^{z\dagger} \otimes L^{z'\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iA_iE_A}\right) \otimes \mathbb{I}_{BE_B}\right)(\mathbb{I}_V \otimes K^z \otimes L^{z'})
\end{aligned}
$$

where in the last equality we used that $L_{BE_B}^{z\dagger} L_{BE_B}^{z\dagger} = \mathbb{I}_{BE_B} = L_{BE_B}^{z'\dagger} L_{BE_B}^{z'}$. Similarly,

$$
\begin{aligned}
&\tilde{N}_v^{z'} \preceq \tilde{N}_{v_B}^{z'} := \\
&(\mathbb{I}_V \otimes K^{z\dagger} \otimes L^{z\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \otimes \mathbb{I}_{A_i}\right) \otimes \left(\bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iQ_{z_i}Q_{1-z_i}}\right) \otimes \mathbb{I}_{E_AE_B}\right)(\mathbb{I}_V \otimes K^z \otimes L^z) \\
&= (\mathbb{I}_V \otimes K^{z\dagger} \otimes L^{z\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iA_iE_A}\right) \otimes \mathbb{I}_{BE_B}\right)(\mathbb{I}_V \otimes K^z \otimes L^z) \\
&= (\mathbb{I}_V \otimes K^{z'\dagger} \otimes L^{z\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iA_iE_A}\right) \otimes \mathbb{I}_{BE_B}\right)(\mathbb{I}_V \otimes K^{z'} \otimes L^z)
\end{aligned}
$$

By Lemma 7.3.5,

$$\|\tilde{N}_v^z \tilde{N}_v^{z'}\| \leq \|\tilde{N}_{v_A}^z \tilde{N}_{v_B}^{z'}\|, \tag{7.19}$$

then,

$$
\begin{aligned}
\tilde{N}_{v_A}^z \tilde{N}_{v_B}^{z'} = &(\mathbb{I}_V \otimes K^{z\dagger} \otimes L^{z'\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iA_iE_A}\right) \otimes \mathbb{I}_{B'E'_B}\right)(\mathbb{I}_V \otimes K^z \otimes L^{z'}) \\
&(\mathbb{I}_V \otimes K^{z'\dagger} \otimes L^{z\dagger})\left(\left(\bigotimes_{i\in\mathcal{T}_A^0} |\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \bigotimes_{i\in[m]\setminus\mathcal{T}_A^0} \mathbb{I}_{R_iA_iE_A}\right) \otimes \mathbb{I}_{BE_B}\right)(\mathbb{I}_V \otimes K^{z'} \otimes L^z)
\end{aligned}
$$

We have that $(\mathbb{I}_V \otimes K_{AE_A}^z \otimes L_{BE_B}^{z'})(\mathbb{I}_V \otimes K_{AE_A}^{z'\dagger} \otimes L_{BE_B}^{z\dagger}) = \mathbb{I}_{VAE_ABE_B}$, and, since the Schatten ∞-norm is unitarily invariant,

$$
\begin{aligned}
&\|\tilde{N}^z_{v_A}\tilde{N}^{z'}_{v_B}\| \\
&= \Big\|\Big(\bigotimes_{i\in\mathcal{T}^0_A}|\Phi^+\rangle\langle\Phi^+|_{R_iA_i}\bigotimes_{i\in[m]\setminus\mathcal{T}^0_A}\mathbb{I}_{R_iA_iE_A}\otimes\mathbb{I}_{BE_B}\Big)\Big(\bigotimes_{i\in\mathcal{T}^0_A}|\Phi^+\rangle\langle\Phi^+|_{R_iB_i}\bigotimes_{i\in[m]\setminus\mathcal{T}^0_A}\mathbb{I}_{R_iB_iE_B}\otimes\mathbb{I}_{AE_A}\Big)\Big\| \\
&= \Big\|\Big(\bigotimes_{i\in\mathcal{T}^0_A}\big(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i}\otimes\mathbb{I}_{B_i}\big)\big(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i}\otimes\mathbb{I}_{A_i}\big)\Big)\bigotimes_{i\in[m]\setminus\mathcal{T}^0_A}\mathbb{I}_{R_iA_iB_i}\otimes\mathbb{I}_{E_AE_B}\Big\| \\
&= \Big\|\bigotimes_{i\in\mathcal{T}^0_A}\big(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i}\otimes\mathbb{I}_{B_i}\big)\big(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i}\otimes\mathbb{I}_{A_i}\big)\Big\|\Big\|\bigotimes_{i\in[m]\setminus\mathcal{T}^0_A}\mathbb{I}_{R_iA_iB_i}\otimes\mathbb{I}_{E_AE_B}\Big\| \\
&= \prod_{i\in\mathcal{T}^0_A}\big\|\big(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i}\otimes\mathbb{I}_{B_i}\big)\big(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i}\otimes\mathbb{I}_{A_i}\big)\big\| = 2^{-t_A},
\end{aligned}
\tag{7.20}
$$

where we used that, for every i,

$$
\big\|\big(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i}\otimes\mathbb{I}_{B_i}\big)\big(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i}\otimes\mathbb{I}_{A_i}\big)\big\| = 2^{-1}. \tag{7.21}
$$

Let $t^1_A \coloneqq |\{i \in \mathcal{T}_A \mid a_i = 1\}|$, then, since in order to accept, $w_H(v) \leq mp_{err}$, in particular, we have that $t^1_A \leq mp_{err}$. Then, using that $t^0_A = t_A - t^1_A \geq t/2 - mp_{err}$, where we used that $t_A \geq t/2$. Then, combining (7.19) and (7.20), we have that

$$
\|\tilde{N}^z_v\tilde{N}^{z'}_v\| \leq \|\tilde{N}^z_{v_A}\tilde{N}^{z'}_{v_B}\| \leq 2^{-\frac{t}{2}+mp_{err}} \tag{7.22}
$$

In order to apply the bound in Lemma 7.3.5, consider the set of permutations given by $\pi_k(z) = z \oplus k$, where $z, k \in \{0,1\}^m$ (they are such that they have the same Hamming distance). There are $\binom{m}{i}$ permutations with Hamming distance i. Then, we have

$$
\begin{aligned}
\omega(\mathrm{QCG}_2^{\times m}, \mathbf{S}, p_{err}) &\leq \frac{1}{2^m}\sum_{v:w_H(v)\leq mp_{err}}\sum_{k\in[2^m]}\max_{z,z'}\|\tilde{N}^z_v\tilde{N}^{z'}_v\| \\
&\leq \frac{1}{2^m}\sum_{v:w_H(v)\leq mp_{err}}\sum_{t=0}^{m}\binom{m}{t}2^{-\frac{t}{2}+mp_{err}} = \left(2^{p_{err}+h_b(p_{err})}\Big(\frac{1}{2}+\frac{1}{2\sqrt{2}}\Big)\right)^m,
\end{aligned}
$$

where we used that $\sum_{v:w_H(v)\leq mp_{err}} \leq 2^{h_b(p_{err})m}$, for $p_{err} \leq 1/2$.

□

7.4 Application to the routing protocol

In this section, we analyze the security of the *routing* QPV protocol, originally introduced in [KMS11]. The protocol presents similarities with the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, see Chapters 1, 3 and 4: one verifier sends a BB84 state to the prover,

and the other verifier, a classical bit, then the prover has to forward the quantum state to one of the two verifiers according to the received bit. The protocol is defined as follows:

7.4.1. DEFINITION. *A round of routing protocol, denoted by* $\mathrm{QPV}_{\mathrm{rout}}$*, is described as follows:*

1. V_0 *and* V_1 *secretly agree on a random bit* $z \in \{0,1\}$*, and a qubit state* $|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle\, |-\rangle\}$*, chosen uniformly at random.*

2. V_0 *sends the qubit* $|\phi\rangle$ *to* P*, and* V_1 *sends* z *to* P*, both at the speed of light in vacuum, coordinating their times so that they arrive at pos at the same time.*

3. *Upon receiving the information sent by* V_0 *and* V_1*, the prover sends the qubit* $|\phi\rangle$ *to the verifier* V_z*.*

4. *If* $|\phi\rangle$ *arrives at the time consistent with pos* ($t = 2$)*, and a projective measurement performed by* V_z *on the state sent by* V_0 *leads to the correct outcome, the verifiers record '*CORRECT*' ('*C*'). If the measurement does not lead to the correct outcome, the verifiers record '*INCORRECT*' ('*I*'). If the timing is inconsistent with pos, the verifiers abort the protocol and reject the location.*

See Figure 7.3 for steps 2. and 3. Assume that the error of the measurement performed by the verifiers is p_{err}. In order to *accept* or *reject* the location, the verifiers run $\mathrm{QPV}_{\mathrm{rout}}$ sequentially r times. Let $v \in \{0,1\}^m$ with $v_i = 0$ if the projective measurement yields to the correct outcome in the ith round, and $v_i = 1$, otherwise, for all $i \in \{1, \ldots, r\}$. If all the qubits arrive at the time consistent with *pos*, and $w_H(v) \leq rp_{err}$—consistency with the error (i.e. the protocol is *complete* by construction)—the verifiers *accept*; otherwise, they *reject*. We will show that in the *No Pre-shared Entanglement* (No-PE) model [BCF+14], any attackers will not pass the check with exponentially high probability (in r), establishing the *soundness* of the protocol. Since both completeness and soundness are satisfied, the protocol is therefore *secure* in the No-PE model.

In [KMS11], it was shown that if adversaries pre-share an EPR pair, they can exploit quantum teleportation to perfectly break the $\mathrm{QPV}_{\mathrm{rout}}$ protocol, similarly as the ERP teleportation attack described for $\mathrm{QPV}_{\mathrm{BB84}}$ described in Chapter 1. To address this, we analyze the security of the protocol under the assumption that the adversaries do not pre-share entanglement prior to the protocol's execution—No-PE model. This is the same adversarial model used in our analysis of the $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ protocol and its variants in Chapter 3.

In a similar manner as the security of $\mathrm{QPV}_{\mathrm{BB84}}$ in the No-PE model can be reduced to a monogamy-of-entanglement game, and it's lossy version and

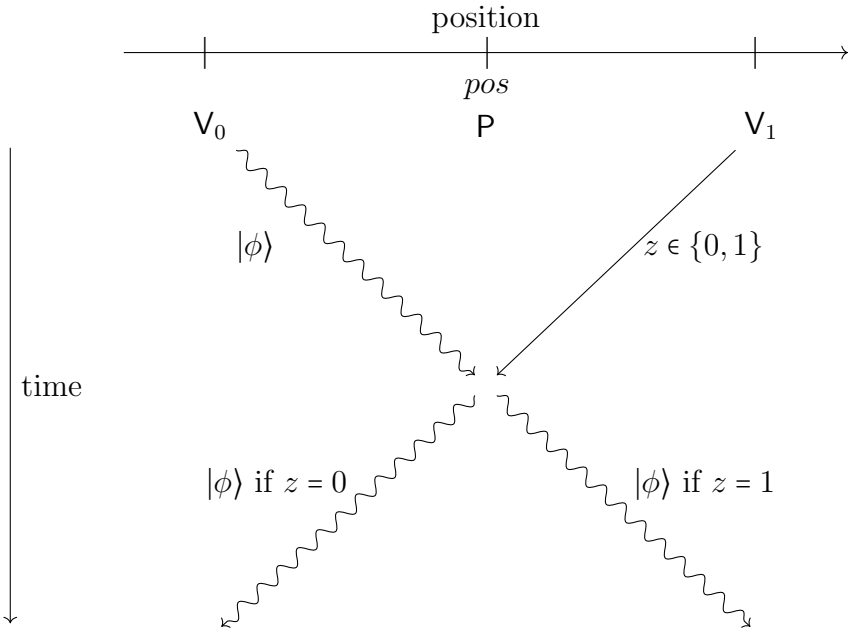


Figure 7.3: Steps 2. and 3. of the QPV_{rout} protocol, where straight lines represent classical information and undulated lines represent quantum information.

extensions, as shown in Chapter 3, we will show that the security of the QPV_{rout} can be reduced to a quantum cloning game. To this end, consider the purified version of the routing protocol, which is equivalent to the original version, and where the only difference relies on V_0, instead of sending the qubit $|\phi\rangle$, prepares the state $|\Phi^+\rangle$ and keeps a register for herself and sends the other register to the prover. Then, the most general attack to the routing QPV protocol consists of placing an adversary between V_0 and *pos*, Alice, and another adversary between *pos* and V_1, Bob. In the No-PE model, (i) Alice intercepts the qubit sent by V_0, applies an arbitrary quantum operation to it, and possibly some ancillary systems she possesses. She keeps a part of it and sends the other to Bob. On the other side, Bob intercepts the classical bit z, copies it, and sends a copy to Alice and kept the other copy. Since they share no entanglement, any quantum operation that Bob could perform as a function of z can be included in Alice's operation. (ii) After one-round of simultaneous communication, Alice and Bob share a tripartite state ρ with V_0, and their task is that the party designated by z—Alice if $z = 0$ and Bob if $z = 1$—has to end up with a maximally entangled state with the V_0, for which they apply quantum channels depending on z. As stated above, in such a case, we can restrict our attention to unitary operations K^z and L^z, then, they send the corresponding qubit register to V_z. The tuple $\mathbf{S}_{\text{rout}} = \{\rho, K^z, L^z\}_z$ is a strategy for the QPV_{rout} protocol in the No-PE model. The probability that the verifiers, after the attackers' actions (for the random

variable V_{AB}) record 'Correct' is given by

$$\Pr[\mathrm{V}_{\mathrm{AB}} = \mathrm{C}] = \frac{1}{2} \sum_{z\in\{0,1\}} \mathrm{Tr}\big[(|\Phi^+\rangle\langle\Phi^+|_{R_z Q_z} \otimes \mathbb{I})(K^z \otimes L^z)\rho(K^z \otimes L^z)^\dagger\big], \tag{7.23}$$

where $Q_z = A$ if $z = 0$ and $Q_z = B$ if $z = 1$. In particular, if they can prepare any state in (ii), this corresponds to the scenario of the QCG_2, and therefore, since the strategies for QCG_2 encode strategies for the $\mathrm{QPV}_{\mathrm{rout}}$m protocol in the No-PE model, the optimal success probability of this game upper bounds the optimal probability that Alice and Bob perform a successful attack. By Theorem 7.2.3, even if Alice and Bob can share any state with the referee (in this case V_0), they can succeed with at most probability $\frac{3}{4}$. This is summarized in the following proposition.

7.4.2. Proposition. *In the No-PE model, the optimal probability that attackers answer 'Correct' in a round of* $\mathrm{QPV}_{\mathrm{rout}}$ *is given by*

$$\max \Pr\{\mathrm{V}_{\mathrm{AB}} = \mathrm{C}\} = \frac{3}{4}. \tag{7.24}$$

On the other hand, to show optimality, consider the attack where

(i) prior to the execution of the protocol, Alice prepares the 3-qubit state

$$\frac{1}{\sqrt{3}}(|\Phi^+\rangle_{A_0 A}|0\rangle_B + |\Phi^+\rangle_{A_0 B}|0\rangle_A). \tag{7.25}$$

(ii) Then, Alice intercepts $|\phi\rangle$ and performs a Bell measurement on the intercepted state and her register A_0, immediately she applies the teleportation corrections to both of her registers A and B. Bob intercepts z and makes a copy.

(iii) Then, Alice keeps register A and sends register B to Bob, and Bob broadcasts z.

(iv) After receiving the information from their fellow attacker, if $z = 0$, Alice sends her register (A) to V_0, whereas if $z = 1$, Bob sends his register (B) to V_1.

This attack is such that has winning probability of $\frac{3}{4}$, attaining the above-mentioned bound.

An analogous reduction applies when the routing QPV protocol is executed m times in parallel, denoted by $\mathrm{QPV}_{\mathrm{rout}}^{\times m}$, and therefore, its security can be reduced to the m-parallel repetition of QCG_2. In the most general attack in the No-PE model, the attackers act similarly as in the attack described for $\mathrm{QPV}_{\mathrm{rout}}$, with the corresponding strategy $\mathbf{S}_{\mathrm{rout}^{\times m}} = \{\rho, K^z, L^z\}_{z\in\{0,1\}^m}$. We consider its error-robust

version, where after the (single) execution of the protocol, the verifiers accept the location if the number of correct outcomes, upon projecting to the maximally entangled state is consistent with an error p_{err}. That is, if $v \in \{0,1\}^m$ with $v_i = 0$ if the projective measurement yields to the correct outcome for z_ith round, and $v_i = 1$, otherwise, for all $i \in \{1,\dots,m\}$, then, the verifiers *accept* the location if all the qubits arrive at the time consistent with *pos*, and $w_H(v) \leq rp_{err}$ (consistency with the error). Otherwise, they *reject*. The probability that the verifiers, after the attackers' actions (for the random variable V_{AB}) record *accept* is given by

$$\Pr[\mathrm{V}_{\mathrm{AB}} = accept] = \frac{1}{2^m} \sum_{\substack{z \\ v: w_H(v) \leq m p_{err}}} \mathrm{Tr}\Big[(N_v^z \otimes \mathbb{I})(K^z \otimes L^z)\rho(K^z \otimes L^z)^\dagger\Big], \tag{7.26}$$

where N_v^z is defined as in (7.11). Therefore, since $\mathbf{S}_{\mathrm{rout}^{\times m}}$ is in particular a strategy for the $\mathrm{QCG}_2^{\times m}$, we have that

$$\Pr[\mathrm{V}_{\mathrm{AB}} = accept] \leq \omega(\mathrm{QCG}_2^{\times m}, p_{err}). \tag{7.27}$$

Then, using Proposition 7.3.2, we can state the following Proposition.

7.4.3. Proposition. *For any attackers to* $\mathrm{QPV}_{\mathrm{rout}}^{\times m}$ *in the No-PE model, the verifiers will accept the location with probability at most* $\left(2^{p_{err}+h_b(p_{err})}\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)\right)^m$.

Then, if the error is below 3.0%, attackers will be caught with exponentially high probability, and thus the protocol is *sound* in the No-PE model.

A direct consequence of Lemma 5.3 in [BK11] implies, similarly as in [TFKW13], security for the routing protocol executed in parallel for attackers who pre-share a linear amount of qubits q:

7.4.4. Corollary. *For any attackers to* $\mathrm{QPV}_{\mathrm{rout}}^{\times m}$ *who pre-share at most q (entangled) qubits prior to the execution of the protocol, the verifiers will accept the location with probability at most* $2^q\left(2^{p_{err}+h_b(p_{err})}\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)\right)^m$.

In particular, the above soundness is exponentially small in m if

$$q < m \log\left(\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^{-1}\right) - (p_{err} + h_b(p_{err})) \tag{7.28}$$

.

Chapter 8

Parallel repetition of the f-BB84 protocol

Quantum position verification aims to verify an untrusted prover's location by timing communication with them. To facilitate real-world implementation, it is desirable for this verification to occur in a single interaction. However, previous protocols achieving one-round secure QPV had critical drawbacks: attackers pre-sharing an EPR pair per qubit could perfectly break them, and their security depended on quantum information traveling at the speed of light in vacuum, a major experimental challenge in quantum networks. Both limitations are exemplified by the routing protocol analyzed in Chapter 7, and correspond to challenges (**EC**) and (**SC**) of QPV outlined in Chapter 1, and illustrated in Figure 1.4.

In this chapter, we prove that a single round of interaction suffices for secure position verification while overcoming these limitations. We show that security for a one-round protocol can rely only on the size of the classical information rather than quantum resources, making implementation more feasible, even with a qubit error tolerance of up to 3.6%, which is experimentally achievable with current technology—and showing that the timing constraints have to apply only to classical communication. Concretely, we establish parallel repetition of the f-BB84 protocol, see Chapter 4. Similar conclusions hold for the parallel repetition of the f-routing QPV protocol. However, a detailed treatment of these results is beyond the scope of this thesis and can be found in [EFS25b], co-authored by the present author.

As a consequence of our techniques, we also demonstrate an order-of-magnitude improvement in the error tolerance for the sequential repetition version of this protocol, compared to the previous bounds of *Nature Physics 18, 623–626 (2022)*.

The results presented in this chapter are based on the following paper:

- "Quantum position verification in one shot: parallel repetition of the f-BB84 and f-routing protocols", by Llorenç Escolà-Farràs, and Florian Speelman, accepted contributed talk at *TQC 2025* [EFS25b].

8.1 Introduction

Security proofs in quantum position verification have been shown by either (i) bounding the probability of a successful attack by a constant and amplifying security through sequential repetition over time, or (ii) directly showing that the attack success probability is exponentially small, corresponding to parallel repetition. These upper bounds are referred to as the protocol's *soundness*. Since quantum position verification is based on timing constraints, parallel repetition implies that the verifiers either *accept* or *reject* the location in a single execution (as discussed in Chapter 7). This stands in contrast to sequential repetition—explored in Chapters 3, 4 and 7. Moreover, a single interaction is necessary in order to verify the location of a non-static prover. However, previous parallel repetition results in the literature for QPV (i) remained insecure if attackers used one EPR pair per qubit used in the protocols, and (ii) required the quantum information to travel at the speed of light in vacuum, see, e.g. Chapter 7—parallel repetition of the routing protocol—which is experimentally challenging[1]. Thus, no existing QPV scheme simultaneously achieved single-round interaction while addressing both (i) and (ii). In this chapter, we present the first QPV protocol that achieves single-round interaction while overcoming both of these limitations.

In this chapter, we will analyze an extension of the BB84 ($\mathrm{QPV}_{\mathrm{BB84}}$) protocol [KMS11]. As introduced in Chapter 1, in the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, V_0 and V_1 send a BB84 state and a classical bit $z \in \{0,1\}$ to the prover P, respectively, then, the prover has to measure the qubit in either the computational ($z = 0$) or the Hadamard ($z = 1$) basis, and broadcast the outcome to both verifiers. We recall that $\mathrm{QPV}_{\mathrm{BB84}}$ was proven to be secure [BCF+14] in the no pre-shared entanglement (No-PE) model—where attackers do not pre-share any entanglement prior to the execution of the protocol—showing constant soundness for a single round, and exponentially decaying soundness when the protocol is executed m times in parallel, $\mathrm{QPV}_{\mathrm{BB84}}^{\times m}$ [TFKW13]. However, it suffices for Alice and Bob to pre-share a single EPR pair per qubit sent by V_0 to perfectly break this protocol [KMS11], see the teleportation-based attack described in Chapter 1. The latter issue, without parallel repetition, i.e. for $m = 1$, was bypassed in [BFSS13, BCS22] by splitting the classical bit z into n-bit strings $x, y \in \{0,1\}^n$, sent by V_0 and V_1, respectively, so that a boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ determines z, i.e. $z = f(x,y)$. We denote this extension by $\mathrm{QPV}_{\mathrm{BB84}}^{f}$, see Chapter 4 where this variant is analyzed in the presence of photon loss. The authors of [BCS22] showed

[1] Whereas the transmission of classical information without loss at the speed of light is technologically feasible, e.g. via radio waves, the quantum counterpart faces obstacles. Most QPV protocols require quantum information to be transmitted at the speed of light in vacuum, but for practical applications this is often unattainable, e.g. the speed of light in optical fibers is significantly lower than in vacuum, or if one wants to use a quantum network, it would be desirable that the infrastructure can be used even if the verifiers and P are not connected in a straight line.

that the protocol has a soundness of at most 0.98, provided that attackers pre-share a number of qubits linear in n—the Bounded-Entanglement (BE(n)) model. This extension requires any attackers to share an amount of entanglement that grows with the classical information, making it an appealing candidate to aim towards implementation. Then, in order to either *accept* or *reject*, the verifiers execute $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ sequentially m times.

In this chapter, we study $\mathrm{QPV}^{f}_{\mathrm{BB84}}$when executed m times in parallel, denoted by $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$, where the classical information $z \in \{0,1\}^m$ is determined by a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$. Unruh [Unr14] showed the security of this protocol in the random oracle model, assuming the function f is a hash function modeled as a quantum random oracle (and quantum information traveling at the speed of light in vacuum). Here, we show that this protocol exhibits exponentially decaying soundness in m in the plain model, provided that the number of pre-shared qubits by attackers scales linearly with the classical information n. Notably, this implies that security is fundamentally tied to the classical information rather than the quantum resources. Moreover, only the classical information is required to travel at the speed of light, whereas the quantum counterpart can be arbitrarily slow. We thus show that a single round of interaction with the prover suffices for secure position verification while overcoming the above-mentioned limitations, preserving exponentially decaying soundness while tolerating an error[2] up to 3.6%, which is currently implementable in a laboratory.

As a consequence of our analysis, we are also able to improve the particular case of $m = 1$ to show soundness of 0.8539. This is essentially tight, since it closely matches the best known attack (which does not use any entanglement), which has success probability $\frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.85355...$, and this result constitutes an improvement of an order of magnitude with respect to the 0.98 soundness shown in [BCS22]. Therefore, our new bounds are useful even when only considering sequential repetition of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. See Table 8.1 for a summary of the previously known results of $\mathrm{QPV}_{\mathrm{BB84}}$ and its variants together with the new results presented in this work.

8.2 Parallel repetition of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$

In this section, we study the m-fold parallel repetition of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, which we denote by $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$. We will describe the protocol, its general attack, and we will prove that the protocol exhibits exponentially small soundness in the quantum information m provided that the attackers' amount of pre-shared entanglement is linearly bounded by the size of the classical information n, i.e. in the BE(n) model.

[2]Because of experimental imperfections, we also study a version of the protocol where the prover only has to answer correctly on a fraction of the parallel rounds.

	No-PE model	BE model			Slow quant.
Protocol	Secure	Sec. EPR	Soundness	Error	Secure
$\mathrm{QPV}_{\mathrm{BB84}}$	✓	✗	–	–	✗
$\mathrm{QPV}_{\mathrm{BB84}}^{\times m}$	✓	✗	$O(2^{-m})$, BE(m)	3.7%	✗
$\mathrm{QPV}_{\mathrm{BB84}}^{f}$	✓	✓	$O(1)$, BE(n)	14.6%	✓
$\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$	✓	✓	$O(2^{-m})$, BE(n)	3.6%	✓

Table 8.1: Summary of results about $\mathrm{QPV}_{\mathrm{BB84}}$ and its variants. We highlight in gray background the cells with the new results presented in this chapter. 'Sec. EPR' means that the protocol is secure if attackers pre-share one EPR pair per qubit in the protocol. BE(m) and BE(n) denote that the security parameter in the Bounded-Entanglement model is the quantum information m and the classical information n, respectively. The soundness column denotes the soundness per round, $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ achieves exponential soundness by sequential repetition. The column corresponding to 'Slow quant.' answers whether the protocol is secure even if the quantum information in an execution of the protocol travels arbitrarily slow.

8.2.1. Definition. ($\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ protocol). *Let $n, m \in \mathbb{N}$, and $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$, and consider an error parameter $p_{err} \in [0, \frac{1}{2})$. The $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ protocol is described as follows:*

1. *The verifiers V_0 and V_1 secretly agree on bit strings $x, y \in \{0,1\}^n$ and $v \in \{0,1\}^m$, chosen uniformly at random. Then, V_0 prepares the m-qubit state $H^{f(x,y)_1}|v_1\rangle \otimes \cdots \otimes H^{f(x,y)_m}|v_m\rangle =: H^{f(x,y)}|v\rangle$.*

2. *V_0 sends $H^{f(x,y)}|v\rangle$ and $x \in \{0,1\}^n$ to P, and V_1 sends $y \in \{0,1\}^n$ to P so that x and y arrive simultaneously at pos. The quantum information can arrive earlier and is only required to be present at pos when the classical information arrives. The classical information is required to travel at the speed of light, whereas the quantum information can be sent arbitrarily slowly.*

3. *Immediately, P measures each qubit $H^{f(x,y)_i}|v_i\rangle$ in the basis $f(x,y)_i =: z_i$ for all $i \in \{1, \ldots, m\}$ ($z := f(x,y)$), and broadcasts her outcome $v_{\mathsf{P}} \in \{0,1\}^m$ to V_0 and V_1.*

4. *The verifiers* accept *if $d_H(v, v_{\mathsf{P}}) \leq m p_{err}$ (consistency with the error), and v arrives at the time consistent with pos. If either the answers do not arrive on time or are different, the verifiers* reject.

See Figure 8.1 for a schematic representation of the $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ protocol. The $\mathrm{QPV}_{\mathrm{BB84}}$ and $\mathrm{QPV}_{\mathrm{BB84}}^{\times m}$ protocols are recovered if the only classical information

that is sent from the verifiers is $y \in \{0,1\}$ and $y \in \{0,1\}^m$, respectively (and $z = y$), and $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ is recovered by setting $m = 1$. By construction, the condition $d_H(v, v_{\mathsf{P}}) \leq mp_{\mathrm{err}}$ ensures *completeness*, and in Section 8.3, we prove *soundness* against attackers who pre-share at most a linear number of entangled qubits in n; in particular, we show that the probability of acceptance by such attackers decays exponentially in m. Together, these two properties imply that the protocol is *secure*.

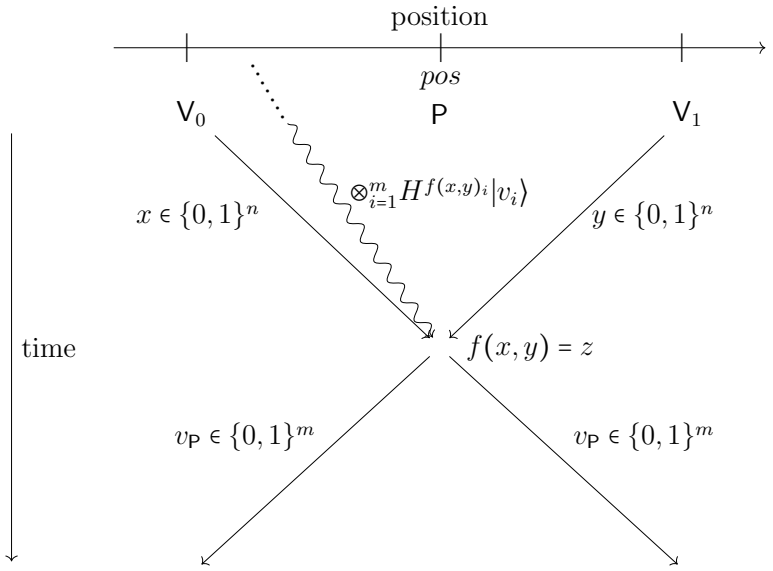


Figure 8.1: Schematic representation of the $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$ protocol. Undulated lines represent quantum information, whereas straight lines represent classical information. The slowly travelling quantum system $\otimes_{i=1}^{m} H^{f(x,y)_i}|v_i\rangle$ originated from V_0 in the past.

Similarly as in Chapters 3, 4 and 7, for the security analysis, we will consider the purified version of $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$, which is equivalent to it. The difference relies on, instead of V_0 sending BB84 states, V_0 prepares m EPR pairs $|\Phi^+\rangle_{V_0^1 P_1} \otimes \cdots \otimes |\Phi^+\rangle_{V_0^m P_m}$ and sends the registers $P_1 \dots P_m$ to the prover. In a later moment, the verifier V_0 performs the measurement $\{H^{f(x,y)}|v\rangle\langle v|_V H^{f(x,y)}\}_{v\in\{0,1\}^m}$ in his local registers $V_0^1 \dots V_0^m =: V$. In this way, the verifiers delay the choice of basis in which the m qubits are encoded, which, in contrast to the above prepare-and-measure version, will make any attack independent of the state sent by V_0.

As introduced in Chapter 1, the most general attack on a 1-dimensional QPV protocol consists on placing an adversary between V_0 and the prover, Alice, and another adversary between the prover and V_1, Bob. In order to attack $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$,

1. Alice intercepts the m qubit state $P_1 \dots P_m$ and applies an arbitrary quantum operation to it and to a local register that she possesses, possibly

entangling them. She keeps part of the resulting state, and sends the rest to Bob. Since the qubits $P_1 \dots P_m$ can be sent arbitrarily slow by V_0 (the verifiers only time the classical information), this happens before Alice and Bob can intercept x and y.

2. Alice intercepts x and Bob intercepts y. At this stage, Alice, Bob, and V_0 share a quantum state $|\varphi\rangle$, make a partition and let q be the number of qubits that Alice and Bob each hold, recall that m qubits are held by V_0 and thus the three parties share a quantum state $|\varphi\rangle$ of $2q+m$ qubits. Alice and Bob apply a unitary $U^x_{A_\mathrm{k}A_\mathrm{c}}$ and $V^y_{B_\mathrm{k}B_\mathrm{c}}$ on their local registers $A_\mathrm{k}A_\mathrm{c} =: A$ and $B_\mathrm{k}B_\mathrm{c} =: B$, both of dimension $d = 2^q$, where k and c denote the registers that will be kept and communicated, respectively. Due to the Stinespring dilation, we consider unitary operations instead of quantum channels. They end up with the quantum state $|\psi_{xy}\rangle = \mathbb{I}_V \otimes U^x_{A_\mathrm{k}A_\mathrm{c}} \otimes V^y_{B_\mathrm{k}B_\mathrm{c}}|\varphi\rangle$. Alice sends register A_c and x to Bob (and keeps register A_k), and Bob sends register B_c and y to Alice (and keeps register B_k).

3. Alice and Bob perform POVMs $\{A^{xy}_a\}_{a\in\{0,1\}^m}$ and $\{B^{xy}_b\}_{b\in\{0,1\}^m}$ on their local registers $A_\mathrm{k}B_\mathrm{c} =: A'$ and $B_\mathrm{k}A_\mathrm{c} =: B'$, and answer their outcomes a and b to their closest verifier, respectively.

The generic attack to $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$ is very similar to the general attack to $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ analyzed in Chapter 4, the differences rely on the size of the quantum system intercepted by Alice and the range of the outputs. We refer to Figure 4.2 in Chapter 3 for a schematic representation of the general attack to $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$. The tuple $\mathbf{S}_{BB84\times m} = \{|\varphi\rangle, U^x, V^y, \{A^{xy}_a\}_a, \{B^{xy}_b\}_b\}_{x,y}$, or $\mathbf{S}$ for short if no ambiguous, will be called a q-qubit strategy for $\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}$. Then, the probability that Alice and Bob perform a successful attack (including an error up to p_{err}), i.e. that the verifiers accept the location, provided the strategy $\mathbf{S}_{BB84\times m}$, which we denote[3] by ω_S, is given by

$$\omega_S(\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}) = \frac{1}{2^{2n}} \sum_{x,y,a} \mathrm{Tr}\left[\left(H^{f(x,y)}|a\rangle\langle a|_V H^{f(x,y)} \otimes \sum_{a':d_H(a,a')\leq mp_{err}} A^{xy}_{a'} \otimes B^{xy}_{a'}\right)|\psi_{xy}\rangle\langle\psi_{xy}|\right]. \tag{8.1}$$

The optimal attack probability is given by

$$\omega(\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}) = \sup_{\mathbf{S}} \omega_S(\mathrm{QPV}^{f:n\to m}_{\mathrm{BB84}}), \tag{8.2}$$

[3]In the previous chapters, we used ω to denote the winning probability of non-local games. Due to the similarities between some non-local games and attacks to quantum position verification seen in Chapters 3 to 7, we will use here ω for the probability that the verifiers accept the location.

where the supremum is taking over all possible strategies $\mathbf{S}$ for the $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$. As mentioned above, the existence of a generic attack for all QPV protocols [BK11, BCF+14] implies that $\omega(\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m})$ can be made arbitrarily close to 1. However, the best known attack requires an exponential amount of pre-shared entanglement. Therefore, we will study the optimal winning probability under restricted strategies $\mathbf{S}$, specifically imposing a constraint on the number of pre-shared qubits q that Alice and Bob hold in step 2 of the general attack. Importantly, we will show security for any state $|\varphi\rangle$ (in step 2) of $2q+m$ qubits, provided that q is linearly bounded by n. The fact that we consider these states instead of states of the form $|\Phi^+\rangle_{VP_1\dots P_m}\otimes|\varphi'\rangle$ of $2q+m$ qubits, which would be the case if the quantum information was sent at the speed of light in vacuum, is the reason why we attain security even if V_0 sends the qubits arbitrarily slow in the protocol. The former are a broader class of states, and capture any transformation that (even globally) Alice and Bob can perform to states of the latter form.

8.3 Security of $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$

In this section, we show that $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ is *sound* by proving that the probability that attackers who pre-share a linear number of qubits (in n) are accepted at the claimed location is exponentially small in m. To enhance readability, we adopt the following notation:

1. we omit $(\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m})$ in $\omega_S(\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m})$, and variants of ω_S (see below),
2. we define, for all $x,y\in\{0,1\}^n$ and $a\in\{0,1\}^m$,
$$M_a^{f(x,y)} := H^{f(x,y)}|a\rangle\langle a|_V H^{f(x,y)}, \tag{8.3}$$
for the measurement that V_0 performs, and
3. given a strategy $\mathbf{S}=\{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$, we introduce, for all $x,y\in\{0,1\}^n$,
$$\Pi_{AB}^{xy} := \sum_a \left(M_a^{f(x,y)} \otimes \sum_{a':d_H(a,a')\le m p_{err}} A_{a'}^{xy}\otimes B_{a'}^{xy} \right), \tag{8.4}$$

in this way, we have
$$\omega_S = \frac{1}{2^{2n}}\sum_{x,y}\mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|]. \tag{8.5}$$

In addition, the following expression will appear often, and we will use the following shorthand notation
$$\nu_{p_{err}} := 2^{h(p_{err})}\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right). \tag{8.6}$$

Ideally, Alice and Bob should prepare a 'good enough' attack for every $(x,y) \in \{0,1\}^{2n}$, however, we do not have control of what potential attackers might do. For this reason, we introduce the following concept for attacks that are 'good enough' for a certain set of pairs of (x,y), meaning that for those pairs they have a probability of successfully attacking the protocol which is above a certain threshold ω_0, which defines 'good enough'.

8.3.1. Definition. *Let $\omega_0, \beta \in (0,1]$. A q-qubit strategy $\mathbf{S}$ for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ is a $(\omega_0, q, \beta \cdot 2^{2n})$-strategy for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ if there exists a set $\mathcal{B} \subseteq \{0,1\}^{2n}$ with $|\mathcal{B}| \geq \beta \cdot 2^{2n}$ such that*

$$\mathrm{Tr}[\Pi_{AB}^{xy} |\psi_{xy}\rangle\langle\psi_{xy}|] \geq \omega_0, \quad \forall (x,y) \in \mathcal{B}. \tag{8.7}$$

Notice that the choice of the function f will determine the probability distribution of the basis $f(x,y) = z \in \{0,1\}^m$ in which the m qubits have to be measured in the protocol. We denote this probability distribution by $q_f(z)$, which is given by

$$q_f(z) = \frac{|\{x,y \mid f(x,y) = z\}|}{2^{2n}} =: \frac{n_z}{2^{2n}}, \tag{8.8}$$

where we denote by n_z the number of pairs (x,y) such that $f(x,y) = z$. We say that *f reproduces a uniform distribution over $z \in \{0,1\}^m$* if $q_f(z) = \frac{1}{2^m} \forall z \in \{0,1\}^m$.

In [TFKW13], the security of the m-fold parallel repetition of $\mathrm{QPV}_{\mathrm{BB84}}$ ($\mathrm{QPV}_{\mathrm{BB84}}^{\times m}$) was analyzed in the No-PE model, and the authors showed that the protocol has exponentially small (in the quantum information m) soundness, provided that the quantum information travels at the speed of light.

Consider now the *fixed initial-state* (FIS) attack model, which we define as the attack model where step 2. in the general attack is constrained by imposing $|\psi_{xy}\rangle \to |\psi\rangle$ for all $x,y \in \{0,1\}^n$, i.e. strategies of the form $\mathbf{S}_{\mathrm{FIS}} = \{|\varphi\rangle, U^x = \mathbb{I}, V^y = \mathbb{I}, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$. Then, the same reduction to a monogamy-of-entanglement game as in [TFKW13] to show security of $\mathrm{QPV}_{\mathrm{BB84}}^{\times m}$ holds for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$. In particular, we have that for all functions f such that reproduce a uniform distribution on the bases in which the qubits have to be measured, i.e. $q_f(z) = \frac{1}{2^m}$ for all $z \in \{0,1\}^m$, the result in [TFKW13] translates to the following lemma. Not surprisingly, the reduction can be done to strategies $\mathbf{S}_{\mathrm{FIS}}$ where $\{A_a^{xy}\}_a$ and $\{B_b^{xy}\}_b$ only depend on $z = f(x,y)$ instead of x and y, i.e. $\{A_a^z\}_a$ and $\{B_b^z\}_b$, see proof of Lemma 8.3.2.

8.3.2. Lemma. *(Adapted version of eq. (9) in [TFKW13]). For every function f such that reproduces a uniform distribution over $z \in \{0,1\}^m$, the following holds for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$:*

$$\omega_{FIS}^* := \sup_{\mathbf{S}_{FIS}} \omega_{S_{FIS}} \leq (\nu_{p_{err}})^m. \tag{8.9}$$

Recall that $\nu_{p_{err}}$ is defined in (8.6).

8.3.3. Remark. For $p_{err} = 0$, Lemma 8.3.2 is tight, since the strategy $\mathbf{S}_{\mathrm{TFKW}}$ described in Chapter 4 [TFKW13] consisting Alice and Bob preparing sharing the state $|\psi\rangle_V = \otimes_{i=1}^m(\cos\frac{\pi}{8}|0\rangle_{V_0^i} + \sin\frac{\pi}{8}|1\rangle_{V_0^i})$, i.e. sending m times to the so-called Breidbart state, and both attackers answering the m-bit string $v = 0\ldots0$, which reaches the upper bound $(\frac{1}{2} + \frac{1}{2\sqrt{2}})^m$.

Proof:
From (8.1), we have that for $\mathbf{S}_{\mathrm{FIS}} = \{|\varphi\rangle, U^x = \mathbb{I}, V^y = \mathbb{I}, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$,

$$\begin{aligned}\omega_{S_{\mathrm{FIS}}} &= \frac{1}{2^{2n}}\sum_{x,y,a}\mathrm{Tr}\left[\left(M_a^{f(x,y)}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right]\\ &= \sum_z\frac{q_f(z)}{n_z}\sum_a\sum_{x,y:f(x,y)=z}\mathrm{Tr}\left[\left(M_a^{z}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right]\\ &\leq \sum_z\frac{q_f(z)}{n_z}\sum_a n_z\max_{x,y:f(x,y)=z}\mathrm{Tr}\left[\left(M_a^{z}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right].\end{aligned} \tag{8.10}$$

Then, denoting by $A_{a'}^z$ and $B_{a'}^z$ the corresponding $A_{a'}^{xy}$ and $B_{a'}^{xy}$ (recall that these x and y are such that $f(x,y) = z$) that attain the maximum in the last inequality, we have that

$$\omega_{S_{\mathrm{FS}}} \leq \frac{1}{2^m}\sum_z\sum_a\mathrm{Tr}\left[\left(M_a^{z}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{z}\otimes B_{a'}^{z}\right)|\psi\rangle\langle\psi|\right]. \tag{8.11}$$

In [TFKW13], it is proven that the right-hand-side of (8.11) is upper bounded by $(\nu_{p_{err}})^m$. □

A quantity that will be of interest is given by the maximum winning probability whenever we fix $|\psi\rangle_{VA'B'}$ in a strategy $\mathbf{S}_{\mathrm{FIS}}$, we denote this quantity by ω_ψ^*, i.e.

$$\omega_\psi^* := \max_{\{A_a^{xy}\}_a,\{B_b^{xy}\}_b}\frac{1}{2^{2n}}\sum_{x,y,a}\mathrm{Tr}\left[\left(M_a^{f(x,y)}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right]. \tag{8.12}$$

As an immediate consequence of Lemma 8.3.2, we have:

8.3.4. Corollary. *For every quantum state* $|\psi\rangle_{VA'B'}$*, with arbitrary registers* A' *and* B'*, for every function* f *such that reproduces a uniform distribution over* $z \in \{0,1\}^m$*, the following holds for* $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$*:*

$$\omega_\psi^* \leq (\nu_{p_{err}})^m. \tag{8.13}$$

Lemma 8.3.2 applies for functions f such that reproduce a uniform distribution over $z \in \{0,1\}^m$, however, while not all functions f might be good to use to implement $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$, e.g. the constant function, only considering uniform distributed values of z restricts the number of functions that we can consider. We will now show that we can still obtain upper bounds for ω^*_{FIS} for a large class of functions, namely those f that reproduce a distribution over z's that is not very far away from the uniform distribution. This class of functions can be made larger by choosing n larger than m, see below. We will see that if one writes the distribution $q_f(z)$ as the uniform distribution plus a deviation, i.e.

$$q_f(z) = \frac{1}{2^m} + \delta_f(z), \tag{8.14}$$

for most of the functions f, $\delta_f(z)$ will be small for most of $z \in \{0,1\}^m$. In order to analyze the probability distribution over the outputs z induced by a random function f, consider the random variable $Q_f(z) = \frac{N_z}{2^m}$ where N_z is the random variable representing the number of times that z appears as an output of f. The values that the random variables $Q_f(z)$ and N_z take will be denoted by $q_f(z)$ and n_z, respectively. Since f is a random function, N_z follows a binomial distribution

$$N_z \sim B\left(2^{2n}, \frac{1}{2^m}\right), \tag{8.15}$$

where 2^{2n} is the number of trials (possible x and y) and $\frac{1}{2^m}$ is the probability of success ('hitting z'). Then, we have that $\mathbb{E}_f[N_z] = 2^{2n-m}$ and thus, the expected value of $Q_f(z)$ is given by

$$\mathbb{E}_f[Q_f(z)] = \frac{\mathbb{E}[N_z]}{2^{2n}} = \frac{2^{2n-m}}{2^{2n}} = \frac{1}{2^m}. \tag{8.16}$$

Using the Chernoff bound [Che52], we can state the following proposition:

8.3.5. Proposition. *Let $\varepsilon > 0$. Then, for a random function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$, with probability at least $1-\varepsilon$, a fixed $z \in \{0,1\}^m$ satisfies*

$$q_f(z) \in \left[\frac{1}{2^m} \pm \frac{\sqrt{3\ln(2/\varepsilon)}}{2^{n+m/2}}\right]. \tag{8.17}$$

From Proposition 8.3.5, we see that for a random function f, if n is large enough (compared to m), then with probability $1-\varepsilon$, the deviation from the uniform distribution $|\delta_f(z)| \leq \frac{\sqrt{3\ln(2/\varepsilon)}}{2^{n+m/2}}$ is small. We introduce the set of functions

$$\mathcal{F}_\varepsilon := \left\{ f : \{0,1\}^{2n} \to \{0,1\}^m \mid q_f(z) \in \left[\frac{1}{2^m} \pm \frac{\sqrt{3\ln(2/\varepsilon)}}{2^{n+m/2}}\right] \forall z \in \{0,1\}^m \right\}, \tag{8.18}$$

which, intuitively, corresponds to the functions $f:\{0,1\}^{2n}\to\{0,1\}^m$ that reproduce a distribution over $\{0,1\}^m$ that is not too far from uniform. Notice that, from Proposition 8.3.5, a random $f:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^m$ will be in $\mathcal{F}_\varepsilon$ with probability $(1-\varepsilon)^{2^m}$, and, using Bernoulli's inequality, this probability is greater than $1-\varepsilon 2^m$, which by properly picking ε, this probability can be made large. We now prove an upper bound for ω_ψ^* for all these functions in $\mathcal{F}_\varepsilon$.

8.3.6. Lemma. *Let $\varepsilon>0$. Then, for every $f\in\mathcal{F}_\varepsilon$ the following bound holds for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$: for every quantum state $|\psi\rangle_{VA'B'}$, with arbitrary dimensional registers A' and B',*

$$\omega_\psi^*\leq(\nu_{p_{err}})^m\big(1+\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}\big). \tag{8.19}$$

Notice that the above upper bound is exponentially small in m if $n>(\frac{1}{2}-\log\frac{1}{\nu_{p_{err}}})m$, i.e. achieving better security requires more classical information than quantum information.

Proof:
We have that for every quantum state $|\psi\rangle_{VA'B'}$,

$$\begin{aligned}
\omega_\psi^* &= \max_{\{A_a^{xy}\}_a,\{B_b^{xy}\}_b}\frac{1}{2^{2n}}\sum_{x,y,a}\mathrm{Tr}\left[\left(M_a^{f(x,y)}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right]\\
&= \max_{\{A_a^{xy}\}_a,\{B_b^{xy}\}_b}\sum_z\frac{q_f(z)}{n_z}\sum_{x,y:f(x,y)=z}\sum_a\mathrm{Tr}\left[\left(M_a^{f(x,y)}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right]\\
&= \max_{\{A_a^{xy}\}_a,\{B_b^{xy}\}_b}\sum_z\frac{q_f(z)}{n_z}\sum_a\mathrm{Tr}\left[\left(M_a^{z}\otimes\sum_{\substack{x,y:f(x,y)=z\\ a':d_H(a,a')\leq mp_{err}}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right].
\end{aligned}$$

Consider the following upper bound

$$\begin{aligned}
&\sum_{x,y:f(x,y)=z}\mathrm{Tr}\left[\left(M_a^{z}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right]\\
&\leq n_z\max_{x,y:f(x,y)=z}\mathrm{Tr}\left[\left(M_a^{z}\otimes\sum_{a':d_H(a,a')\leq mp_{err}}A_{a'}^{xy}\otimes B_{a'}^{xy}\right)|\psi\rangle\langle\psi|\right],
\end{aligned}\tag{8.20}$$

then, denoting by $A_{a'}^z$ and $B_{a'}^z$ the corresponding $A_{a'}^{xy}$ and $B_{a'}^{xy}$ (recall that these x and y are such that $f(x,y)=z$) that attain the maximum in the right-hand

side of (8.20), we have that

$$\begin{aligned}
\omega_\psi^* &\leq \max_{\{A_a^z\}_a,\{B_b^z\}_b} \sum_z q_f(z) \sum_a \mathrm{Tr}\left[\left(M_a^z \otimes \sum_{a':d_H(a,a')\leq mp_{err}} A_{a'}^z \otimes B_{a'}^z\right)|\psi\rangle\langle\psi|\right] \\
&\leq \max_{\{A_a^z\}_a,\{B_b^z\}_b} \sum_z \frac{1}{2^m} \sum_a \mathrm{Tr}\left[\left(M_a^z \otimes \sum_{a':d_H(a,a')\leq mp_{err}} A_{a'}^z \otimes B_{a'}^z\right)|\psi\rangle\langle\psi|\right] \\
&+ \max_{\{A_a^z\}_a,\{B_b^z\}_b} \sum_z \delta_f(z) \sum_a \mathrm{Tr}\left[\left(M_a^z \otimes \sum_{a':d_H(a,a')\leq mp_{err}} A_{a'}^z \otimes B_{a'}^z\right)|\psi\rangle\langle\psi|\right] \\
&\leq (\nu_{p_{err}})^m + 2^m\Big(\max_z |\delta_f(z)|\Big) \max_{\{A_a^z\}_a,\{B_b^z\}_b} \sum_z \sum_a \mathrm{Tr}\left[\left(M_a^z \otimes \sum_{a':d_H(a,a')\leq mp_{err}} A_{a'}^z \otimes B_{a'}^z\right)|\psi\rangle\langle\psi|\right].
\end{aligned} \tag{8.21}$$

Where we used $q_f(z) = \frac{1}{2^m} + \delta_f(z)$ and Corollary 8.3.4.

Since $f \in \mathcal{F}_\varepsilon$, we have that $\max_z |\delta_f(z)| \leq \frac{\sqrt{3\ln(2/\varepsilon)}}{2^{n+m/2}}$, and applying again Corollary 8.3.4, we have that

$$\omega_\psi \leq (\nu_{p_{err}})^m + (\nu_{p_{err}})^m \sqrt{3\ln(2/\varepsilon)} 2^{-n+m/2}. \tag{8.22}$$

□

Now, consider the following subset of $\mathcal{F}_\varepsilon$:

$$\mathcal{F}_\varepsilon^* := \Big\{ f \in \mathcal{F}_\varepsilon \text{ with } \sqrt{3\ln(2/\varepsilon)} 2^{-n+m/2} < 2^{-2} \Big\}. \tag{8.23}$$

notice that $\sqrt{3\ln(2/\varepsilon)} 2^{-n+m/2} < 2^{-2}$ is not overly restrictive and can be easily achieved by picking n larger than $m/2$. Next, we will show that for any function $f \in \mathcal{F}_\varepsilon^*$, if a quantum state $|\psi\rangle_{VA'B'}$ is 'good' to attack a given basis $z \in \{0,1\}^m$—meaning that the probability to successfully attack z is above the bound in Lemma 8.3.6, see Definition 8.3.7—then, this state can only be good for a small fraction of all the possible z's. Then, similarly as argued in [BCS22] for $\mathrm{QPV}_{\mathrm{BB84}}^f$, and also in Chapter 4, we will use this to show that the attackers are restricted and, in some sense, they have to decide a small set of possible z's to attack in step 2. of the general attack (before they communicate and learn z).

8.3.7. Definition. *Let $\varepsilon, \Delta > 0$. We say that a state $|\psi\rangle_{VA'B'}$ is* Δ–good to attack $z \in \{0,1\}^m$ *for* $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ *if there exists POVMs $\{A_a^z\}_a$ and $\{B_b^z\}_b$ acting on A' and B', respectively, such that the probability that the verifiers* accept *on input z (the left-hand side of the following inequality) is such that*

$$\sum_a \mathrm{Tr}\left[\left(M_a^z \otimes \sum_{a':d_H(a,a')\leq mp_{err}} A_{a'}^z \otimes B_{a'}^z\right)|\psi\rangle\langle\psi|\right] \geq (\nu_{p_{err}} + \Delta)^m\Big(1 + 3\sqrt{3\ln(2/\varepsilon)} 2^{-n+m/2}\Big).$$

We will see that we will have freedom to choose $\Delta > 0$. For now, we only require that Δ is such that $\nu_{p_{err}} + \Delta < 1$ to ensure that the bound in Definition 8.3.7 is nontrivial.

8.3.8. Lemma. *Let $\varepsilon, \Delta > 0$. Then, for every $f \in \mathcal{F}_\varepsilon^*$, any quantum state $|\psi\rangle_{VA'B'}$ can be $\Delta-$good for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ on at most a fraction of all the possible $z \in \{0,1\}^m$ given by*

$$\left(\frac{\nu_{p_{err}}}{\nu_{p_{err}} + \Delta}\right)^m. \tag{8.24}$$

Proof:
Let $I_\psi = \{z \in \{0,1\}^m \mid |\psi\rangle_{VA'B'} \text{ is } \Delta-\text{good to attack } z\}$. We want to upper bound the size of I_ψ. By Lemma 8.3.6, see (8.21),

$$\begin{aligned}
&(\nu_{p_{err}})^m\Big(1 + \sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}\Big) \\
&\geq \omega_\psi^* = \max_{\{A_a^z\}_a, \{B_b^z\}_b} \sum_{z\in\{0,1\}^m} q_f(z) \sum_a \mathrm{Tr}\left[\left(M_a^z \otimes \sum_{a': d_H(a,a')\leq m p_{err}} A_{a'}^z \otimes B_{a'}^z\right)|\psi\rangle\langle\psi|_{VA'B'}\right] \\
&\geq \max_{\{A_a^z\}_a, \{B_b^z\}_b} \sum_{z\in I_\psi} q_f(z) \sum_a \mathrm{Tr}\left[\left(M_a^z \otimes \sum_{a': d_H(a,a')\leq m p_{err}} A_{a'}^z \otimes B_{a'}^z\right)|\psi\rangle\langle\psi|_{VA'B'}\right] \\
&\geq (\nu_{p_{err}} + \Delta)^m\Big(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}\Big) \sum_{z\in I_\psi} \Big(\frac{1}{2^m} - \sqrt{3\ln(2/\varepsilon)}2^{-n-m/2}\Big),
\end{aligned} \tag{8.25}$$

where in the second inequality we just summed over a smaller set of non-negative elements, and the third inequality comes from the hypothesis the $|\psi\rangle_{VAB}$ is $\Delta-$good for z for all $z \in I_\psi$. Then, since the element in the summand do not depend on z, we have that

$$|I_\psi| \leq \frac{(\nu_{p_{err}})^m\Big(1 + \sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}\Big)}{(\nu_{p_{err}} + \Delta)^m \frac{1}{2^m}\Big(1 - \sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}\Big)\Big(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}\Big)} \leq \left(\frac{\nu_{p_{err}}}{\nu_{p_{err}} + \Delta}\right)^m 2^m,$$

where, since $f \in \mathcal{F}_\varepsilon^*$, then $\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2} < 2^{-2}$, we used that $\frac{1+x}{1-x} \leq 1 + 3x$ for $0 \leq x < 2^{-2}$. □

In what follows, we will show that, with exponentially high probability, a uniformly drawn function $f \in \mathcal{F}_\varepsilon^*$ will be such that any q-qubit strategy $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$ with q linear in n will have exponentially small soundness. The high level idea consists of providing a classical description (up to a certain precision) of $|\varphi\rangle$, U^x and V^y, i.e. a classical description of the actions in step 2. of the general attack (before they communicate). We will show that a classical description is 'almost as good as' $\mathbf{S}$, and we will use this to show that the

description allows to recover a set of z's of size at most $2^{(1-\log\frac{\nu_{perr}+\Delta}{\nu_{perr}})m}$ for which $f(x,y)$ belongs to. This essentially consists on a (set-valued) compression of f, where we relax the condition for the attackers to have a good attack by instead of having to learn the exact value $z = f(x,y)$ they learn set of z containing $f(x,y)$, see Definition 8.3.9. Then, similarly as in [BCS22], by using a counting argument with δ-nets, we will see that if $\mathbf{S}$ has at least a certain soundness (which is still exponentially small) and q is not large enough (larger than n), then, the number of possible compressions will be exponentially smaller than the number of functions $f \in \mathcal{F}_\varepsilon^*$, and therefore attackers, with high probability, will not be able to break the protocol.

For $s \in [0,1]$, and $m \in \mathbb{N}$, we will use the notation

$$\mathcal{P}_{\leq s}(\{0,1\}^m) = \{S \subseteq \{0,1\}^m \mid |S| \leq 2^{sm}\}, \tag{8.26}$$

for the set of subsets of $\{0,1\}^m$ of size at most 2^{sm}.

8.3.9. Definition. *Let $\omega_0 \in (0,1]$, $\Delta > 0$, $s = 1 - \log\frac{\nu_{perr}+\Delta}{\nu_{perr}}$ and $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{N}$. A function*

$$g : \{0,1\}^{\kappa_1} \times \{0,1\}^{\kappa_2} \times \{0,1\}^{\kappa_3} \to \mathcal{P}_{\leq s}(\{0,1\}^m) \tag{8.27}$$

is a (ω_0, q)-set-valued classical rounding for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ of sizes $\kappa_1, \kappa_2, \kappa_3$ if for all functions $f \in \mathcal{F}_\varepsilon^*$, all $\ell \in \{1, \dots, 2^{2n}\}$, for all (ω_0, q, ℓ)−strategies for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$, there exist functions $f_A : \{0,1\}^n \to \{0,1\}^{\kappa_1}$, $f_B : \{0,1\}^n \to \{0,1\}^{\kappa_2}$ and $\mu \in \{0,1\}^{\kappa_3}$ such that, on at least ℓ pairs (x,y),

$$f(x,y) \in g(f_A(x), f_B(y), \mu). \tag{8.28}$$

Next, we will construct a set-valued classical rounding using a discretization of a strategy $\mathbf{S}$. To this end, we define an approximation of $\mathbf{S}$—will show that can be constructed with a classical description (discretization) of $\mathbf{S}$, see proof of Lemma 8.3.13—and we use the following lemmas to prove that an approximation preserves the probabilities induced by $\mathbf{S}$ up to a small constant, see Lemma 8.3.12.

8.3.10. Definition. *Let $\delta \in (0,1)$. A* δ−approximation *of a strategy $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$ is the tuple $\mathbf{S}_\delta = \{|\varphi_\delta\rangle, U_\delta^x, V_\delta^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$, where $|\varphi_\delta\rangle$, U_δ^x and V_δ^y are such that, for every $x, y \in \{0,1\}^n$,*

$$\||\varphi\rangle - |\varphi_\delta\rangle\|_2 \leq \delta, \ \|U^x - U_\delta^x\|_\infty \leq \delta, \text{ and } \|V^y - V_\delta^y\|_\infty \leq \delta. \tag{8.29}$$

We will use the notation $|\psi_{xy}^\delta\rangle := U_\delta^x \otimes V_\delta^y |\varphi_\delta\rangle$.

Since the purified distance is an upper bound of the trace distance, we have that, from Proposition 4.2.5, and Lemma 4.3.3,

8.3.11. Corollary. *Let $|x\rangle$, $|y\rangle$ be two unit complex-vectors of the same dimension. Then,*

$$\frac{1}{2}\||x\rangle\langle x| - |y\rangle\langle y|\|_1 \leq \||x\rangle - |y\rangle\|_2. \tag{8.30}$$

8.3.12. Lemma. *Let* $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$ *be a* $q-$*qubit strategy for* $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$. *Then, every* $\delta-$approximation *of* $\mathbf{S}$, *fulfills the following inequality for all* (x,y)*:*

$$\mathrm{Tr}\big[\Pi_{AB}^{xy}|\psi_{xy}^{\delta}\rangle\langle\psi_{xy}^{\delta}|\big] \geq \mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] - 7\delta. \tag{8.31}$$

Lemma 8.3.12 essentially tells us that a δ-approximation of a strategy $\mathbf{S}$ does not change much the probabilities induced by $\mathbf{S}$, and, therefore, it captures the essence of it, providing probabilities that are 'almost as good as' the original ones. As an immediate consequence we have that for every δ-approximation $\mathbf{S}_\delta$ of $\mathbf{S}$,

$$\omega_{S_\delta} \geq \omega_S - 7\delta. \tag{8.32}$$

Proof:
Let $\mathbf{S}_\delta$ be a $\delta-$approximation of a q-qubit strategy $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$. Recall that $|\psi_{xy}^{\delta}\rangle = U_\delta^x \otimes V_\delta^y|\varphi_\delta\rangle$, for all $x, y \in \{0,1\}^n$. Then, similarly as shown in [BCS22],

$$\begin{aligned}
&\frac{1}{2}\||\psi_{xy}\rangle\langle\psi_{xy}| - |\psi_{xy}^{\delta}\rangle\langle\psi_{xy}^{\delta}|\|_1 \leq \||\psi_{xy}\rangle - |\psi_{xy}^{\delta}\rangle\|_2 = \|U^x \otimes V^y|\varphi\rangle - U_\delta^x \otimes V_\delta^y|\varphi_\delta\rangle\|_2 \\
&\quad = \|(U^x - U_\delta^x + U_\delta^x) \otimes (V^y - V_\delta^y + V_\delta^y)|\varphi\rangle - U_\delta^x \otimes V_\delta^y|\varphi_\delta\rangle\|_2 \\
&\quad \leq 3\delta + 3\delta^2 + \delta^3 \leq 7\delta,
\end{aligned} \tag{8.33}$$

where in the first inequality we used Corollary 8.3.11, in the second inequality we used that $\|X \otimes Y|\xi\rangle\|_2 \leq \|X\|_\infty \|Y\|_\infty \||\xi\rangle\|_2$, by hypothesis, $\||\varphi\rangle - |\varphi_\delta\rangle\|_2 \leq \delta$, $\|U^x - U_\delta^x\|_\infty \leq \delta$, and $\|V^y - V_\delta^y\|_\infty \leq \delta$, and in the last inequality we used that $\delta^2, \delta^3 \leq \delta$ for $\delta \in (0,1)$. Then, using Proposition 4.2.5, see Chapter 4,

$$\begin{aligned}
&\mathrm{Tr}\big[\Pi^{xy}\big(|\psi_{xy}\rangle\langle\psi_{xy}| - |\psi_{xy}^{\delta}\rangle\langle\psi_{xy}^{\delta}|\big)\big] \leq \big|\mathrm{Tr}\big[\Pi^{xy}\big(|\psi_{xy}\rangle\langle\psi_{xy}| - |\psi_{xy}^{\delta}\rangle\langle\psi_{xy}^{\delta}|\big)\big]\big| \\
&\leq \frac{1}{2}\||\psi_{xy}\rangle\langle\psi_{xy}| - |\psi_{xy}^{\delta}\rangle\langle\psi_{xy}^{\delta}|\|_1 \|\Pi^{xy}\| \leq \frac{1}{2}\||\psi_{xy}\rangle\langle\psi_{xy}| - |\psi_{xy}^{\delta}\rangle\langle\psi_{xy}^{\delta}|\|_1,
\end{aligned} \tag{8.34}$$

where in the last inequality we used that $A_a^{xy} \preceq \mathbb{I}_{A'}$ and $\sum_b B_b^{xy} \preceq \mathbb{I}_{B'}$, and then we have that

$$\Pi_{AB}^{xy} \preceq \sum_a M_a^{f(x,y)} \otimes \mathbb{I}_{A'} \otimes \mathbb{I}_{B'} = \mathbb{I}_{VAB}, \tag{8.35}$$

and thus, $\|\Pi_{AB}^{xy}\| \leq \|\mathbb{I}_{VA'B'}\| = 1$. Combining (8.33) and (8.34), we have that

$$\mathrm{Tr}\big[\Pi_{AB}^{xy}|\psi_{xy}^{\delta}\rangle\langle\psi_{xy}^{\delta}|\big] \geq \mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] - 7\delta. \tag{8.36}$$

□

Now, we have seen that a δ-approximation of a strategy $\mathbf{S}$ captures its essence, and we will use it together with δ-nets, to construct a set-valued classical rounding. In order to do so, we will make use of the Lemma 4.2.8, stated in Chapter 4.

8.3.13. Lemma. *Let $\varepsilon, \Delta > 0$, and $\omega_0 \geq (\nu_{p_{err}} + \Delta)^m(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}) + 7 \cdot 3\Delta^m$. Then, there exists an (ω_0, q)-set-valued classical rounding for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ of sizes*

$$\kappa_1, \kappa_2 \leq \log_2\left(\frac{1}{\Delta}\right) m 2^{2q+1}, \text{ and } \kappa_3 \leq \log_2\left(\frac{1}{\Delta}\right) m 2^{2q+m+1}. \tag{8.37}$$

Proof:
As argued in Chapter 4, any state $|\varphi\rangle$ of $2q+m$ qubits can be decomposed as $|\varphi\rangle = \sum_{j=0}^{2^{2q+m}-1} \varphi_j |j\rangle$ with $\varphi_j \in \mathbb{C}$ for all $j \in [2^{2q+m}]$ and $1 = \sum_j |\varphi_j|^2 = \sum_j \mathrm{Re}(\varphi_j)^2 + \mathrm{Im}(\varphi_j)^2$. The latter corresponds to the condition for a point to be on the unit sphere in $\mathbb{R}^{2\cdot 2^{2q+m}}$, i.e. the unit $(2^{2q+m+1}-1)$-sphere and therefore the set of states can be seen as a unit sphere. Similarly, the set of unitary matrices of dimension d can be seen as the unit $(2d^2-1)$-sphere, since for every $U \in \mathcal{U}(d)$, $UU^\dagger = \mathbb{I}_d$, this will correspond to the unitaries that Alice and Bob apply in the step 2. of the general attack.

Let $\delta = 3\Delta^m$ and consider a $3\Delta^m$-net $\mathcal{N}_S$ in Euclidean norm of the $(2^{2q+m+1}-1)$-sphere, which, as argued above, corresponds to the set of quantum states of $2q+m$ qubits, i.e. the set of possible states $|\varphi\rangle_{VAB}$ that attackers will start in step 2. of the general attack. Moreover, consider $3\Delta^m$-nets $\mathcal{N}_A$ in and $\mathcal{N}_B$ in the Schatten ∞-norm of the $(2d^2-1)$-sphere, where $d = 2^q$, which, also as argued above, correspond to the set of unitary operators that Alice and Bob apply in step 2. of the general attack, respectively. Pick the these Δ^m-nets such that their cardinalities are at most $(3/\Delta^m)^{2^{2q+m+1}}$, $(3/\Delta^m)^{2d^2}$ and, $(3/\Delta^m)^{2d^2}$, respectively, which exist due to Lemma 4.2.8.

We now construct a an (ω_0, q)-set-valued classical rounding, whose sizes, as argued above, are of size at most $\kappa_1 = \kappa_2 = \log_2\left(\frac{1}{\Delta}\right) m 2^{2q+1}$, $\kappa_3 = \log_2\left(\frac{1}{\Delta}\right) m 2^{2q+m+1}$. Let $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$ be an $(\omega_0, q, \ell)-$ strategy for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$, we define

- μ as the element in $\mathcal{N}_S$ that is closest to $|\varphi\rangle$ in Euclidean norm, and denote by $|\varphi_\delta\rangle$ the state described by μ,
- $f_A(x)$ as the element in $\mathcal{N}_A$ that is closest to U^x in operator norm, and denote by U_δ^x the unitary described by $f_A(x)$,
- $f_B(y)$ as the element in $\mathcal{N}_B$ that is closest to V^y in operator norm, and denote by V_δ^y the unitary described by $f_A(y)$.

If the closest element is not unique, make an arbitrary choice. Let $|\psi_{xy}^\delta\rangle = U_\delta^x \otimes V_\delta^y |\varphi_\delta\rangle$. By construction,

$$\||\varphi\rangle - |\varphi_\delta\rangle\|_2 \leq \delta, \ \|U^x - U_\delta^x\|_\infty \leq \delta, \text{ and } \|V^y - V_\delta^y\|_\infty \leq \delta, \tag{8.38}$$

and therefore, $\mathbf{S}_\delta = \{|\varphi_\delta\rangle, U_\delta^x, V_\delta^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$ is a δ-approximation of $\mathbf{S}$. Now, define

$$g(f_A(x), f_B(y), \mu) := \{z | \exists \{A_a^z\}_a, \{B_b^z\}_b \text{ with } \sum_a \mathrm{Tr}\left[M_a^z \otimes \sum_{a': d_H(a,a') \leq m p_{err}} A_{a'}^z \otimes B_{a'}^z |\psi_{xy}^\delta\rangle\langle\psi_{xy}^\delta|\right] \geq \omega_0 - 7\delta\}. \tag{8.39}$$

Since, by hypothesis, $\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2} < \frac{1}{4}$, and $f \in \mathcal{F}_\varepsilon^*$, by Lemma 8.3.8, the right-hand side of (8.39) has cardinality at most $2^{(1-\log(\frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}}))m}$. We want to show that g is a (ω_0, q)-set-valued classical rounding (the sizes κ_1, κ_2, and κ_3 are already bounded). Consider a (ω_0, q, ℓ)–strategy, then, there exists a set $\mathcal{B} \subseteq \{0,1\}^{2n}$ with $|\mathcal{B}| \geq \ell$ such that for all $(x, y) \in \mathcal{B}$,

$$\sum_a \mathrm{Tr}\left[M_a^{f(x,y)} \otimes \sum_{a': d_H(a,a') \leq m p_{err}} A_{a'}^{xy} \otimes B_{a'}^{xy} |\psi_{xy}\rangle\langle\psi_{xy}|\right] \geq \omega_0. \tag{8.40}$$

Then, since $\mathbf{S}_\delta$ is a δ-approximation of $\mathbf{S}$, by Lemma 8.3.12, we have that, for all $(x, y) \in \mathcal{B}$

$$\sum_a \mathrm{Tr}\left[M_a^{f(x,y)} \otimes \sum_{a': d_H(a,a') \leq m p_{err}} A_{a'}^{xy} \otimes B_{a'}^{xy} |\psi_{xy}^\delta\rangle\langle\psi_{xy}^\delta|\right] \geq \omega_0 - 7\delta, \tag{8.41}$$

since $|\mathcal{B}| \geq \ell$, we have that $f(x, y) \in g(f_A(x), f_B(y), \mu)$, on at least ℓ pairs (x, y). □

A (ω_0, q)-set-valued classical rounding g for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$, defined in Definition 8.3.9, 'covers' (ω_0, q, ℓ)–strategies for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$. Next, we will show that there exists g such that if one has $f(x, y) \in g(f_A(x), f_B(y), \mu)$ on a fraction β of all the possible inputs (x, y), i.e. those pairs for which attackers prepared a 'good' attack (success probability of at least ω_0), then the number of qubits q that Alice and Bob pre-share grows with both β and n. This means that the more pairs (x, y) the attackers have to prepare a 'good' attack, the more qubits they need to pre-share. In particular, in the following lemma, we show that q grows logarithmically in β and linearly in n.

8.3.14. Lemma. *Let* $\varepsilon > 0$, $\beta \in (0, 1]$, *and* $\omega_0 \geq (\nu_{p_{err}}+\Delta)^m(1+3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2})+ 7 \cdot 3\Delta^m$. *Fix an* (ω_0, q)*-set-valued classical rounding* g *for* $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ *of sizes* $\kappa_1, \kappa_2 \leq \log_2\left(\frac{1}{\Delta}\right)m2^{2q+1}$, $\kappa_3 \leq \log_2\left(\frac{1}{\Delta}\right)m2^{2q+m+1}$. *Let* $f \in \mathcal{F}_\varepsilon^*$ *be such that for any* f_A, f_B *and* μ *as defined in Definition 8.3.9,* $f(x, y) \in g(f_A(x), f_B(y), \mu)$ *holds on more than* $\beta \cdot 2^{2n}$ *pairs* (x, y), *then with probability at least* $1 - 2^{-m2^{n-\log(1/\beta)}}$, f *is such that*

$$\log\left(\frac{1}{\Delta}\right)2^{2q+2}(1 + 2^{-n+m-1}) \geq \beta \log\left(\frac{\nu_{p_{err}} + \Delta}{\nu_{p_{err}}}\right)2^n + \frac{1}{m}2^{-n+m}\log(1 - \varepsilon). \tag{8.42}$$

Proof:
By Lemma 8.3.13, there exists an (ω_0, q)-set-valued classical rounding g of sizes $\kappa_1, \kappa_2 \leq \log_2\left(\frac{1}{\Delta}\right) m 2^{2q+1}, \log_2\left(\frac{1}{\Delta}\right) m 2^{2q+1}$, $\kappa_3 \leq \log_2\left(\frac{1}{\Delta}\right) m 2^{2q+m+1}$. The number of possible functions $g(f_A(x), f_B(y), \mu)$ that Alice and Bob can implement depends on the number of choices of $f_A : \{0,1\}^n \to \{0,1\}^{\kappa_1}$, $f_B : \{0,1\}^n \to \{0,1\}^{\kappa_2}$ and $\mu \in \{0,1\}^{\kappa_3}$. In total, there are $(2^{\kappa_1})^{2^n} \cdot (2^{\kappa_2})^{2^n} \cdot (2^{\kappa_3})$ such functions. By hypothesis, $f(x,y) \in g(f_A(x), f_B(y), \mu)$ on at least $\beta \cdot 2^{2n}$ pairs (x,y), denote by $\mathcal{B}$ the set of these (x,y), and, recalling that the cardinality of the set $g(f_A(x), f_B(y), \mu)$ is at most $2^{(1-\log \frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}})m}$, we have that, given g, the total number of ways to assign outputs for these pairs is $(2^{(1-\log \frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}})m})^{\beta 2^{2n}}$. For the remaining $(1-\beta)\cdot 2^{2n}$ pairs of (x,y), no compression is applied (i.e. we do not have the guarantee $f(x,y) \in g(f_A(x), f_B(y), \mu)$). In these cases, we have that $f(x,y) \in \{0,1\}^m$, for which we have $(2^m)^{(1-\beta)2^{2n}}$ possible ways to assign values.

On the other hand, we have seen that the cardinality of $\mathcal{F}^*$ is $(1-\varepsilon)^{2^m} 2^{m 2^{2n}}$. Then, we have that, using that $f \in \mathcal{F}^*_\varepsilon$ is drawn uniformly at random,

$$
\begin{aligned}
&\Pr\{f \in \mathcal{F}^*_\varepsilon : \exists f_A, f_B, \mu \text{ s.t. } f(x,y) \in g(f_A(x), f_B(y), \mu)\ \forall (x,y) \in \mathcal{B}\} \\
&= \frac{|f \in \mathcal{F}^*_\varepsilon : \exists f_A, f_B, \mu \text{ s.t. } f(x,y) \in g(f_A(x), f_B(y), \mu)\ \forall (x,y) \in \mathcal{B}|}{|\mathcal{F}^*_\varepsilon|} \\
&\leq \frac{\left(2^{\log_2(\frac{1}{\Delta}) m 2^{2q+1}}\right)^{2^n} \left(2^{\log_2(\frac{1}{\Delta}) m 2^{2q+1}}\right)^{2^n} \left(2^{\log_2(\frac{1}{\Delta}) m 2^{2q+m+1}}\right) (2^{(1-\log(\frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}}))m})^{\beta 2^{2n}} (2^m)^{(1-\beta)2^{2n}}}{(1-\varepsilon)^{2^m} 2^{m 2^{2m}}} \\
&= 2^{\log(\frac{1}{\Delta}) m 2^{2q+n+2}(1+2^{-n+m-1}) + 2^m \log(\frac{1}{1-\varepsilon}) - \beta \log(\frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}}) m 2^{2n}}.
\end{aligned}
\tag{8.43}
$$

Notice that the above quantity will be decreasing in m and n if the 'dominating' term is the negative one, i.e.

$$
\log(\frac{1}{\Delta}) m 2^{2q+n+2}(1 + 2^{-n+m-1}) + 2^m \log(\frac{1}{1-\varepsilon}) < \beta \log(\frac{\nu_{p_{err}} + \Delta}{\nu_{p_{err}}}) m 2^{2n}, \tag{8.44}
$$

which is the converse of condition (8.42). In particular, we have that if (8.44) holds,

$$
2^{\log(\frac{1}{\Delta}) m 2^{2q+n+2}(1+2^{-n+m-1}) + 2^m \log(\frac{1}{1-\varepsilon}) - \beta \log(\frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}}) m 2^{2n}} < 2^{-m 2^{n - \log(\frac{1}{\beta})}}. \tag{8.45}
$$

□

From (8.42), we see that, picking $n > m$ and small ε, the terms 2^{-n+m-1} and $\frac{1}{m} 2^{-n+m} \log(1-\varepsilon)$ become negligible, and in order to have a 'good' attack (i.e. $f(x,y) \in g(f_A(x), f_B(y), \mu)$) for at least $\beta \cdot 2^{2n}$ possible (x,y)'s, the inequality (8.42) becomes: "2^{2q} is approximately greater or equal to $\beta 2^n$", which implies that

$$
2q \gtrsim n - \log(1/\beta) \qquad \text{(up to constant factors)}. \tag{8.46}
$$

However, we do not have control over the number of pairs that attackers have prepared a good attack for. The following lemma states that if attackers have prepared a strategy that has at least a certain soundness, then, there must be a number of pairs (x,y) for which they prepared a good attack.

8.3.15. Lemma. *Let* $\omega_1 \in (0,1]$, *and* $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$ *be a q-qubit strategy for* $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ *such that* $\omega_S \geq \omega_1$. *Then, for* $\omega_0 < \omega_1$, *there exist at least* $\frac{\omega_1-\omega_0}{1-\omega_0}2^{2n}$ *of pairs* (x,y) *such that*

$$\mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] \geq \omega_0, \tag{8.47}$$

this is, $\mathbf{S}$ *is an* $(\omega_0, q, \frac{\omega_1-\omega_0}{1-\omega_0}2^{2n})$*-strategy.*

Proof:
Let $J := \{(x,y) \mid \mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] \geq \omega_0\}$, we want to find a lower bound on the cardinality of J, and denote by J^c its complementary set. We have that

$$\begin{aligned}\omega_1 \leq \omega_S = \frac{1}{2^{2n}}\sum_{x,y}\mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] = \frac{1}{2^{2n}}\sum_{(x,y)\in J}\mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] \\ + \frac{1}{2^{2n}}\sum_{(x,y)\in J^c}\mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] \leq \frac{1}{2^{2n}}|J| + \frac{1}{2^{2n}}\omega_0|J^c|,\end{aligned}$$

where the first inequality holds by hypothesis, and in the last inequality we used the trivial bound $\mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] \leq 1$ for $(x,y) \in J$ and we used the bound $\mathrm{Tr}[\Pi_{AB}^{xy}|\psi_{xy}\rangle\langle\psi_{xy}|] \leq \omega_0$ for $(x,y) \in J^c$. Then, using that $|J^c| = 2^{2n} - |J|$, we have that $|J| \leq \frac{\omega_1-\omega_0}{1-\omega_0}2^{2n}$. □

8.3.16. Theorem. *Let* $n > m$, $\varepsilon \leq 2^{-m-1}$ *and* $\Delta > 0$. *For every* $c < 1$, *with probability at least* $1 - 2^{-m}2^{n-cm\log(\frac{1}{\nu_{p_{err}}+\Delta})}$, *a uniformly random* $f \in \mathcal{F}_\varepsilon^*$ *will be such that, if the number of qubits* q *that the attackers pre-share to attack* $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ *is such that*

$$2q < n - cm\log\left(\frac{1}{\nu_{p_{err}}+\Delta}\right) + \log\frac{(1-(\nu_{p_{err}}+\Delta)^{1-c})\log\left(\frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}}\right)}{8\log(1/\Delta)}, \tag{8.48}$$

then, the probability that the verifiers accept *is at most*

$$((\nu_{p_{err}}+\Delta)^c)^m(1+3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}) + 7\cdot 3\Delta^m. \tag{8.49}$$

Notice that the bound in Theorem 8.3.16 exponentially decays in m if $\nu_{p_{err}} + \Delta < 1$. Moreover, since, by hypothesis $\varepsilon \leq 2^{-m-1}$, in particular we have that, under the conditions of Theorem 8.3.16, any q-qubit strategy S for $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$ is such that

$$\omega_S \leq ((\nu_{p_{err}}+\Delta)^c)^m(1+3\sqrt{3m\ln(2)}2^{-n+m/2}) + 7\cdot 3\Delta^m. \tag{8.50}$$

Theorem 8.3.16 leaves freedom to pick the values Δ and c. If one wants a lower upper bound on the soundness, these should be picked small and big, respectively. By picking Δ small enough, e.g, $\Delta = 10^{-5}$, the term $\nu_{p_{err}} + \Delta$ is strictly smaller than 1 for an error p_{err} up to roughly 3.6% and we have that up to that error, the upper bound on the soundness in Theorem 8.3.16 will decay exponentially. Notice that the asymptotic behavior of the upper bound on the soundness is

$$((\nu_{p_{err}} + \Delta)^c)^m. \tag{8.51}$$

Proof:
Let S be a q-qubit strategy S such that

$$\omega_S \geq (\nu_{p_{err}} + \Delta)^{cm}(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}) + 7 \cdot 3\Delta^m, \tag{8.52}$$

and let $\omega_0 = (\nu_{p_{err}} + \Delta)^m(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2}) + 7 \cdot 3\Delta^m$, then, by Lemma 8.3.15, S is an $(\omega_0, q, \beta \cdot 2^{2n})$-strategy, with

$$\beta = \frac{(\nu_{p_{err}} + \Delta)^{cm}(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2})(1 - (\nu_{p_{err}} + \Delta)^{(1-c)m})}{1 - (\nu_{p_{err}} + \Delta)^m(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2})}. \tag{8.53}$$

Since $3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2} \geq 0$, we have that

$$\beta \geq \frac{(\nu_{p_{err}} + \Delta)^{cm}(1 - (\nu_{p_{err}} + \Delta)^{(1-c)m})}{1 - (\nu_{p_{err}} + \Delta)^m(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2})} \geq \frac{(\nu_{p_{err}} + \Delta)^{cm}(1 - (\nu_{p_{err}} + \Delta)^{1-c})}{1 - (\nu_{p_{err}} + \Delta)^m(1 + 3\sqrt{3\ln(2/\varepsilon)}2^{-n+m/2})}, \tag{8.54}$$

where we used that $1 - (\nu_{p_{err}} + \Delta)^{cm} \geq 1 - (\nu_{p_{err}} + \Delta)^{1-c}$. Then, using the inequality $\frac{1}{1-x} \geq 1$ for $x \in (0, 1)$,

$$\beta \geq (\nu_{p_{err}} + \Delta)^{cm}(1 - (\nu_{p_{err}} + \Delta)^{1-c}) =: \beta_0, \tag{8.55}$$

then, in particular, S is a $(\omega_0, q, \beta_0 \cdot 2^{2n})$-strategy. Then, by Lemma 8.3.13, there exist an (ω_0, q)-set-valued classical rounding of sizes $\kappa_1, \kappa_2 \leq \log_2\left(\frac{1}{\Delta}\right)m2^{2q+1}$, $\kappa_3 \leq \log_2\left(\frac{1}{\Delta}\right)m2^{2q+m+1}$.

Let $f \in \mathcal{F}_\varepsilon^*$ be such that $f(x, y) \in g(f_A(x), f_B(y), \mu)$ holds on more than $\beta_0 \cdot 2^{2n}$ pairs (x, y) for any f_A, f_B and μ, by the counterstatement of Lemma 8.3.14, a uniformly random $f \in \mathcal{F}_\varepsilon^*$, with probability at least $1 - 2^{-m2^{n-\log(1/\beta)}}$, will be such that

$$\log\left(\frac{1}{\Delta}\right)2^{2q+2}(1 + 2^{-n+m-1}) \geq \beta \log\left(\frac{\nu_{p_{err}} + \Delta}{\nu_{p_{err}}}\right)2^n + \frac{1}{m}2^{-n+m}\log(1 - \varepsilon). \tag{8.56}$$

Since $n > m$, we have that $1 \geq 2^{-n+m-1}$, and, using that $\varepsilon \leq 2^{-m-1}$, the last summand above is such that

$$\frac{1}{m}2^{-n+m}\log(1 - \varepsilon) \geq -\frac{1}{m}2^{-n}, \tag{8.57}$$

where we used that $-\log(1-x) \geq 2x$ for $x \leq \frac{1}{2}$, therefore (8.57) is exponentially decreasing in n and then, we have

$$\log\left(\frac{1}{\Delta}\right) m 2^{2q+3} \geq m\beta_0 \log\left(\frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}}\right) 2^n, \tag{8.58}$$

and therefore,

$$2q+3 \geq n - cm\log\left(\frac{1}{\nu_{p_{err}}+\Delta}\right) + \log\left(1-(\nu_{p_{err}}+\Delta)^{1-c}\right) + \log\log\left(\frac{\nu_{p_{err}}+\Delta}{\nu_{p_{err}}}\right) - \log\log\frac{1}{\Delta}.$$

We have seen that, with probability at least $1-2^{-m2^{n-\log(1/\beta)}}$, a uniformly random $f \in \mathcal{F}_\varepsilon^\star$ with (8.52) implies (8.58). However, by hypothesis, we have strict inequality in the other direction in (8.58), and therefore, this implies (8.48). □

8.3.1 Improved error-tolerance for $\mathrm{QPV}_{\mathrm{BB84}}^{f}$

In [BCS22], it was shown that $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ is secure for attackers who pre-share a linear amount (in n) of qubits as long as the error remains below 2%. Here, by considering the case $m = 1$ in $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$, which corresponds to $\mathrm{QPV}_{\mathrm{BB84}}^{f}$, we show that the protocol can tolerate an error almost up to 14.6%, presenting an order-of-magnitude improvement in error tolerance.

For the case of $m = 1$, the verifiers accept if, in step 4. of the description of $\mathrm{QPV}_{\mathrm{BB84}}^{f}$, $a = v$, i.e. if they received the correct outcome. Then, applying Theorem 8.3.16 for $m = 1$ and, recall that since the acceptance criterion is binary, $\nu_{p_{err}} = \nu_0 = (\frac{1}{2} + \frac{1}{2\sqrt{2}})$, picking $\Delta = 10^{-5}$ and $c = 0.999$, then we have the following corollary:

8.3.17. Corollary. *Let $n, m \in \mathbb{N}$, with $n > m$ and $n \geq 36$, and $\varepsilon \leq 2^{-m-1}$. Then, with probability at least $1-2^{-2^{n-c\log(\frac{1}{\nu_0+\Delta})}}$, a uniformly random $f \in \mathcal{F}_\varepsilon^\star$ will be such that, if*

$$q < \frac{1}{2}n + \frac{1}{2}\log\frac{(\nu_0+\Delta)^c(1-(\nu_0+\Delta)^{1-c})\log\left(\frac{\nu_0+\Delta}{\nu_0}\right)}{8\log(1/\Delta)} \simeq \frac{1}{2}n - 17.8797, \tag{8.59}$$

any q-qubit strategy S for $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ is such that

$$\omega_S \leq \left(\frac{1}{2}+\frac{1}{2\sqrt{2}}+\Delta\right)^c (1+3\sqrt{6\ln(2)}2^{-n}) + 7\cdot 3\Delta \simeq 0.853699(1+3\sqrt{6\ln(2)}2^{-n}) + 0.00021. \tag{8.60}$$

Thus, the upper bound in (8.60) converges exponentially in n to

$$0.853909\ldots. \tag{8.61}$$

Notably, the attack described in Theorem 8.3.3 achieves a success probability of $\frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.85355\ldots$, showing that our bound is essentially tight. This implies that even if Alice and Bob share a linear amount $q = O(n)$ of pre-shared qubits, they cannot outperform an attack that relies on no pre-shared entanglement.

Essentially tight result in the error-free case

We have shown after Theorem 8.3.16 that the asymptotic behavior of the soundness of $\mathrm{QPV}_{\mathrm{BB84}}^{f:n\to m}$is given by $((\nu_{p_{err}} + \Delta)^c)^m$. Similarly as above, picking $\Delta = 10^{-5}$ and $c = 0.999$, the upper bound for the free-error case scales asymptotically as $(0.853699...)^m$, which is almost achieved by the attack described in Theorem 8.3.3 that has winning probability of $(\frac{1}{2} + \frac{1}{2\sqrt{2}})^m = (0.85355\ldots)^m$, which recall that uses no pre-shared entanglement.

Chapter 9

Entanglement in continuous-variable position verification

To conclude this thesis, we turn to *continuous-variable* (CV) quantum position verification (QPV). The decisive advantage of CV technology over discrete-variable platforms is practicality: coherent states are easier and inexpensive to generate, manipulate, and detect, building on decades of expertise from optical-communication engineering. In this chapter, we analyze a CV-QPV protocol, denoted $\mathrm{QPV}_{\mathrm{coh}}$—the natural analog of $\mathrm{QPV}_{\mathrm{BB84}}$—whose security was established in the No Pre-shared Entanglement (No-PE) model. In $\mathrm{QPV}_{\mathrm{coh}}$, one verifier sends a coherent quantum state while the other transmits a classical bit z that specifies the measurement the prover must perform. As with $\mathrm{QPV}_{\mathrm{BB84}}$, two shortcomings persist: adversaries who share a maximally entangled CV resource can execute a perfect teleportation attack[1] , and the quantum signal must propagate at the speed of light—issues (i) and (iii) from Chapter 1, illustrated in Figure 1.4.

This chapter adopts the function-splitting variation used for $\mathrm{QPV}_{\mathrm{BB84}}$ and $\mathrm{QPV}_{\mathrm{rout}}$ (Chapters 4 and 8): the single bit z is replaced by two n-bit strings $x, y \in \{0,1\}^n$ chosen by the verifiers, with $z = f(x,y)$ for a prescribed Boolean function f. We show that the resulting protocol, $\mathrm{QPV}^{f}_{\mathrm{coh}}$, inherits the favorable security guarantees of $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ (Chapter 4): it is secure (i) against attackers possessing fewer than cn pre-shared entangled qubits, for some constant c; (ii) under a constant fraction of attenuation and noise/error; and (iii) even when the quantum information propagates arbitrarily slowly. Consequently, $\mathrm{QPV}^{f}_{\mathrm{coh}}$ emerges as an experimentally economical candidate that simultaneously overcomes the three principal obstacles of quantum position verification.

The results presented in this chapter are based on the following publication:

- "Continuous-variable quantum position verification secure against entangled attackers", by Llorenç Escolà-Farràs, Arpan Akash Ray, Rene Allerstorfer, Boris Škorić, and Florian Speelman [EFRA+24].

[1] Perfection requires infinite energy; however, finite energy can still make it effective.

9.1 Introduction

Recent work has focused on the practicality of implementing position-verification protocols. Aspects such as channel loss and error tolerance of certain QPV protocols have begun to be taken into consideration [ABSL22a, EFS23, ABB+23]. Moreover, most previous QPV protocols have been based on finite-dimensional quantum systems, with the exception of [QS15, AEFR+23]. Continuous-variable quantum systems are relevant for quantum communication and quantum-limited detection and imaging techniques, as they provide a quantum description of the propagating electromagnetic field. Much research has been conducted on continuous-variable quantum key distribution (QKD). Initially proposed using discrete [Ral99, Hil00, Rei00] and Gaussian [CLA01] representations of squeezed states, a range of techniques were subsequently introduced for Gaussian-encoded continuous-variable quantum key distribution (CV-QKD) using coherent states [GG02, GAW+03, GCW+03, WLB+04].

The primary advantage of CV-QKD over its discrete-variable (DV) analog is practicality, see e.g. [WPGP+12]. Fundamentally, CV systems are much simpler to handle and leverage several decades of experience in coherent optical communication technology. Unlike DV systems, no true single-photon preparation or detection is necessary, which is still expensive and technically challenging (especially if photon number resolution is desired). In contrast, homodyne and heterodyne measurements are much easier and cheaper to implement. Much existing infrastructure is geared towards handling light at low-loss telecom wavelengths (1310nm, 1550nm), whereas an ideal single photon source in these wavelength bands still has to be discovered, and frequency up-conversion is challenging and introduces new losses and errors.

In [AEFR+23], the CV analog of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol [KMS11] based on BB84 states [BB84] was defined and analyzed. In this chapter, we extend the CV-QPV literature by considering the CV version of the practically interesting $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [BCS22, EFS23] protocol, see Chapter 4. Crucially, in $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ the classical input information is split up (into, say, x, y) and each verifier sends out either x or y. The prover then applies the appropriate measurement based on the value $f(x, y)$ for the chosen protocol function f. The advantage of this is that the quantum resources required for a successful attack become larger and scale linearly in the size n of the *classical* input strings x, y. Thus, increasing the classical input size makes the quantum attack harder—a very favorable property of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. We are theoretically, and also potentially practically, motivated to investigate whether this property holds the same way in the CV case as well. Employing previous results from [BCS22] and [AEFR+23], the main take-away of this chapter is that, indeed, the CV protocol shares the desired characteristics regarding entanglement attacks of the discrete variable version. More concretely, we show that, for a random Boolean function f, the protocol remains secure against attackers who pre-share CV entangled states with a cutoff at the photon

number linear in n. Moreover, the protocol remains secure even if the quantum information is sent arbitrarily slowly. We also present an analysis of the protocol for non-zero levels of attenuation and excess noise in the CV channel.

9.2 The $\mathrm{QPV}^{f}_{\mathrm{coh}}$ protocol

Based on the ideas in [BFSS13, Unr14, BCS22], we introduce a variation of the quantum position verification protocol studied in [AEFR+23]. Instead of only a single verifier sending classical information, both verifiers send classical information that, combined, determines the action of the prover. When sent through a channel, a continuous-variable state gets attenuated and acquires excess noise. We will denote by $t \in [0,1]$ the attenuation parameter, and by $u \geq 0$ the excess noise power of the quantum channel connecting V_0 and P. The excess noise can be modeled as $u = u_0\sigma^2$, with, for instance, a reasonable $u_0 = 0.01$, due to the prevalence of phase noise [LPF+18]. The protocol becomes insecure for $u > 0.25$, and thus the constant u_0 places a practical upper limit on the modulation variance σ. Then, the protocol is described as follows:

9.2.1. Definition. *Let $n \in \mathbb{N}$ and consider a $2n$-bit boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. A round of the $\mathrm{QPV}^{f}_{\mathrm{coh}}$ protocol is described as follows.*

1. *The verifiers V_0 and V_1 randomly choose bit strings $x, y \in \{0,1\}^n$, respectively. They draw two random variables $(\xi, \xi^{\perp})$ from the Gaussian distribution $\mathcal{N}_{0,\sigma^2}$, for $\sigma \gg 1$, and compute $f(x,y)$. Verifier V_0 prepares a coherent state $|\phi\rangle$ with quadratures $(x_0, p_0) = (\xi\cos\theta + \xi^{\perp}\sin\theta,\ \xi\sin\theta - \xi^{\perp}\cos\theta)$, where $\theta = 0$ if $f(x,y) = 0$ and $\theta = \frac{\pi}{2}$ if $f(x,y) = 1$.*

2. *The verifier V_0 sends $|\phi\rangle$ and x to P, and the verifier V_1 sends y to P so that x and y arrive simultaneously at pos. The quantum information can arrive earlier and is only required to be present at pos when the classical information arrives. The classical information is required to travel at the speed of light, whereas the quantum information can be sent arbitrarily slowly.*

3. *Immediately, P computes $f(x,y)$ and performs a homodyne measurement on $|\phi\rangle$ in the direction $\theta = 0$ if $f(x,y) = 0$ or $\theta = \frac{\pi}{2}$ if $f(x,y) = 1$, resulting in a value $\xi_{\mathsf{P}} \in \mathbb{R}$. The prover broadcasts the classical result ξ_{P} to both verifiers at the speed of light.*

See Figure 9.1 for a schematic representation of one round of the $\mathrm{QPV}^{f}_{\mathrm{coh}}$ protocol. Notice that, since the homodyne measurement is performed along the θ direction, the component $\xi^{\perp}$ does not affect the measurement outcome. Therefore, the choice of $\xi^{\perp}$ has no impact on the protocol.

In order to decide whether to *accept* or *reject* the prover's location, the verifiers execute r sequential repetitions of the $\mathrm{QPV}^{f}_{\mathrm{coh}}$ protocol. We present a statistical

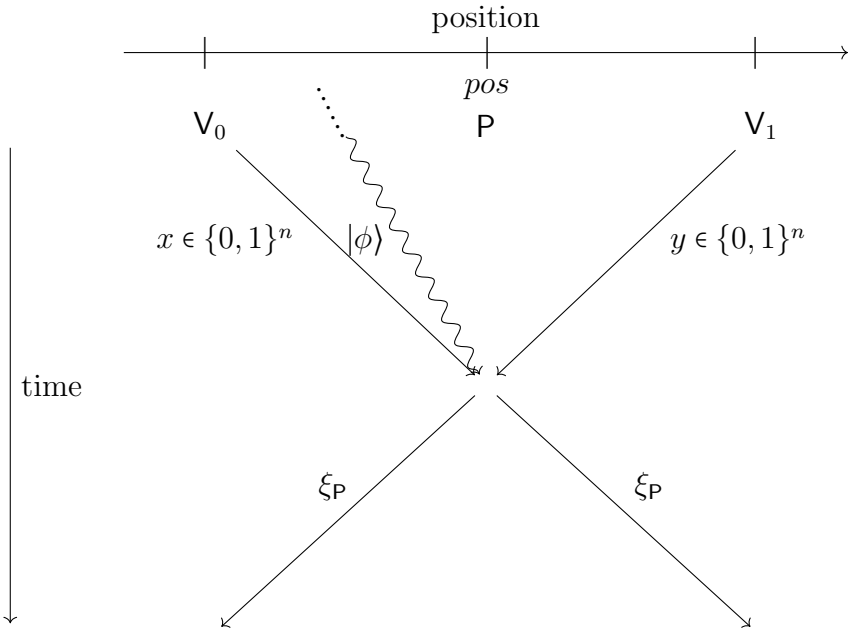


Figure 9.1: Schematic representation of one round of the $\mathrm{QPV}^{f}_{\mathrm{coh}}$ protocol. The coherent state $|\phi\rangle$ originates from V_0 in the past.

test that enables this decision. In each round, the verifiers sample $(\xi_i)_{i=1}^r$ from the Gaussian distribution $\mathcal{N}(0,\sigma^2)$, and receive a corresponding set of prover responses $(\xi_{\mathsf{P}_i})_{i=1}^r$. In the ith round, the honest prover performs a homodyne measurement at angle θ_i on a coherent state with displacement ξ_i in the θ_i direction (and displacement $\xi_i^\perp$ in the orthogonal direction $\theta_i + \frac{\pi}{2}$). Similarly as in Sections 3.2.2 and 4.2.2, we define the *score* (or *payoff function*) Γ_r as:

$$\Gamma_r = \sum_{i=1}^{r} \frac{(\xi_{\mathsf{P}_i} - \xi_i\sqrt{t})^2}{1/2 + u}. \tag{9.1}$$

Since $(\xi_{\mathsf{P}_i})_i$ are Gaussian-distributed, Γ_r will follow a chi-square distribution with parameter r. Then, we use the following lemma to establish a decision criterion.

9.2.2. Lemma. *(Eq.(4.3) in [LM00]) Let X be sampled from a χ^2_r distributed random variable. Then, for all $a > 0$, the following holds:*

$$\Pr\big[X - r \geq 2\sqrt{ra} + 2a\big] \leq e^{-a}. \tag{9.2}$$

Next, we provide a test to verify the location of the honest prover with a confidence level of $\varepsilon_{\mathrm{h}} > 0$.

9.2.3. Definition. *Let* $\varepsilon_h > 0$. *For the* $\mathrm{QPV}_{\mathrm{coh}}$ *protocol executed sequentially* r *times, we define the acceptance test* $\mathsf{T}_{\varepsilon_h}^{r-\mathrm{coh}}$, *also referred to as the decision criterion, as follows: the verifiers* accept *the prover's location if*

$$\Gamma_r \leq r + \frac{2}{\sqrt{r}}\sqrt{\ln(1/\varepsilon_h)} + \frac{2}{r}\ln(1/\varepsilon_h) =: \gamma_r. \tag{9.3}$$

Otherwise, they reject.

The bound in Lemma 9.2.2 guarantees that an honest prover will be accepted except with small probability at most ε_{h} (*completeness*). We will prove that attackers who pre-share a linear amount of qubits in n, will fail the test $\mathsf{T}_{\varepsilon_{\mathrm{h}}}^{r-\mathrm{coh}}$ with probability $1 - O(\varepsilon_{\mathrm{h}})$ (*soundness*). Showing both completeness and soundness implies that the protocol is *secure*.

The protocol in [AEFR+23] is as in Definition 9.2.1 but instead of sending x and y, V_1 directly sends θ. For the honest party, the only difference is that he has to compute $f(x, y)$ to determine θ. We will use the following notation, for $\theta \in \{0, \frac{\pi}{2}\}$ we will denote by $\bar{\theta}$ the remaining value, i.e. if $\theta = 0$, then $\bar{\theta} = \frac{\pi}{2}$ and if $\theta = \frac{\pi}{2}$, then $\bar{\theta} = 0$.

The honest prover's uncertainty about the displacements ξ, drawn by the random variable denoted by Ξ in each round, conditioned on his measurement outcomes ξ_{P}, drawn from the random variable denoted by Ξ_{P} in each round, is the same as in the protocol where θ is sent directly from V_1, since the only change for P is to compute $f(x, y)$ to determine θ. In order to make this mathematically precise, we need the following definitions.

As introduced in [FBT+14], let ρ_{AB} be a bipartite state on systems A and B, which correspond to a system to be measured, and a system held by an observer. Let $\mathbf{X}$ be a continuous random variable, $\alpha = 2^{-l}$ for some $l \in \mathbb{N}$, and consider the intervals $\mathcal{I}_{j;\alpha} := (j\alpha, (j+1)\alpha]$ for $j \in \mathbb{Z}$. Here $\rho_B^{j;\alpha}$ denotes the sub-normalized density matrix in B when $\mathbf{X}$ takes value $\mathbf{x}$ in $\mathcal{I}_{j;\alpha}$, $\rho_B^{\mathbf{x}}$ denotes the conditional reduced density matrix in B so that $\int_{\mathcal{I}_{j;\alpha}} \rho_B^{\mathbf{x}} d\mathbf{x} = \rho_B^{j;\alpha}$, and $\mathbf{X}_\alpha$ denotes the random variable that indicates which interval $\mathbf{x}$ belongs to. These notions are used in the continuous version of the conditional entropy.

9.2.4. Definition. *The* quantum conditional von Neumann entropy *is defined as*

$$H(\mathbf{X}_\alpha|B)_\rho := -\sum_{j\in\mathbb{Z}} D(\rho_B^{j;\alpha}||\rho_B). \tag{9.4}$$

9.2.5. Definition. *The* differential quantum conditional von Neumann entropy *is defined as*

$$h(\mathbf{X}|B)_\rho := -\int_{\mathbb{R}} D(\rho_B^{\mathbf{x}}||\rho_B)\,\mathrm{d}\mathbf{x}. \tag{9.5}$$

Then, the uncertainty of the prover with respect to Ξ_{P} in the $\mathrm{QPV}_{\mathrm{coh}}$ protocol provided in [AEFR+23]:

$$h(\Xi|\Xi_{\mathsf{P}})_{\phi} = \frac{1}{2}\log 2\pi e\Sigma^2, \tag{9.6}$$

where

$$\Sigma^2 = \left(\frac{1}{\sigma^2} + \frac{t}{1/2+u}\right)^{-1}. \tag{9.7}$$

It is well known that the preparation of a coherent state with Gaussian distributed displacements $(x_0, p_0) \sim \mathcal{N}_{0,\sigma^2}$ is equivalent to preparing a two-mode squeezed state with squeezing parameter $\sinh^{-1}\sigma$ and then performing a heterodyne $(\hat{x}, \hat{p})$ measurement on one mode, with measurement outcome $\frac{(x_0,-p_0)}{\sqrt{2}\tanh\sinh^{-1}\sigma}$. For notational brevity, we set $\lambda = \tanh\sinh^{-1}\sigma$.

In the purified version of $\mathrm{QPV}^{f}_{\mathrm{coh}}$, the verifier V_0 prepares the two-mode squeezed state $|\Phi\rangle_{V_0P}$ with the above-mentioned λ-dependent squeezing, which is given by

$$|\Phi\rangle = \sqrt{1-\lambda^2}\sum_{m=0}^{\infty}\lambda^m|mm\rangle, \tag{9.8}$$

in the Fock space. Notice that $\lambda < 1$. The verifier V_0 performs a heterodyne measurement with quadratures rotated by an angle θ on their register. The measurement outcomes are $\xi/(\sqrt{2}\lambda)$ and $-\xi^{\perp}/(\sqrt{2}\lambda)$, resulting in displacement $(\xi, \xi^{\perp})$ in the state sent to the prover P. P then performs a homodyne measurement under angle θ to recover ξ, as in the original protocol.

V_0's heterodyne measurement can be described as a double-homodyne measurement. First V_0 mixes its own mode with the vacuum using a beam splitter, resulting in a two-mode state. On one of these modes, V_0 then performs a homodyne measurement in the θ-direction, on the other mode in the $\theta + \frac{\pi}{2}$ direction. In [AEFR+23], it is shown that the honest prover's uncertainty about Ξ evaluates to

$$h(\Xi|P)_{\Phi} = \frac{1}{2}\log\frac{\pi e(1+2u)}{t} + O\left(\frac{1}{\sigma}\right). \tag{9.9}$$

Let $\mathcal{U} = \Xi/(\lambda\sqrt{2})$ be the displacement in the θ direction as measured by V_0. Then

$$\begin{aligned} h(\mathcal{U}|P)_{\Phi} &= h\left(\frac{\Xi}{\sqrt{2}\lambda}\middle|P\right)_{\Phi} = h(\Xi|P)_{\Phi} - \log(\sqrt{2}\lambda) \\ &= \frac{1}{2}\log\frac{\pi e(1+2u)}{t} + O\left(\frac{1}{\sigma}\right) - \log(\sqrt{2}\lambda). \end{aligned} \tag{9.10}$$

In the regime $\sigma \gg 1$ (i.e. $\lambda \to 1$),

$$h(\mathcal{U}|P)_{\Phi} \to h(\mathcal{U}|P)_{\phi} = \frac{1}{2}\log\frac{\pi e(1+2u)}{2t}. \tag{9.11}$$

Unless stated otherwise, we will work in the regime $\sigma \gg 1$. Recall that σ is in control of the verifiers.

9.3 Security against bounded entanglement

In this section, we prove security of the $\mathrm{QPV}^{f}_{\mathrm{coh}}$ protocol, showing that with high probability, attackers who possess CV entangled states with a cutoff at photon number linear in n will not be able to attack the protocol.

To do so, we consider an 'imaginary world' where the $\mathrm{QPV}^{f}_{\mathrm{coh}}$ protocol, instead of using the state $|\Phi\rangle$, is executed with a cutoff at photon number 2^{m_0} using the state $|\Phi_{m_0}\rangle$, given by

$$|\Phi_{m_0}\rangle = \sqrt{\frac{1-\lambda^2}{1-(\lambda^2)^{2^{m_0}}}} \sum_{m=0}^{2^{m_0}-1} \lambda^m |mm\rangle. \tag{9.12}$$

We will denote this variation of the protocol by $\mathrm{QPV}^{f}_{\mathrm{coh}_{m_0}}$. The state $|\Phi_{m_0}\rangle$ is an approximation of the state $|\Phi\rangle$ and can be made arbitrary close to it by increasing m_0. Note that the purified distance (see (2.14)) between $|\Phi\rangle$ and $|\Phi_{m_0}\rangle$ is

$$\mathcal{P}(|\Phi\rangle, |\Phi_{m_0}\rangle) = \lambda^{2^{m_0}}, \tag{9.13}$$

i.e. $|\Phi_{m_0}\rangle$ is double exponentially close (in m_0) to $|\Phi\rangle$ (recall that $\lambda < 1$). If one replaces the state $|\Phi\rangle$ by $|\Phi_{m_0}\rangle$, the probability that the verifiers accept the action of an honest party will change with probability at most $O(\lambda^{2^{m_0}})$. The cutoff reduces the dimension of the Hilbert space from infinite to 2^{m_0}, which is the dimension of an m_0-qubit state space.

The Hamiltonian $\hat{H}_{V_0}$ on V_0's system is given by the harmonic oscillator, where

$$\hat{H} = \hbar\omega \hat{N}, \tag{9.14}$$

with the unusual energy convention that the ground state has energy 0 instead of $\frac{1}{2}\hbar\omega$, and $\hat{N}$ is the number operator. Throughout this chapter, we will consider units such that $\hbar\omega = 1$. The energy of the V_0 subsystem is thus given by

$$\langle \Phi_{m_0}| \hat{H}_{V_0} \otimes \mathbb{I}_P |\Phi_{m_0}\rangle_{V_0 P} = \frac{\lambda^2 + (2^{m_0}-1)\lambda^{2^{m_0+1}+2} - 2^{m_0}\lambda^{2^{m_0+1}}}{(\lambda^2-1)\left(\lambda^{2^{m_0+1}}-1\right)} = \frac{2^{m_0}\left(\frac{\sigma^2}{\sigma^2+1}\right)^{2^{m_0}}}{\left(\frac{\sigma^2}{\sigma^2+1}\right)^{2^{m_0}}-1} + \sigma^2, \tag{9.15}$$

which tends to σ^2 (the expected energy of the challenge state chosen by the verifiers) as m_0 tends to infinity.

The most general attack to $\mathrm{QPV}^{f}_{\mathrm{coh}_{m_0}}$ for adversaries with a photon-number cutoff such that their Hilbert space is isomorphic to a multi-qubit Hilbert space, consists of an adversary Alice between V_0 and P, and an adversary Bob between V_1 and P. They proceed as follows:

1. Alice intercepts the quantum information sent by V_0, and applies an arbitrary quantum operation to it and to a local register that she possesses,

possibly entangling them. She keeps part of the resulting state, and sends the rest to Bob. Since the quantum information in the protocol can be sent arbitrarily slow by V_0, this happens before Alice and Bob can intercept x and y.

2. Alice intercepts x and Bob intercepts y. At this stage, Alice, Bob, and V_0 share a quantum state $|\varphi\rangle$, make a partition and let q be the number of qubits that Alice and Bob each hold, recall that m_0 qubits are held by V_0 and thus the three parties share a quantum state $|\varphi\rangle$ of $2q+m_0$ qubits. Alice and Bob apply a unitary $U^x_{A_\mathrm{k}A_\mathrm{c}}$ and $V^y_{B_\mathrm{k}B_\mathrm{c}}$ on their local registers $A_\mathrm{k}A_\mathrm{c} =: A$ and $B_\mathrm{k}B_\mathrm{c} =: B$, both of dimension $d = 2^q$, where k and c denote the registers that will be kept and communicated, respectively. Due to the Stinespring dilation, we consider unitary operations instead of quantum channels. They end up with the quantum state $|\psi_{xy}\rangle = \mathbb{I}_V \otimes U^x_{A_\mathrm{k}A_\mathrm{c}} \otimes V^y_{B_\mathrm{k}B_\mathrm{c}}|\varphi\rangle$.

3. Alice sends register A_c and x to Bob (and keeps register A_k), and Bob sends register B_c and y to Alice (and keeps register B_k).

4. Alice and Bob perform POVMs $\{A^{xy}_a\}_a$ and $\{B^{xy}_b\}_b$ on their local registers $A_\mathrm{k}B_\mathrm{c} =: A'$ and $B_\mathrm{k}A_\mathrm{c} =: B'$ to obtain classical answers and reply to their closest verifier, respectively.

9.3.1. Remark. Notice that we consider strategies starting with the state $|\varphi\rangle_{VPA_\mathrm{k}A_\mathrm{c}B_\mathrm{c}B_\mathrm{k}}$ instead of $|\Phi_{m_0}\rangle_{VP} \otimes |\varphi'\rangle_{A_\mathrm{k}A_\mathrm{c}B_\mathrm{c}B_\mathrm{k}}$. This will give more power to the attackers, but it will include the fact that the quantum information sent from V_0 can travel arbitrarily slow, and the attackers are allowed to modify $|\Phi_{m_0}\rangle_{VP} \otimes |\varphi'\rangle_{A_\mathrm{k}A_\mathrm{c}B_\mathrm{c}B_\mathrm{k}}$ to end up with any arbitrary state $|\varphi\rangle_{VPA_\mathrm{k}A_\mathrm{c}B_\mathrm{c}B_\mathrm{k}}$.

See Figure 4.2 for a schematic representation of a generic attack to $\mathrm{QPV}^f_{\mathrm{coh}}$. Note that the actions of the attackers are similar to the actions described in Chapter 4 to attack $\mathrm{QPV}^\eta_{\mathrm{BB84}}$. We exploit these similarities to extend the technical analysis to the continuous-variable setting, and establish security guarantees for $\mathrm{QPV}^f_{\mathrm{coh}}$ analogous to those previously shown for $\mathrm{QPV}^f_{\mathrm{BB84}}$.

9.3.2. Definition. *The tuple $\{|\varphi\rangle, U^x, V^y, A^{xy}, B^{xy}\}_{x,y,a,b}$ is a q-*qubit strategy for $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$. *Moreover, let $|\phi\rangle$ be as in the* $\mathrm{QPV}^f_{\mathrm{coh}}$ *protocol (Definition 9.2.1), we say that a q-qubit strategy for* $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$ *is (ε, l)-perfect if for l pairs of strings (x, y), for $\theta \in \{0, \frac{\pi}{2}\}$, if it holds that*

$$h(\mathcal{U}_\theta|A')_\psi \leq h(\mathcal{U}|P)_\phi + \varepsilon \quad \textit{and} \quad h(\mathcal{U}_\theta|B')_\psi \leq h(\mathcal{U}|P)_\phi + \varepsilon. \tag{9.16}$$

Notice that there is no θ-dependence on the right-hand side of the inequality since $h(\mathcal{U}|P)_\phi$ does not depend on θ, see (9.11). The parameter ε, see analysis below, will quantify the difference between the uncertainty of the honest prover and

attackers. It will have to be picked depending on the number of rounds that the protocol is run sequentially. Next, we define 'good' states to attack the protocol for either $\theta = 0$ or $\theta = \pi/2$. We will see that a good state for the $\theta = 0$ case cannot be too close (in trace distance) to a good state for the $\theta = \pi/2$ case. This restricts the attackers.

9.3.3. Definition. *Let $\varepsilon \geq 0$, let A' and B' be arbitrary dimensional registers and V be an m_0 qubit register. We define $\mathcal{S}_\theta^\varepsilon$ as*

$$\mathcal{S}_\theta^\varepsilon := \{|\psi\rangle_{VAB} \mid \exists \text{ POVMs } \{A_{A'}^{xy}\}, \{B_{B'}^{xy}\} \text{ s.t. } h(\mathcal{U}_\theta|A')_\psi, h(\mathcal{U}_\theta|B')_\psi \leq h(\mathcal{U}|P)_\phi + \varepsilon\}.$$

Next, we will use a entropic uncertainty relation for position and momentum, along with a continuity bound for the entropy, to show the following: if Alice and Bob prepare one state that is "good" for attacking $\theta = 0$, and another that is "good" for attacking $\theta = \frac{\pi}{2}$—that is, they have states $|\psi_0\rangle \in \mathcal{S}_0^\varepsilon$ and $|\psi_{\frac{\pi}{2}}\rangle \in \mathcal{S}_{\frac{\pi}{2}}^\varepsilon$—then these two states cannot be arbitrarily close in trace distance.

9.3.4. Lemma. *[FBT+14] Let ρ_{VAB} be a tripartite density matrix on systems V, A and B. Let $\mathbf{X}$ and $\mathbf{P}$ denote the random variables of position and momentum respectively, resulting from a homodyne measurement on the V system and let the following hold: $h(\mathbf{X}|A)_\rho, h(\mathbf{P}|B)_\rho > -\infty$ and $H(\mathbf{X}_\alpha|A)_\rho, H(\mathbf{P}_\alpha|B)_\rho < \infty$ for any $\alpha > 0$. Then*

$$h(\mathbf{X}|A)_\rho + h(\mathbf{P}|B)_\rho \geq \log(2\pi). \tag{9.17}$$

We will make use of a type of Alicki-Fannes [AF04] inequality (Lemma 9.3.5) for continuity of the conditional entropy for continuous variables in terms of the energy, as shown in [Win16].

9.3.5. Lemma. *(Lemma 18, [Win16]) Let $\alpha \in [0, \frac{1}{2}]$. Consider a Hamiltonian $\hat{H} = \hat{H}_V \otimes \mathbb{I}_C$, with system V composed of one harmonic oscillator and arbitrary system C. Let there be states ρ and σ on the bipartite system $\mathcal{H}_V \otimes \mathcal{H}_C$ with $\mathrm{Tr}\big[\rho\hat{H}\big], \mathrm{Tr}\big[\sigma\hat{H}\big] \leq E$. If $\frac{1}{2}\|\rho - \sigma\|_1 \leq \tilde{\varepsilon}$, then*

$$|h(V|C)_\rho - h(V|C)_\sigma| \leq \left(\frac{1+\alpha}{1-\alpha} + 2\alpha\right)\left[2\tilde{\varepsilon}\left(\log(E+1) + \log\frac{e}{\alpha(1-\tilde{\varepsilon})}\right) + 6\tilde{h}\left(\frac{1+\alpha}{1-\alpha}\tilde{\varepsilon}\right)\right], \tag{9.18}$$

where

$$\tilde{h}(p) := \begin{cases} -p\log p - (1-p)\log(1-p) & \text{if } p \leq \frac{1}{2}, \\ 1 & \text{if } p > \frac{1}{2}. \end{cases} \tag{9.19}$$

9.3.6. Proposition. *Let $\varepsilon > 0$, and $|\psi_0\rangle \in \mathcal{S}_0^\varepsilon$, and $|\psi_{\frac{\pi}{2}}\rangle \in \mathcal{S}_{\frac{\pi}{2}}^\varepsilon$, with bounded energies $\mathrm{Tr}\big[\rho^0\hat{H}\big], \mathrm{Tr}\big[\rho^1\hat{H}\big] \leq E$, where ρ^0 and ρ^1 are the respective density matrices*

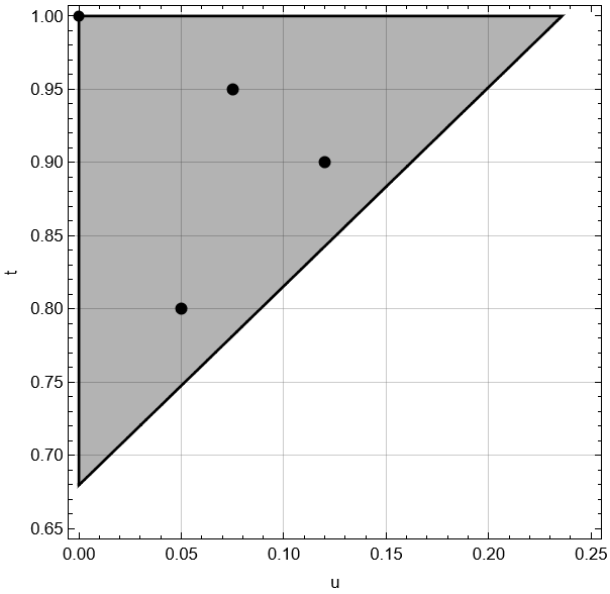


Figure 9.2: Necessary condition for u and t so that (9.20) is fulfilled (gray region). The blue dots are specific (u,t) for which we do numerical analysis in Section 9.4.

of $|\psi_0\rangle$ *and* $|\psi_{\frac{\pi}{2}}\rangle$. *The corresponding Hamiltonian is the harmonic oscillator on system* V *and identity on the other systems. Let* $\frac{1}{2} \geq \alpha \geq 0$ *and* $\tilde{\varepsilon} > 0$ *be such that*

$$\varepsilon < \frac{1}{2}\log\frac{4t}{e(1+2u)} - \left(\frac{1+\alpha}{2(1-\alpha)} + \alpha\right)\left[2\tilde{\varepsilon}\left(\log(E+1) + \log\frac{e}{\alpha(1-\tilde{\varepsilon})}\right) + 6\tilde{h}\left(\frac{1+\alpha}{1-\alpha}\tilde{\varepsilon}\right)\right]. \tag{9.20}$$

Then,

$$\frac{1}{2}\||\psi_0\rangle - |\psi_{\frac{\pi}{2}}\rangle\|_1 > \tilde{\varepsilon}. \tag{9.21}$$

Notice that the energy bound E is the energy given by the Hamiltonian corresponding to one harmonic oscillator in the V system (9.15), which approaches σ^2 from below. Moreover, from (9.20), we see that the ε will need to be picked taking a value at most $\frac{1}{2}\log\frac{4t}{e(1+2u)}$. In order to have non-negative $\tilde{\varepsilon}$, we need

$$4t > e(1+2u), \tag{9.22}$$

see Figure 9.2. The maximum value of ε will be upper bounded by

$$\varepsilon < \frac{1}{2}\log\frac{4t}{e(1+2u)} \leq \frac{1}{2}\log\frac{4}{e} \simeq 0.278652, \tag{9.23}$$

since the maximum value is reached by $t = 1$ and $u = 0$.

Proof:
Let ρ^{θ} and $\rho^{\bar{\theta}}$ be the density matrices of $|\psi_\theta\rangle_{VPA_{\mathrm{k}}A_{\mathrm{c}}B_{\mathrm{k}}B_{\mathrm{c}}}$ and $|\psi_{\bar{\theta}}\rangle_{VPA_{\mathrm{k}}A_{\mathrm{c}}B_{\mathrm{k}}B_{\mathrm{c}}}$, respectively. By hypothesis,

$$h(\mathcal{U}_\theta|A')_{\rho^\theta} \leq h(\mathcal{U}|P)_\phi + \varepsilon, \text{ and } h(\mathcal{U}_{\bar{\theta}}|A')_{\rho^{\bar{\theta}}} \leq h(\mathcal{U}|P)_\phi + \varepsilon. \tag{9.24}$$

By Lemma 9.3.4,

$$h(\mathcal{U}_\theta|A')_{\rho^\theta} + h(\mathcal{U}_{\bar{\theta}}|B')_{\rho^\theta} \geq \log 2\pi. \tag{9.25}$$

Then,

$$h(\mathcal{U}_{\bar{\theta}}|B')_{\rho^\theta} \geq \log 2\pi - h(\mathcal{U}_\theta|A')_{\rho^\theta} \geq \log 2\pi - h(\mathcal{U}|P)_\phi - \varepsilon, \tag{9.26}$$

where in the last inequality we used (9.24). Therefore,

$$h(\mathcal{U}_{\bar{\theta}}|B')_{\rho^\theta} - h(\mathcal{U}_{\bar{\theta}}|A')_{\rho^{\bar{\theta}}} \geq \log 2\pi - 2h(\mathcal{U}|P)_\phi - 2\varepsilon. \tag{9.27}$$

In the regime $\sigma \gg 1$, $h(\mathcal{U}|P)_\phi \to \frac{1}{2}\log\frac{\pi e(1+2u)}{2t}$, and thus,

$$h(\mathcal{U}_{\bar{\theta}}|B')_{\rho^\theta} - h(\mathcal{U}_{\bar{\theta}}|A')_{\rho^{\bar{\theta}}} \geq \log\frac{4t}{e(1+2u)} - 2\varepsilon > 0, \tag{9.28}$$

where the last inequality comes from the fact that, by hypothesis, $\frac{1}{2}\log\frac{4t}{e(1+2u)} > \varepsilon$. This leads to

$$|h(\mathcal{U}_{\bar{\theta}}|B')_{\rho^\theta} - h(\mathcal{U}_{\bar{\theta}}|A')_{\rho^{\bar{\theta}}}| \geq \log\frac{4t}{e(1+2u)} - 2\varepsilon, \tag{9.29}$$

By hypothesis, $\log\frac{4t}{e(1+2u)} - 2\varepsilon > \left(\frac{1+\alpha}{1-\alpha} + 2\alpha\right)\left[2\tilde{\varepsilon}\left(\log(E+1) + \log\frac{e}{\alpha(1-\tilde{\varepsilon})}\right) + 6\tilde{h}\left(\frac{1+\alpha}{1-\alpha}\tilde{\varepsilon}\right)\right]$. Thus, by the contrapositive of Lemma 9.3.5, $\frac{1}{2}\|\rho^\theta - \rho^{\bar{\theta}}\|_1 > \tilde{\varepsilon}$.

□

9.3.7. Definition. *[BCS22] Let $q, \kappa, n \in \mathbb{N}$, $\varepsilon > 0$. Then, $g : \{0,1\}^{3\kappa} \to \{0,1\}$ is an (ε, l)-classical rounding of size κ if for all $f : \{0,1\}^{2n} \to \{0,1\}$, for all states $|\varphi\rangle$ on $2q+2m_0$ qubits, for all $l \in \{1, ..., 2^{2n}\}$ and for all (ε, l)-perfect q-qubit strategies for $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$, there are functions $f_A : \{0,1\}^n \to \{0,1\}^\kappa$, $f_B : \{0,1\}^n \to \{0,1\}^\kappa$ and $\mu \in \{0,1\}^\kappa$ such that $g(f_A(x), f_B(y), \mu) = f(x,y)$ on at least l pairs (x,y).*

9.3.8. Lemma. *Let ε, $\tilde{\varepsilon}$ be such that if $|\varphi_\theta\rangle \in \mathcal{S}^\varepsilon_\theta$ and $|\varphi_{\bar{\theta}}\rangle \in \mathcal{S}^\varepsilon_{\bar{\theta}}$ implies $\mathcal{P}(|\varphi_\theta\rangle, |\varphi_{\bar{\theta}}\rangle) > \tilde{\varepsilon}$. Then, there exists an (ε, q)-classical rounding of size $\kappa \leq 2^{2q+2m_0}\log\left(1 + \frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})}-2}\right)$.*

Proof:
We follow the same techniques as in the proof of Lemma 3.12 in [BCS22]. Let $\delta < \sqrt[3]{\frac{2+\tilde{\varepsilon}}{2}} - 1$, and consider δ-nets $\mathcal{N}_S$, $\mathcal{N}_A$ and $\mathcal{N}_B$, where the first is for the set of pure states on $2q + 2m_0$ qubits in Euclidean norm and the other nets are for the

set of unitaries in dimension 2^q in operator norm. They are such that $|\mathcal{N}_S|$, $|\mathcal{N}_A|$, $|\mathcal{N}_B| \leq 2^\kappa$, with κ to be set later. Let $\mathbf{S} = \{|\varphi\rangle, U^x, V^y, \{A_a^{xy}\}_a, \{B_b^{xy}\}_b\}_{x,y}$ be an (ε, ℓ)– strategy for $\mathrm{QPV}^{\eta,f}_{k_{\theta\varphi}}$, we define (i) μ as the element in $\mathcal{N}_S$ that is closest to $|\varphi\rangle$ in Euclidean norm, and denote by $|\varphi_\delta\rangle$ the state described by μ, (ii) $f_A(x)$ as the element in $\mathcal{N}_A$ that is closest to U^x in operator norm, and denote by U_δ^x the unitary described by $f_A(x)$, and (iii) $f_B(y)$ as the element in $\mathcal{N}_B$ that is closest to V^y in operator norm, and denote by V_δ^y the unitary described by $f_A(y)$. If the closest element is not unique, make an arbitrary choice.

We define g as $g(x, y, \mu) = 0$ if $U \otimes V|\varphi\rangle$ is closer to $\mathcal{S}_\theta^\varepsilon$ than to $\mathcal{S}_{\bar{\theta}}^\varepsilon$ in purified distance and $g(x, y, \mu) = 1$ if $U \otimes V|\varphi\rangle$ is closer to $\mathcal{S}_{\bar{\theta}}^\varepsilon$ than to $\mathcal{S}_\theta^\varepsilon$ in purified distance. If neither is the case, we make the arbitrary choice $g(x, y, \mu) = 1$. By the assumption on ε, $\mathcal{S}_\theta^\varepsilon \cap \mathcal{S}_{\bar{\theta}}^\varepsilon = \varnothing$, and thus g is well-defined.

We are going to show that g is an (ε, q)-classical rounding. Consider an arbitrary $f : \{0,1\}^{2n} \to \{0,1\}$ and an arbitrary state $|\varphi\rangle$ on $2q + 2m_0$ qubits. Let $|\varphi\rangle$, $\{U^x, V^y\}_{xy}$ be from a q-qubit strategy for $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$, and choose μ, $f_A(x)$ and $f_B(y)$ to be the closest elements to $|\varphi\rangle$, U^x and V^y, respectively, in their corresponding δ-nets in the Euclidean and operator norm, respectively, (if not unique, make an arbitrary choice) and let $|\varphi\rangle, U, V$ be their corresponding elements. Assume $U^x \otimes V^y|\varphi\rangle \in \mathcal{S}_\theta^\varepsilon$. Then,

$$\begin{aligned}
\mathcal{D}(U^x \otimes V^y|\psi\rangle, U_\delta^x \otimes V_\delta^y|\varphi_\delta\rangle) &\leq \|U^x \otimes V^y|\varphi\rangle - U_\delta^x \otimes V_\delta^y|\varphi\rangle\|_2 \\
&\leq \|(U_\delta^x + U^x - U_\delta^x) \otimes (V_\delta^y + V^y - V_\delta^y)(|\varphi_\delta\rangle + |\varphi\rangle - |\varphi_\delta\rangle) - U_\delta^x \otimes V_\delta^y|\varphi\rangle\|_2 \\
&\leq 3\delta + 3\delta^2 + \delta^3 < \frac{\tilde{\varepsilon}}{2},
\end{aligned} \tag{9.30}$$

where in the first inequality, we used Lemma 4.3.3, in the second, we used the triangle inequality and the inequality $\|X \otimes Y|x\rangle\|_2 \leq \|X\|_\infty \|Y\|_\infty \||x\rangle\|_2$, together with $\|U^x - U_\delta^x\|_\infty, \|U^y - U_\delta^y\|_\infty, \||\varphi\rangle - |\varphi_\delta\rangle\| \leq \delta$. Thus, $U_\delta^x \otimes V_\delta^y|\varphi_\delta\rangle$ is closer to $\mathcal{S}_\theta^\varepsilon$ than to $\mathcal{S}_{\bar{\theta}}^\varepsilon$.

Consider the above (ε, l)-perfect strategy for $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$ and let (x, y) be such that $h(\mathcal{U}_\theta|A')_\psi, h(\mathcal{U}_\theta|B')_\psi \leq h(\mathcal{U}|P)_\phi + \varepsilon$ for $f(x, y) = 0$. In particular, we have that $U^x \otimes U^y|\varphi\rangle \in \mathcal{S}_\theta^\varepsilon$, and because of (9.30), $f(x, y) = g(f_A(x), f_B(y), \mu)$. Since there are at least l pairs (x, y) fulfilling it, $f(x, y) = g(f_A(x), f_B(y), \mu)$ holds on at least l pairs (x, y) and therefore g is an (ε, q)-classical rounding. The size of κ follows from Lemma 4.2.8. □

9.3.9. Lemma. *Let $\varepsilon \in [0,1]$, $E, t, u > 0$ be such that there exist $\tilde{\varepsilon} > 0$ and α such that (9.20) holds. Let κ, $q \in \mathbb{N}$, $n = \Omega(m_0)$. Moreover, fix an (ε, q)-classical rounding g of size κ with $\kappa \leq 2^{2q+2m_0} \log\left(1 + \frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})}-2}\right)$. Let $q = O(n - m_0)$. Then, with probability $1 - O(\lambda^{2^{m_0}})$ the following holds. A uniformly random $f : \{0,1\}^{2n} \to \{0,1\}$ fulfills the following with probability at least $1 - O(2^{-2^n})$:*

For any $f_A : \{0,1\}^n \to \{0,1\}^\kappa$, $f_B : \{0,1\}^n \to \{0,1\}^\kappa$, $\mu \in \{0,1\}^\kappa$, *the equality* $g(f_A(x), f_B(y), \mu) = f(x,y)$ *holds on less than* $3/4$ *of all pairs* (x,y).

Proof:
We want to estimate the probability that for a randomly chosen f, we can find f_A and f_B such that the corresponding function g fulfils $\mathbb{P}_{x,y}[f(x,y) = g(f_A(x), f_B(y), \mu)] \geq 3/4$. Analogous to Lemma 4.2.10, we have that

$$\mathbb{P}[f : \exists f_A, f_B, \mu \text{ s.t. } \mathbb{P}_{x,y}[f(x,y) = g(f_A(x), f_B(y), \mu)]] \leq 2^{(2^{n+1}+1)k} 2^{2^{2n} h_b(1/4)} 2^{-2^{2n}}, \tag{9.31}$$

where $h_b(\cdot)$ denotes the binary entropy function, see (2.1). If $q = O(n - m_0)$ and $\kappa = 2^{2q+2m_0} \log\left(1 + \frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})-2}}\right)$, the above expression is strictly upper bounded by $O(2^{-2^n})$. □

In order to have explicit expressions instead of $n = \Theta(m_0)$ and $q = O(n - m_0)$, we have to fix the value of $\tilde{\varepsilon}$. To obtain better bounds, we are interested in picking $\tilde{\varepsilon}$ as large as possible. Given parameters E, t, u and ε, known by the verifiers, we will be interested in picking values of α such that (9.20) holds for $\tilde{\varepsilon}$ as large as possible. This needs to be done numerically, since (9.20) leads to a transcendental equation, see Section 9.4 for this analysis. This applies as well for the below theorem, which in short states that if the number of qubits the attackers pre-share at the beginning of the protocol, with high probability at least one of them will have a finite gap to the uncertainty of the honest prover regarding the value of the random variable $\mathcal{U}$. That is, at least one attacker will have strictly larger uncertainty than the prover.

9.3.10. Theorem. *Let* $\varepsilon \in [0,1]$, $E, t, u > 0$ *(under the control of the verifiers) be such that there exists* $\tilde{\varepsilon} > 0$ *and* α *such that* (9.20) *holds. Let* $n = \Theta(m_0)$. *Let the number of qubits that Alice and Bob each control at the beginning of the protocol be*

$$q = O(n - m_0). \tag{9.32}$$

Then, with probability $1 - O(\lambda^{2^{m_0}})$ *the following holds. A random function* f *fulfills the following with probability at least* $1 - O(2^{-2^n})$ *: the uncertainties for Alice and Bob when attacking the protocol* $\mathrm{QPV}^f_{\mathrm{coh}}$ *are such that, for* $\theta \in \{0, \frac{\pi}{2}\}$,

$$\max\{h(\mathcal{U}_\theta|A')_\phi, h(\mathcal{U}_\theta|B')_\phi\} \geq h(\mathcal{U}|P)_\phi + \frac{\varepsilon}{4}, \tag{9.33}$$

for every state $|\psi\rangle$ *they possess in step 4. of the attack (i.e. end of the attack).*

Proof:
By Lemma 4.2.10, with probability at least $1 - O(2^{-2^n})$, the function f is such that there are no $(\varepsilon, \frac{3}{4}2^{2n})$-perfect q-qubit strategies for $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$. That means that for every strategy, on a fraction at least $\frac{1}{4}$ of (x,y), either $h(\mathcal{U}_\theta|A')_\psi \geq h(\mathcal{U}|P)_\phi + \frac{\varepsilon}{4}$ or $h(\mathcal{U}_\theta|B')_\psi \geq h(\mathcal{U}|P)_\phi + \frac{\varepsilon}{4}$. □

9.3.1 Sequential repetition of $\mathrm{QPV}^{f}_{\mathrm{coh}}$

In the following, we will consider $\sigma \gg 1$, which is equivalent to $\lambda \to 1$. Recall that the verifiers either accept or reject the location after r sequential repetitions. We provided a statistical test, $\mathsf{T}^{r-\mathrm{coh}}_{\varepsilon_{\mathrm{h}}}$—see Definition 9.2.3—to make the decision to either accept or reject the position *pos* that an honest prover will pass with probability at least $1-\varepsilon_{\mathrm{h}}$, for $\varepsilon_{\mathrm{h}} > 0$. Now, we will show that attackers who pre-share a bounded number of qubits (in n) and, motivated by realistic constraints, perform independent identically distributed (i.i.d.) attacks, will fail the test, and therefore be *caught*, with high probability in the number of rounds.

By Theorem 9.3.10, we have that provided that the attackers pre-share a linear amount of qubits in n, then, for every state $|\psi\rangle$ that they share after communicating

$$h(\mathcal{U}_\theta|E)_\psi := \max\{h(\mathcal{U}_\theta|A')_\psi, h(\mathcal{U}_\theta|B')_\psi\} \geq h(\mathcal{U}|P)_\phi + \frac{\varepsilon}{4} = \frac{1}{2}\log\left(\pi e \frac{1/2+u}{t}\right) + \frac{\varepsilon}{4},$$

for ε as in Theorem 9.3.10.

Now re-substituting $\Xi = \sqrt{2}\lambda\mathcal{U}$ yields

$$h(\Xi|E)_\psi \geq h(\Xi|P)_\phi + \frac{\varepsilon}{4} = \frac{1}{2}\log\left(2\pi e \frac{1/2+u}{t}\right) + \frac{\varepsilon}{4} \geq \frac{1}{2}\log(\pi e) + \frac{\varepsilon}{4}, \tag{9.34}$$

where the last equation follows from (9.11) and the lower bound is smallest for the ideal channel with $t = 1$ and $u = 0$, which we assume attackers can use. Via the continuous variable version of Fano's inequality, Theorem 9.3.11, we can straightforwardly convert this into a lower bound for the estimation error of the attackers.

9.3.11. Theorem. *[CT06] Let X be a random variable and $\hat{X}(Y)$ an estimator of X given side information Y, then*

$$\mathbb{E}\Big[\big(X - \hat{X}(Y)\big)^2\Big] \geq \frac{1}{2\pi e} e^{2h_{\mathrm{nats}}(X|Y)}, \tag{9.35}$$

where $h_{\mathrm{nats}}(X|Y)$ is the conditional entropy in natural units. Moreover, if X is Gaussian and $\hat{X}(Y)$ is its mean, then equality holds.

Let Ξ_{att} be the random variable representing the attackers' answer (guess for Ξ). Then, by Theorem 9.3.11, we have:

$$\mathbb{E}\big[(\Xi - \Xi_{\mathsf{att}})^2\big] \geq \frac{1}{2\pi e} e^{2h_{\mathrm{nats}}(\Xi|E)_\psi} = \frac{1}{2} e^{\varepsilon/2}, \tag{9.36}$$

holding for any transmission t. Let $(\xi_i^{\mathrm{att}})_{i=1}^r$ be the sample of the attackers after r i.i.d. rounds, then, consider the score or pay-off associated to the attackers,

$$\Gamma_r^{att} = \sum_{i=1}^{r} \frac{(\sqrt{t}\xi_i - \xi_i^{\mathrm{att}})^2}{1/2+u}. \tag{9.37}$$

We will use Chebyshev's inequality [Che67] to show that attackers will be caught with high probability, that is, by not being able to get a score below γ_r:

9.3.12. Proposition. *Assume the setting of Theorem 9.3.10 and fix a confidence parameter $\varepsilon_{\mathrm{h}} > 0$. Let r be the number of sequential rounds of $\mathrm{QPV}_{\mathrm{coh}}^{f}$. If $r = \Omega\Big(\frac{1}{\varepsilon_{\mathrm{h}}\left(\frac{1}{2}e^{\varepsilon/2}-\gamma_r/r\right)^2}\Big)$ then, for every i.i.d. adversarial strategy,*

$$\Pr[\Gamma_r^{att} \leq \gamma_r] = O(\varepsilon_h). \tag{9.38}$$

Equivalently, the probability that the attackers pass the test $\mathsf{T}_{\varepsilon_{\mathrm{h}}}^{r-\mathrm{coh}}$ (Definition 9.2.3) is at most $O(\varepsilon_{\mathrm{h}})$.

Proof:
Let $\tilde{\sigma}^2 > 0$ be the variance of $\frac{(\sqrt{t}\Xi_i - \Xi_i^{\mathrm{att}})^2}{1/2+u}$ for the ith round. Since, by hypothesis, the attacks are i.i.d, this variance is the same for every round i. Thus, the variance of Γ_r^{att} is $r\tilde{\sigma}^2$. Then, the probability that the attackers pass the test $\mathsf{T}_{\varepsilon_{\mathrm{h}}}^{r-\mathrm{coh}}$ is

$$\begin{aligned}\Pr[\Gamma_r^{att} \leq \gamma_r] &= \Pr[\mathbb{E}[\Gamma_r^{att}] - \Gamma_r^{att} \geq E[\Gamma_r^{att}] - \gamma_r] \leq \Pr[|\mathbb{E}[\Gamma_r^{att}] - \Gamma_r^{att}| \geq E[\Gamma_r^{att}] - \gamma_r] \\ &\leq \Pr\left[|\mathbb{E}[\Gamma_r^{att}] - \Gamma_r^{att}| \geq \frac{r}{2}e^{\varepsilon/2} - \gamma_r\right] \leq \frac{r\tilde{\sigma}^2}{\left(\frac{r}{2}e^{\varepsilon/2} - \gamma_r\right)^2},\end{aligned}$$

where we used, from (9.36) that $\mathbb{E}[\Gamma_r^{att}] \geq r\frac{1}{2}e^{\varepsilon/2}$, and Chebychev's inequality for the last upper bound.
By hypothesis, $r = \Omega\Big(\frac{1}{\varepsilon_{\mathrm{hon}}\left(\frac{1}{2}e^{\varepsilon/2}-\gamma_r/r\right)^2}\Big)$, and thus, (9.38) is recovered. □

We have therefore introduced a sequential-repetition test $\mathsf{T}_{\varepsilon_{\mathrm{h}}}^{r-\mathrm{coh}}$, parametrized by a confidence level $\varepsilon_{\mathrm{h}} > 0$, with the following guarantees:

- *completeness*: an honest prover at the claimed position *pos* is accepted with probability at least $1 - \varepsilon_{\mathrm{h}}$.
- *soundness*: any i.i.d. adversaries that pre-share at most a linear amount of entangled qubits will be rejected with probability at least $1 - O(\varepsilon_{\mathrm{h}})$.

Hence, by choosing ε_{h} sufficiently small and running the protocol for the prescribed number of rounds, the verifiers can certify the prover's location with high confidence while forcing well-resourced attackers to fail with essentially the same high probability.

9.4 Concrete bounds for given experimental parameters

In the above section, we proved that, if V_0 prepares a two-mode squeezed state with squeezing parameter ζ and $\lambda = \tanh\zeta$, with probability $1 - O(\lambda^{2^{m_0}})$ attackers

who pre-share $q = O(n - m_0)$ qubits will not be able to mimic arbitrarily close an honest prover. For that, we need that ε, E, t and u are such that exists $\tilde{\varepsilon} > 0$ and α for which (9.20) holds. In order to have parameters fulfilling (9.20) for $\varepsilon > 0$ we need that the attenuation parameter t and the excess noise power u of the quantum channel connecting V_0 and P fulfill the relation (9.22). In the section we analyze perfect and imperfect channels.

9.4.1 Perfect channel

We start by considering a perfect channel connecting V_0 and P, given by $t = 1$ and $u = 0$. We fix $\varepsilon = 0.1$ and assume the protocol is played enough rounds to statistically distinguish the honest party with an uncertainty

$$h(\mathcal{U}|P)_\phi \to \frac{1}{2}\log\frac{\pi e}{2} \simeq 1.0471, \tag{9.39}$$

from the uncertainty of at least one of the attackers being lower bounded by

$$\frac{1}{2}\log\frac{\pi e}{2} + \frac{\varepsilon}{4} \simeq 1.0721. \tag{9.40}$$

Fix an energy bound $E = 10^3$ in units such that $\hbar\omega = 1$. Then, the largest $\tilde{\varepsilon}$ that fulfills (9.20) is

$$\tilde{\varepsilon} \simeq 0.0037, \tag{9.41}$$

for $\alpha \simeq 0.036$, see Figure 9.3 for a representation of the inequality (9.20) where the value of ε is fixed and represented as the black plane and the gray surface represents the right-hand side of the inequality.

Notice that the energy term in (9.20) scales as $\tilde{\varepsilon}\log(E+1)$, i.e. logarithmically in E with a small factor $\tilde{\varepsilon}$ in front. Therefore, the inequality remains very stable with respect to E. For instance, if one picks $E = 10, 10^2, 10^4$, the values of the maximum $\tilde{\varepsilon}$ remain almost unchanged.

For the values of $\varepsilon = 0.1$ and $\tilde{\varepsilon} = 0.004$, the size of the (ε, q)-classical rounding in Lemma 9.3.8 is $\kappa = 12 \cdot 2^{2q+2m_0}$. Then, (9.31) in the proof of Lemma 9.3.8 is strictly upper bounded by 2^{-2^n} if $q \leq \frac{n}{2} - m_0 - 5$, for $n > 2(m_0 + 5)$. Then, for the above energies, Theorem 9.3.10 can be restated as follows.

9.4.1. Corollary. *Let $\varepsilon = 0.1$, $t = 1, u = 0$. Let $n > 2(m_0 + 5)$. Let the number of qubits that each Alice and Bob control at the beginning of the protocol be*

$$q \leq \frac{n}{2} - m_0 - 5. \tag{9.42}$$

Then, with probability $1 - O(\lambda^{2^{m_0}})$ the following holds. A random function f fulfills the following with probability at least $1 - 2^{-2^n}$: the uncertainties for Alice and Bob when attacking the protocol $\mathrm{QPV}^f_{\mathrm{coh}}$ are such that, for $\theta \in \{0, \frac{\pi}{2}\}$,

$$\max\{h(\mathcal{U}_\theta|A')_\psi, h(\mathcal{U}_\theta|B')_\psi\} \geq h(\mathcal{U}|P)_\phi + \frac{\varepsilon}{4}, \tag{9.43}$$

for every state $|\psi\rangle$ they possess in step 4. of the attack (end of the attack).

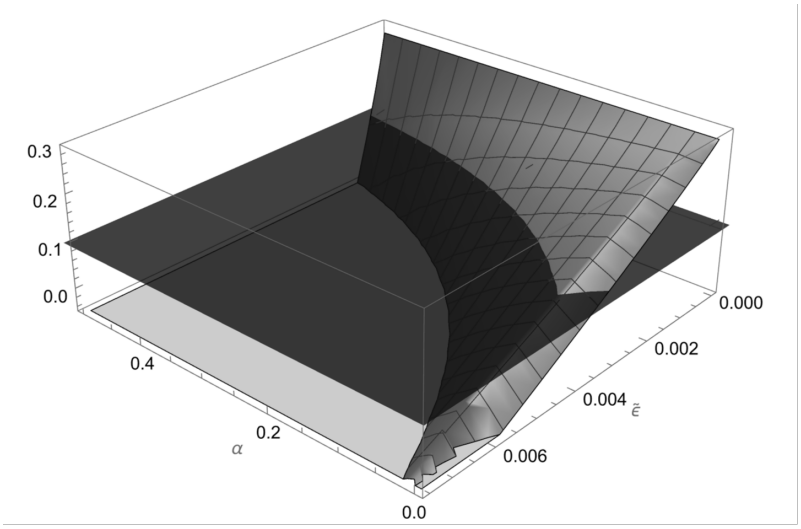


Figure 9.3: Representation of the left (transparent black) and right (gray surface) hand sides of the inequality (9.20) for $\varepsilon = 0.1, E = 10^3, t = 1$ and $u = 0$. The region where the gray surface is above the black plain gives the $(\alpha, \tilde{\varepsilon})$ such that the inequality (9.20) holds.

9.4.2 Imperfect channel

We now turn to lossy and noisy channels, characterized by parameters (t, u) that satisfy the admissibility condition (9.22). For such channels the quantity $\tilde{\varepsilon}$ appearing in Theorem 9.3.10 is obtained by solving the transcendental equation obtained by saturating (9.20); analytical closed forms are unavailable, so we determine $\tilde{\varepsilon}$ numerically.

For illustration, we pick three representative triples (ε, t, u) (see Table 9.1). For each chosen triple, we fix the verifier–controlled energy to $E = 10^3$, and optimize over $\alpha \in (0, \frac{1}{2})$ to obtain the corresponding value of $\tilde{\varepsilon}$. Exactly the same numerical routine can be repeated for any other set of channel parameters to yield the appropriate security constants for that operating point.

The admissible region in the (u, t)-plane is illustrated in Figure 9.2; the three operating points listed in Table 9.1 are marked therein.

The maximal values of $\tilde{\varepsilon}$ we obtain are collected in Table 9.1. For these values, we recover the same linear bounds as in Corollary 9.4.1. We have that for

- *Moderate loss, low noise* $(t = 0.8, u = 0.05)$. Even with 20% attenuation and 5% excess noise the protocol tolerates $\varepsilon = 0.03$ while retaining $\tilde{\varepsilon} \approx 3 \times 10^{-4}$.

- *High transmissivity, higher noise* $(t = 0.9, u = 0.12)$. Better transmission partly compensates for the larger u; the achievable $\tilde{\varepsilon}$ decreases only marginally.

- *Low loss, moderate noise* $(t = 0.95, u = 0.075)$. A larger target accuracy $\varepsilon =$

ε	t	u	α	$\tilde{\varepsilon}$
0.03	0.8	0.05	0.013	0.00031
0.03	0.9	0.12	0.013	0.00029
0.07	0.95	0.075	0.025	0.00131

Table 9.1: Maximum value of $\tilde{\varepsilon}$ fulfilling (9.20) given ε, t and u with its corresponding value of α that attains it.

0.07 is feasible, yielding $\tilde{\varepsilon} \approx 1.3 \times 10^{-3}$, an order of magnitude improvement over the previous settings.

In summary, solving (9.20) numerically shows that the security guarantees of $\mathrm{QPV}^{f}_{\mathrm{coh}}$ are robust against certain attenuation and excess noise. As long as the chosen (t, u) pair lies inside the shaded region of Figure 9.2, the linear soundness bounds of the perfect channel carry over unchanged.

Chapter 10

Discussion and future directions

In this thesis, we have analyzed the security of quantum position verification (QPV) protocols under various adversarial models, showing both fundamental properties and security threats when losses and errors are introduced. We have made progress toward real-world implementation by proposing protocols that maintain desirable security guarantees, taking into account the current technological barriers.

However, our results do not represent the end of the story for QPV, and some important problems remain open. Below, we highlight some directions for future research that build on the work presented in this thesis.

First, we showed QPV protocols that remain secure as long as the adversaries pre-share at most a *linear* amount of entanglement. In contrast, the best known generic attack requires adversaries to pre-share an *exponential* amount of entanglement, thereby constituting an upper bound on the resources needed to break QPV. No tighter lower bounds are currently known, and thus an exponential gap remains open.

We have seen that incorporating loss into the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol and its variants (using additional bases) still allows for security to be preserved. However, optimal attacks within our analysis framework are not known. This suggests that further improvements in error tolerance may be possible.

We have provided a generic method that makes use of semidefinite programming (SDP) to bound non-local quantum correlations whenever losses in quantum communication and errors in experimental set-ups are considered. We have analyzed scenarios where numerically solving SDPs provides tight bounds. However, it would be desirable to translate the numerical results to analytical proofs. Moreover, while we have provided code to implement our method, improving its efficiency and usability would make it more accessible to a broader range of users.

In the case of the routing protocol, we observed that the optimal attack succeeds with probability $\frac{3}{4} = 0.75$. For the m-fold parallel repetition, we derived an upper bound on the success probability of $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^{m} \simeq 0.85^{m}$. The best known

explicit attack, based on repeating the one-round strategy, achieves 0.75^m, leaving an unresolved gap between the performance of this attack and the upper bound.

For $\mathrm{QPV}^f_{\mathrm{BB84}}$, we established that attackers who pre-share a linear amount of entanglement in the size of the classical information can tolerate a qubit error rate of up to roughly 15%. We showed that this bound is essentially tight in the single-repetition setting, but tightness remains open for an arbitrary number of parallel repetitions, where our analysis allows up to 3.6% error. Furthermore, a structural modification of $\mathrm{QPV}^f_{\mathrm{BB84}}$ introduced in [ABB+23] makes the protocol fully loss tolerant while preserving its security guarantees. It is an open question whether this modification can be adapted to the parallel repetition setting, potentially preserving the security guarantees that we provided for $\mathrm{QPV}^{f;n\to m}_{\mathrm{BB84}}$ as well.

Finally, we demonstrated that QPV can be securely implemented using continuous-variable (CV) quantum systems—specifically, coherent states—while simultaneously addressing the three major challenges in QPV. However, the protocol that we presented has a fundamental limit on the amount of attenuation of the coherent states that can be tolerated, and therefore, current technology imposes a limit on the distances over which this protocol can be implemented. It remains unresolved whether alternative CV protocols can tolerate more attenuation while maintaining security, or whether a structural modification similar to that of [ABB+23] can be applied to $\mathrm{QPV}^f_{\mathrm{coh}}$ to achieve full attenuation tolerance.

Bibliography

[AB09] Janet Anders and Dan E. Browne. Computational power of correlations. *Phys. Rev. Lett.*, 102:050502, 2009. doi:10.1103/PhysRevLett.102.050502.

[ABB+23] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss, 2023. URL: https://arxiv.org/abs/2312.12614.

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007. doi:10.1103/PhysRevLett.98.230501.

[ABM+24] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8:1387, 2024. doi:10.22331/q-2024-06-27-1387.

[ABSL22a] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. On the role of quantum communication and loss in attacks on quantum position verification, 2022. URL: https://arxiv.org/abs/2208.04341.

[ABSL22b] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification, 2022. URL: https://arxiv.org/abs/2106.12911, arXiv:2106.12911.

[ACC+24] Omar Amer, Kaushik Chakraborty, David Cui, Fatih Kaleoglu, Charles Lim, Minzhao Liu, and Marco Pistoia. Certified randomness implies secure classical position-verification, 2024. URL: https://arxiv.org/abs/2410.03982.

[ACCM24] Vahid Asadi, Richard Cleve, Eric Culf, and Alex May. Linear gate bounds against natural functions for position-verification, 2024. URL: https://arxiv.org/abs/2402.18648.

[AEFR+23] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, Florian Speelman, and Philip Verduyn Lunel. Security of a continuous-variable based quantum position verification protocol, 2023. URL: https://arxiv.org/abs/2308.04166.

[AF04] Robert Alicki and Mark Fannes. Continuity of quantum conditional information. *Journal of Physics A: Mathematical and General*, 37(5):L55–L57, 2004. doi:http://doi.org/10.1088/0305-4470/37/5/L01.

[Agr10] Govind P. Agrawal. *Fiber-Optic Communication Systems*. Wiley Series in Microwave and Optical Engineering. Wiley, 2010. URL: https://books.google.nl/books?id=IvqNSQAACAAJ.

[AKL+22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. In *Advances in Cryptology – CRYPTO 2022*, pages 212–241. Springer Nature, 2022. doi:10.1007/978-3-031-15979-4_8.

[Ala40] Leon Alaoglu. Weak topologies of normed linear spaces. *Annals of Mathematics*, 41(1):252–267, 1940. doi:10.2307/1968829.

[Ali95] Farid Alizadeh. Interior point methods in semidefinite programming with applications to combinatorial optimization. *SIAM Journal on Optimization*, 5(1):13–51, 1995. doi:10.1137/0805005.

[Azu67] Kazuoki Azuma. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal*, 19(3), 1967. doi:10.2748/tmj/1178243286.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Process (Bangalore) (Piscataway, NJ: IEEE)*, 1984.

[BC94] Stefan Brands and David Chaum. Distance-bounding protocols. In *Advances in Cryptology — EUROCRYPT '93*, pages 344–359,

Berlin, Heidelberg, 1994. Springer Berlin Heidelberg. doi:10.1007/3-540-48285-7_30.

[BC23] Anne Broadbent and Eric Culf. Rigidity for monogamy-of-entanglement games. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 28:1–28:29, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2023.28.

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014. doi:10.1137/130913687.

[BCMdW10] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Reviews of Modern Physics*, 82(1):665–698, 2010. doi:10.1103/RevModPhys.82.665.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, 2014. doi:10.1103/RevModPhys.86.419.

[BCS22] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 18(6):623–626, 2022. doi:10.1038/s41567-022-01577-0.

[BCWW24] Mathieu Bozzio, Claude Crépeau, Petros Wallden, and Philip Walther. Quantum cryptography beyond key distribution: theory and experiment, 2024. URL: https://arxiv.org/abs/2411.08877.

[BDF+99] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070–1091, 1999. doi:10.1103/physreva.59.1070.

[Bel64] John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.

[BFSS13] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference*

on Innovations in Theoretical Computer Science - ITCS '13. ACM Press, 2013. doi:10.1145/2422436.2422455.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011. doi:10.1088/1367-2630/13/9/093036.

[BK15] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, 2015. URL: http://dx.doi.org/10.1088/1751-8113/48/8/083001, doi:10.1088/1751-8113/48/8/083001.

[BL20] Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:22, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.TQC.2020.4.

[Bla74] Richard E. Blahut. Hypothesis testing and information theory. *IEEE Transactions on Information Theory*, 20(4):405–417, 1974. doi:10.1109/TIT.1974.1055254.

[Boh13] Niels Bohr. On the constitution of atoms and molecules. *Philosophical Magazine*, 26(151):1–25, 1913. doi:10.1080/14786441308634955.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004. doi:10.1017/CBO9780511804441.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference*, volume 5677 of *Lecture Notes in Computer Science*, pages 391–407. Springer, 2009. doi:10.1007/978-3-642-03356-8_23.

[Che67] Pafnouty L. Chebyshev. Des valeurs moyennes. *Journal de Mathématiques Pures et Appliquées*, 12:177–184, 1867. French original; introduces the mean-value (Chebyshev) inequality.

[Che52] Herman Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of*

Mathematical Statistics, 23(4):493 – 507, 1952. doi:10.1214/aoms/1177729330.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett. 23*, 1969. doi:10.1103/PhysRevLett.23.880.

[CHTW04] Richard Cleve, Peter Hoyer, Ben Toner, and John Watrous. Consequences and limits of nonlocal strategies, 2004. URL: https://arxiv.org/abs/quant-ph/0404076.

[CJPPG15] Tom Cooney, Marius Junge, Carlos Palazuelos, and David Pérez-García. Rank-one quantum games. *Computational Complexity*, 24(1):133–196, 2015. doi:10.1007/s00037-014-0096-x.

[CKW00] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Physical Review A*, 61(5), 2000. doi:10.1103/physreva.61.052306.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5), 2015. doi:10.1103/physreva.92.052304.

[CLA01] Nicolas J. Cerf, Mel Lévy, and Gilles Van Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, 2001. doi:http://doi.org/10.1103/PhysRevA.63.052311.

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In *Advances in Cryptology – Crypto 2021*, pages 556–584. Springer, 2021. doi:10.1007/978-3-030-84242-0_20.

[CLMO13] Andrew M. Childs, Debbie Leung, Laura Mančinska, and Maris Ozols. A framework for bounding nonlocality of state discrimination. *Communications in Mathematical Physics*, 323(3):1121–1153, 2013. doi:10.1007/s00220-013-1784-0.

[CM23] Joy Cree and Alex May. Code-routing: a new attack on position verification. *Quantum*, 7:1079, 2023. doi:10.22331/q-2023-08-09-1079.

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2nd edition, 2006. doi:10.1002/047174882X.

[CZD19] Xin Cao, Michael Zopf, and Fei Ding. Telecom wavelength single photon sources. *Journal of Semiconductors*, 40(7):071901, 2019. doi:10.1088/1674-4926/40/7/071901.

[Dan47] George B. Dantzig. Programming in a linear structure. Technical Report P-53, The RAND Corporation, Santa Monica, CA, 1947. Unpublished manuscript that first presented the simplex method.

[DC22] Kfir Dolev and Sam Cree. Non-local computation of quantum circuits with small light cones. 2022. URL: https://arxiv.org/abs/2203.10106.

[Dir30] Paul. A. M. Dirac. *The Principles of Quantum Mechanics*. Oxford University Press, Oxford, 1st edition, 1930.

[DJ92] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558, 1992. doi:10.1098/rspa.1992.0167.

[Dol22] Kfir Dolev. Constraining the doability of relativistic quantum tasks. 2022. URL: https://arxiv.org/abs/1909.05403.

[DVC00] Wolfgang Dür, Guifré Vidal, and Juan Ignacio Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:062314, 2000. doi:10.1103/PhysRevA.62.062314.

[EF] Llorenç Escolà-Farràs. https://github.com/llorensescola/LossyAndConstrainedGames.

[EFB22] Llorenç Escolà-Farràs and Daniel Braun. Quantifying causal influence in quantum mechanics. *Physical Review A*, 106(6), 2022. doi:10.1103/physreva.106.062415.

[EFHO+25] Llorenç Escolà-Farràs, Jaròn Has, Maris Ozols, Christian Schaffner, and Mehrdad Tahmasbi. Parallel repetition of local simultaneous state discrimination. *Quantum*, 9:1706, 2025. doi:10.22331/q-2025-04-15-1706.

[EFPS24] Llorenç Escolà-Farràs, Léo Colisson Palais, and Florian Speelman. A quantum cloning game with applications to quantum position verification, 2024. URL: https://arxiv.org/abs/2410.22157, arXiv:2410.22157.

[EFRA+24] Llorenç Escolà-Farràs, Arpan Akash Ray, Rene Allerstorfer, Boris Škorić, and Florian Speelman. Continuous-variable quantum position verification secure against entangled attackers. *Phys. Rev. A*, 110:062605, 2024. doi:10.1103/PhysRevA.110.062605.

[EFS] Llorenç Escolà-Farràs and Florian Speelman. https://github.com/llorensescola/QPV_NPA_hierarchy.

[EFS23] Llorenç Escolà-Farràs and Florian Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *Phys. Rev. Lett.*, 131:140802, 2023. doi:http://doi.org/10.1103/PhysRevLett.131.140802.

[EFS25a] Llorenç Escolà-Farràs and Florian Speelman. Lossy-and-constrained extended non-local games with applications to quantum cryptography. *Quantum*, 9:1712, 2025. doi:10.22331/q-2025-04-18-1712.

[EFS25b] Llorenç Escolà-Farràs and Florian Speelman. Quantum position verification in one shot: parallel repetition of the f-BB84 and f-routing protocols, 2025. URL: https://arxiv.org/abs/2503.09544.

[Ein05a] Albert Einstein. On a heuristic viewpoint concerning the production and transformation of light. *Annalen der Physik*, 322(6):132–148, 1905. doi:10.1002/andp.19053220607.

[Ein05b] Albert Einstein. Zur elektrodynamik bewegter körper. *Annalen der Physik*, 17:891–921, 1905. English translation: On the Electrodynamics of Moving Bodies.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935. doi:10.1103/PhysRev.47.777.

[FBT+14] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B. Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, 55(12), 2014. doi:http://doi.org/10.1063/1.4903989.

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, 1982. doi:10.1007/BF02650179.

[Gas03] Stephen Gasiorowicz. *Quantum Physics*. Wiley, 3rd edition, 2003.

[GAW+03] Frédéric Grosshans, Gilles Assche, Jerome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421:238–41, 2003. doi:http://doi.org/10.1038/nature01289.

[GC20] Alvin Gonzales and Eric Chitambar. Bounds on instantaneous nonlocal quantum computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, 2020. doi:10.1109/TIT.2019.2950190.

[GCW+03] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Info. Comput.*, 3(7), 2003. doi:http://doi.org/10.26421/QIC3.s-6.

[GG02] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, 2002. doi:http://doi.org/10.1103/PhysRevLett.88.057902.

[GHZ89] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Going Beyond Bell's Theorem*, pages 69–72. Springer Netherlands, Dordrecht, 1989. doi:10.1007/978-94-017-0849-4_10.

[GLW16] Fei Gao, Bin Liu, and QiaoYan Wen. Quantum position verification in bounded-attack-frequency model. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 59(11):1–11, 2016.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pages 212–219. ACM, 1996. doi:10.1145/237814.237866.

[HEFO24] Jaron Has, Llorenç Escolà-Farràs, and Maris Ozols. Parallel repetition of LSSD (GitHub repository). https://github.com/JaronHas/ParallelRepetitionOfLSSD, 2024.

[Hei25] Werner Heisenberg. Über quantentheoretische umdeutung kinematischer und mechanischer beziehungen. *Zeitschrift für Physik*, 33:879–893, 1925. doi:10.1007/BF01328377.

[Hei27] Werner Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3-4):172–198, 1927. doi:10.1007/BF01397280.

[Hel69] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969. doi:10.1007/BF01007479.

[Hil00] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, 2000. doi:http://doi.org/10.1103/PhysRevA.61.022309.

[Hoe63] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[JKJL+13] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7:378–381, 2013. doi:10.1038/nphoton.2013.63.

[JMRW16] Nathaniel Johnston, Rajat Mittal, Vincent Russo, and John Watrous. Extended non-local games and monogamy-of-entanglement games. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 472(2189):20160003, 2016. doi:10.1098/rspa.2016.0003.

[Kar84] Narendra Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica*, 4(4):373–395, 1984. doi:10.1007/BF02579150.

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1), 2011. URL: http://dx.doi.org/10.1103/PhysRevA.84.012326, doi:10.1103/physreva.84.012326.

[KMSB06] Adrian Kent, William Munro, Tomothy Spiller, and Raymond Beausoleil. Tagging systems. US patent nr 2006/0022832. 2006. URL: https://patents.google.com/patent/US20060022832A1/en.

[KPB+25] Kirsten Kanneworff, Mio Poortvliet, Dirk Bouwmeester, Rene Allerstorfer, Philip Verduyn Lunel, Florian Speelman, Harry Buhrman, Petr Steindl, and Wolfgang Löffler. Towards experimental demonstration of quantum position verification using true single photons. 2025. URL: https://arxiv.org/abs/2502.04125, doi:10.48550/arXiv.2502.04125.

[Kum90] Prem Kumar. Quantum frequency conversion. *Optics Letters*, 15(24):1476–1478, 1990. doi:10.1364/OL.15.001476.

[LCL+17] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017. URL: `http://dx.doi.org/10.1038/nature23655`, `doi:10.1038/nature23655`.

[LD07] Yeong-Cherng Liang and Andrew C. Doherty. Bounds on quantum correlations in bell-inequality experiments. *Phys. Rev. A*, 75:042103, 2007. URL: `https://link.aps.org/doi/10.1103/PhysRevA.75.042103`, `doi:10.1103/PhysRevA.75.042103`.

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1), 2011. `doi:10.1103/physreva.83.012322`.

[LM00] Beatrice Laurent and Pascal Massart. Adaptive estimation of a quadratic functional by model selection. *Annals of statistics*, pages 1302–1338, 2000. `doi:10.1214/aos/1015957395`.

[LPF+18] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations (adv. quantum technol. 1/2018). *Advanced Quantum Technologies*, 1(1):1870011, 2018. URL: `https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.201870011`, `arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/qute.201870011`, `doi:10.1002/qute.201870011`.

[LR05] Monique Laurent and Franz Rendl. Semidefinite programming and integer programming. In *Discrete Optimization*, volume 12 of *Handbooks in Operations Research and Management Science*, pages 393–514. Elsevier, 2005. `doi:10.1016/S0927-0507(05)12008-8`.

[LXS+16] Charles Ci Wen Lim, Feihu Xu, George Siopsis, Eric Chitambar, Philip G. Evans, and Bing Qi. Loss-tolerant quantum secure positioning with weak laser sources. *Physical Review A*, 94(3), 2016. `doi:10.1103/physreva.94.032315`.

[Mal10] Robert A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81:042319, 2010. URL: https://link.aps.org/doi/10.1103/PhysRevA.81.042319, doi:10.1103/PhysRevA.81.042319.

[Mau00] Ueli Maurer. Authentication theory and hypothesis testing. *IEEE Transactions on Information Theory*, 46(4):1350–1356, 2000. doi:10.1109/18.850674.

[MOST24] Christian Majenz, Maris Ozols, Christian Schaffner, and Mehrdad Tahmasbi. Local simultaneous state discrimination. *Physical Review A*, 109(5), 2024. doi:10.1103/physreva.109.052217.

[MS77] Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*, volume 16 of *North-Holland Mathematical Library*. North-Holland, Amsterdam, 1977.

[MST21] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding, 2021. URL: https://arxiv.org/abs/2103.14510, arXiv:2103.14510.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, 2004. URL: http://dl.acm.org/citation.cfm?id=2011827.2011830.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011. doi:10.1017/CBO9780511976667.

[NN94] Yurii Nesterov and Arkadi Nemirovskii. *Interior-Point Polynomial Methods in Convex Programming*. SIAM, 1994. doi:10.1137/1.9781611970791.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, 2007. doi:10.1103/PhysRevLett.98.010401.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. doi:10.1088/1367-2630/10/7/073013.

[PAB+20] Stefano Pirandola, Ulrik L. Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, Jose Luis Pereira, Mohsen

Razavi, Jasni Shamsul Shaari, Marco Tomamichel, Vladyslav C. Usenko, Giuseppe Vallone, Paolo Villoresi, and Petros Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012, 2020. doi:10.1364/aop.361502.

[PAM+10] Stefano Pironio, Antonio Acín, Serge Massar, Alain Boyer de la Giroday, Dzmitry N. Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Luming Luo, Thomas A. Manning, and Christopher Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010. doi:10.1038/nature09008.

[PGK18] Damián Pitalúa-García and Iordanis Kerenidis. Practical and unconditionally secure spacetime-constrained oblivious transfer. *Physical Review A*, 98(3), 2018. doi:10.1103/physreva.98.032327.

[Pla01] Max Planck. On the law of distribution of energy in the normal spectrum. *Annalen der Physik*, 309(3):553–563, 1901. doi:10.1002/andp.19013090310.

[PPV10] Yury Polyanskiy, H. Vincent Poor, and Sergio Verdu. Channel coding rate in the finite blocklength regime. *IEEE Transactions on Information Theory*, 56(5):2307–2359, 2010. doi:10.1109/TIT.2010.2043769.

[QLP+15] Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, 5(4):041009, 2015. doi:10.1103/PhysRevX.5.041009.

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Physical Review A*, 91(4), 2015. doi:10.1103/physreva.91.042337.

[Ral99] Timothy C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, 1999. doi:http://doi.org/10.1103/PhysRevA.61.010303.

[Rei00] Margaret D. Reid. Quantum cryptography with a predetermined key using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A*, 62:062308, 2000. doi:http://doi.org/10.1103/PhysRevA.62.062308.

[RG15] Jérémy Ribeiro and Frédéric Grosshans. A tight lower bound for the BB84-states quantum-position-verification protocol, 2015. doi:10.48550/ARXIV.1504.07171.

[Rus17] Vincent Russo. Extended nonlocal games, 2017. URL: https://arxiv.org/abs/1704.07375.

[RV12] Oded Regev and Thomas Vidick. Quantum XOR games, 2012. URL: https://arxiv.org/abs/1207.4939.

[RW17] Vincent Russo and John Watrous. Extended nonlocal games from quantum-classical games, 2017. URL: https://arxiv.org/abs/1709.01837, arXiv:1709.01837.

[ŠB20] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, 2020. doi:10.22331/q-2020-09-30-337.

[Sch26] Erwin Schrödinger. Quantisierung als Eigenwertproblem (Erste Mitteilung). *Annalen der Physik*, 384(4):361–376, 1926.

[Sch35] Erwin Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(4):555–563, 1935.

[Sch07] Christian Schaffner. Cryptography in the bounded-quantum-storage model, 2007. URL: https://arxiv.org/abs/0709.0289.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE, 1994. doi:10.1109/SFCS.1994.365700.

[Sla59] Morton Slater. Lagrange multipliers revisited. Technical Report 80, Cowles Foundation for Research in Economics, 1959. URL: https://elischolar.library.yale.edu/cowles-discussion-paper-series/304/.

[Spe16a] Florian Speelman. Instantaneous non-local computation of low T-depth quantum circuits. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPIcs.TQC.2016.9.

[Spe16b] Florian Speelman. *Position-based quantum cryptography and catalytic computation*. PhD thesis, University of Amsterdam, 2016. URL: https://eprints.illc.uva.nl/id/eprint/2138.

[TFKW13] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. doi:10.1088/1367-2630/15/10/103002.

[TiHT+10] Hiroki Takesue, Ken ichi Harada, Kiyoshi Tamaki, Hiroshi Fukuda, Tai Tsuchizawa, Toshifumi Watanabe, Koji Yamada, and Sei ichi Itabashi. Long-distance entanglement-based quantum key distribution experiment using practical detectors. *Opt. Express*, 18(16):16777–16787, 2010. doi:10.1364/OE.18.016777.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology – CRYPTO 2014*, Lecture Notes in Computer Science, pages 1–18, Berlin, Heidelberg, 2014. Springer. doi:10.1007/978-3-662-44381-1_1.

[VB96] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996. doi:10.1137/1038003.

[Ver18] Roman Vershynin. *High-dimensional probability: an introduction with applications in data science*. Cambridge University Press, 2018. doi:10.1017/9781108231596.

[Was04] Larry Wasserman. *All of statistics: a concise course in statistical inference*. Springer Texts in Statistics. Springer, New York, 1st edition, 2004. doi:10.1007/978-0-387-21736-9.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. doi:10.1017/9781316848142.

[Wat21] John Watrous. Lecture 8: The hierarchy of Navascués, Pironio, and Acín. Lecture notes of "Advanced topics in quantum information theory", https://johnwatrous.com/wp-content/uploads/2023/08/QIT-notes.08.pdf, 2021.

[Weh06] Stephanie Wehner. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Physical Review A*, 73(2), 2006. doi:10.1103/physreva.73.022110.

[Wei] Eric W. Weisstein. Sphere point picking. From MathWorld–a Wolfram web resource. URL: https://mathworld.wolfram.com/SpherePointPicking.html.

[Wie83] Stephen Wiesner. Conjugate observables and the storage of quantum information. *SIGACT News*, 15(1):78–88, 1983. doi:10.1145/1008908.1008920.

[Wig32] Eugene Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749–759, 1932. doi:10.1103/PhysRev.40.749.

[Win16] Andreas Winter. Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1), 2016. doi:http://doi.org/10.1007/s00220-016-2609-8.

[Wit15] Peter Wittek. Algorithm 950. *ACM Transactions on Mathematical Software*, 41(3):1–12, 2015. URL: https://doi.org/10.1145%2F2699464, doi:10.1145/2699464.

[WLB+04] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93:170504, 2004. doi:http://doi.org/10.1103/PhysRevLett.93.170504.

[WPGP+12] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, 2012. doi:10.1103/RevModPhys.84.621.

[WZ82] William K. Wootters and Wojciech Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. doi:10.1038/299802a0.

Abstract

**On Quantum Position Verification:
Security and Experimental Constraints**

Quantum position verification (QPV) aims to verify an untrusted prover's location by combining quantum mechanics and special relativity. It is well-known that the use of quantum particles enhances security compared to solely using classical information, where a generic straightforward attack applies to any protocol. However, a generic attack exists for QPV as well. Nevertheless, such an attack requires an impractical amount of entanglement—even if fully fault-tolerant quantum computers are used—thus leaving open the possibility of security against powerful but resource-limited adversaries. As a result, several works in the literature have explored the security of QPV protocols under different adversarial models.

In this thesis, we work toward a fundamental understanding of certain QPV protocols and investigate how experimental constraints—which can severely compromise security—can be addressed. Three major problems must be considered in order to implement QPV in the real world: (i) entangled attackers—a fundamental problem, given that attackers with unlimited entanglement can successfully break any QPV protocol—(ii) transmission loss in quantum communication, and (iii) propagation of quantum messages significantly slower than the speed of light—both arising from current technological constraints.

We first address issue (ii) by providing the exact loss-tolerance of $\mathrm{QPV}_{\mathrm{BB84}}$, one of the most popular QPV protocols in the literature, which uses BB84 states. Motivated by the fact that generating entanglement over long distances is currently technologically challenging, we show security in the No-PE model, where adversaries do not pre-share entanglement prior to the execution of the protocol. However, $\mathrm{QPV}_{\mathrm{BB84}}$ has a fundamental loss-tolerance limit of 50%, and any loss above this threshold admits a perfect straightforward attack. This limitation imposes a bound on the physical distance for which the protocol can be securely implemented. We then show that a proper modification of this protocol can lead to a family of protocols that allow for greater loss tolerance while preserving security.

For $\mathrm{QPV}_{\mathrm{BB84}}$ and its family of extensions, two of the three critical drawbacks still apply: (i) little entanglement suffices to perfectly break them, and (iii) they require the quantum information to travel at the speed of light. Based on ideas

from the literature, we modify these protocols by adding extra classical information. Importantly, we show that this modification suffices to overcome both obstacles (i) and (iii), while preserving their loss-tolerant properties—(ii).

For the protocols analyzed in this thesis, two parties suffice to model any attack, and a way to quantify their performance (in a given model) can be done by analyzing the correlations that they can attain. Non-local games constitute an operational setting to understand them, and the security of various quantum cryptographic protocols, including some QPV protocols, can be reduced to a certain type of these games. In particular, a quantum referee distributes classical questions to quantum players. We provide a generic method using semidefinite programming (SDPs) to analyze any such game under experimental considerations such as loss in quantum communication and errors, which naturally arise in laboratories. This method applies to a broad class of cryptographic protocols. In this thesis, we show applications to QPV; in particular, by numerically solving SDPs, we recover, sharpen, and present new results.

In addition, we analytically analyze local simultaneous state discrimination (LSSD), which can be viewed as a particular class of non-local games with a quantum referee that naturally arise in quantum cryptography. We study the performance of classical and no-signaling (supra-quantum) correlations, which provide lower and upper bounds to the quantum correlations for a class of LSSD games.

Continuing with non-local correlations, we analyze the scenario where several parties receive a classical question from a quantum referee, but their answers must be a *quantum state*. We show that the security of the routing QPV protocol executed in parallel can be reduced to a game of this class, and we prove an exponentially small success probability for any attackers who do not pre-share entanglement.

Previous parallel repetition results in the QPV literature—including our results for the routing protocol, which allow verifying the location in a single execution—still suffered from drawbacks (i) and (iii). We prove that a single round of interaction suffices for secure position verification while overcoming these limitations by showing the security of the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol (an extension of $\mathrm{QPV}_{\mathrm{BB84}}$ using additional classical information) when executed in parallel.

Finally, motivated by practicality, we turn our attention to QPV using continuous variables. In particular, we analyze a protocol ($\mathrm{QPV}^{f}_{\mathrm{coh}}$) that uses coherent states, which are more efficient and economical to handle than single-photon preparations. We show that this protocol partially bypasses all three major problems of QPV, and thus presents a candidate for near-future implementation.

Samenvatting

Over Kwantumpositieverificatie:
Beveiliging en Experimentele Beperkingen

Kwantumpositieverificatie (QPV) heeft als doel de locatie van een niet-vertrouwde persoon te verifiëren door kwantummechanica en speciale relativiteit te combineren. Het is bekend dat het gebruik van kwantumdeeltjes de veiligheid verhoogt ten opzichte van protocollen met enkel klassieke informatie, welke met een gemakkelijke aanval gebroken worden. Er bestaat echter ook een generieke aanval op QPV. Niettemin vereist een dergelijke aanval een onpraktische hoeveelheid verstrengeling, zelfs als volledig fouttolerante kwantumcomputers worden gebruikt. Er is dus een mogelijkheid dat protocollen bestaan die veilig zijn tegen aanvallers met beperkte resources, en in de literatuur wordt de veiligheid van QPV-protocollen in diverse aanvalsmodellen bestudeerd.

In dit proefschrift werken we aan een fundamenteel begrip van bepaalde QPV-protocollen en onderzoeken we hoe experimentele beperkingen—die de veiligheid ernstig in gevaar kunnen brengen—aangepakt kunnen worden. Drie grote problemen moeten overwogen worden om QPV in de echte wereld te implementeren: (i) verstrengelde aanvallers—een fundamenteel probleem, gezien het feit dat aanvallers met onbeperkte verstrengeling elk QPV-protocol succesvol kunnen breken—(ii) transmissieverlies in kwantumcommunicatie, en (iii) voortplantingssnelheden van kwantumboodschappen die aanzienlijk langzamer zijn dan dat van licht—beiden voortkomend uit de huidige technologische beperkingen.

We gaan eerst in op probleem (ii) door de exacte verlies-tolerantie te berekenen van $\mathrm{QPV}_{\mathrm{BB84}}$, een van de populairste QPV-protocollen in de literatuur, gebaseerd op BB84 toestanden. Gemotiveerd door het feit dat het genereren van verstrengeling over lange afstanden momenteel technologisch uitdagend is, laten we veiligheid zien in het No-PE model, waar tegenstanders geen verstrengeling delen voorafgaand aan het protocol. Echter, $\mathrm{QPV}_{\mathrm{BB84}}$ heeft een fundamentele verliestolerantiegrens van 50%, en elk verlies boven deze drempelwaarde laat een perfecte en ongecompliceerde aanval toe. Deze beperking geeft een aan de fysieke afstand waarvoor het protocol veilig kan worden geïmplementeerd. Vervolgens brengen we een aanpassing aan in het protocol, wat leidt tot een familie protocollen met een grotere verliesbestendigheid terwijl de veiligheid gewaarborgd blijft.

Voor $\mathrm{QPV}_{\mathrm{BB84}}$ en zijn familie van uitbreidingen zijn twee van de drie kritieke nadelen nog steeds van toepassing: (i) weinig verstrengeling volstaat om ze perfect te breken, en (iii) ze vereisen dat de kwantuminformatie met de snelheid van het licht reist. Op basis van ideeën uit de literatuur passen we deze protocollen aan

door extra klassieke informatie toe te voegen. Belangrijk is dat we laten zien dat deze aanpassing voldoende is om beide obstakels (i) en (iii) weg te nemen, met behoud van hun verlies-tolerante eigenschappen (ii).

Voor de protocollen die in dit proefschrift worden geanalyseerd, volstaan twee partijen om elke aanval te modelleren. Een manier om hun prestaties te kwantificeren (in een gegeven model) is door de correlaties die ze kunnen bereiken te analyseren. Niet-lokale spellen vormen een operationele omgeving om ze te begrijpen; de veiligheid van verschillende kwantumcryptografische protocollen, waaronder sommige QPV-protocollen, kan worden gereduceerd tot een bepaald type van deze spellen. In het bijzonder verdeelt een kwantumscheidsrechter klassieke vragen onder kwantumspelers. We bieden een generieke methode die gebruik maakt van semidefinite programming (SDP's) om zo'n spel te analyseren onder experimentele omstandigheden, met verliezen en fouten in de kwantumcommunicatie die van nature voorkomen in laboratoria. Deze methode is van toepassing op een brede klasse van cryptografische protocollen. In dit proefschrift tonen we toepassingen op QPV, lossen we SDP's numeriek op waarmee eerdere resultaten worden teruggevonden en verscherpt, en presenteren we nieuwe resultaten.

Daarnaast bestuderen we op analytische wijze lokale simultane toestandsdiscriminatie (LSSD), die kan worden gezien als een bepaalde klasse van niet-lokale spellen met een kwantumscheidsrechter die van nature voorkomen in kwantumcryptografie. We bestuderen de prestaties van klassieke en niet-signalerende (supra-kwantum) correlaties, die onder- en bovengrenzen geven aan de kwantumcorrelaties voor een klasse van LSSD-spellen.

Voortbouwend op niet-lokale correlaties, analyseren we het scenario waarbij meerdere partijen een klassieke vraag krijgen van een kwantumscheidsrechter, maar waarbij hun antwoorden een kwantumtoestand zijn. We laten zien dat de veiligheid van het routing QPV-protocol dat parallel wordt uitgevoerd gereduceerd kan worden tot een enkel spel van deze klasse, en we bewijzen een exponentieel kleine succeskans voor aanvallers die voorafgaand geen verstrengeling delen.

Eerdere parallelle herhalingsresultaten in de QPV literatuur—inclusief onze resultaten voor het routeringsprotocol, die het mogelijk maken om de locatie in een enkele uitvoering te verifiëren—hebben nog steeds te lijden onder de nadelen (i) en (iii). We bewijzen dat een enkele interactieronde voldoende is voor een veilige positieverificatie en nemen eerdergenoemde beperkingen weg door de veiligheid van het $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol (een uitbreiding van $\mathrm{QPV}_{\mathrm{BB84}}$ met extra klassieke informatie) aan te tonen wanneer het parallel wordt uitgevoerd.

Om praktische redenen richten we onze aandacht ook op QPV met continue variabelen. In het bijzonder analyseren we een protocol ($\mathrm{QPV}^{f}_{\mathrm{coh}}$) dat coherente toestanden gebruikt, die efficiënter en economischer te hanteren zijn dan éénfotontoestanden. We laten zien dat dit protocol alle drie de grote problemen van QPV gedeeltelijk omzeilt en dus een kandidaat is voor praktische implementatie in de nabije toekomst.