Lossy-and-Constrained Extended Non-Local Games with Applications to Quantum Cryptography

Llorenç Escolà-Farràs[1,2] and Florian Speelman[1,2]

[1]QuSoft, CWI Amsterdam, Science Park 123, 1098 XG Amsterdam, The Netherlands
[2]Multiscale Networked Systems (MNS), Informatics Institute, University of Amsterdam, Science Park 904, 1098 XH Amsterdam, The Netherlands

arXiv:2405.13717v2 [quant-ph] 9 Apr 2025

Extended non-local games are a generalization of monogamy-of-entanglement games, played by two quantum parties and a quantum referee that performs a measurement on their local quantum system. Along the lines of the NPA hierarchy, the optimal winning probability of those games can be upper bounded by a hierarchy of semidefinite programs (SDPs) converging to the optimal value. Here, we show that if one extends such games by considering *constraints* and *loss*, motivated by experimental errors and loss through quantum communication, the convergence of the SDPs to the optimal value still holds. We give applications of this result, and we compute SDPs that show tighter security of protocols for relativistic bit commitment, quantum key distribution, and quantum position verification.

Contents

1 Introduction **2**

2 Preliminaries **3**

3 Lossy-and-constrained extended non-local games **3**
3.1 Convergence of $\omega_{comm}(\mathcal{G}_{C,\eta})$ via SDPs . . . 7

4 Concrete games **12**
4.1 Constrained BB84 monogamy-of-entanglement game . . . 12
4.2 Alice guessing game with constraints . . . 13
4.3 Local guessing game . . . 14
4.4 Lossy monogamy-of-entanglement games . . . 16

5 Applications to quantum cryptography **19**
5.1 Application to relativistic Bit Commitment (with loss) . . . 19
5.1.1 Security for dishonest Charlie . . . 22
5.2 Application to device-independent quantum key distribution . . . 23
5.3 Application to quantum position verification . . . 24
5.3.1 Security for 2-fold parallel repetition of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ . . . 26

6 Discussion and open problems **27**

7 Acknowledgments **27**

A Proof of Proposition 4.3 **30**

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 [1], but also lead to many applications such as secure key distribution [2], certified randomness [3], reduced communication complexity [4], self-testing [5, 6], and computation [7].

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 [8].

The usage of semidefinite programming (SDP) techniques to bound correlations of non-local games was initiated by Cleve, Høyer, Toner and Watrous [9], Wehner [10], and Liang and Doherty [11]. 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 [12], with the subsequent result showing that this hierarchy is complete [13].

Non-local correlations have also been investigated beyond the classical questions and answers scenario, e.g. in a quantum XOR game [14], a quantum referee who sends quantum questions to Alice and Bob, who have to respond with classical answers —classical-quantum games—, or in a rank-one quantum game [15], both the questions and the 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 type of games are known in the literature as extended non-local games, introduced by [16]. They are a generalization of monogamy-of-entanglement games [17], where the referee, Alice and Bob pre-share a joint quantum state, the referee performs a local measurement on their local register, chosen from a given 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 [17], and have been studied in the context of quantum steering [18]. Using similar ideas as in [13], it was shown [16] that there exists a hierarchy of SDPs that bound the optimal winning probability of an extended non-local game, and it is such that converges to its optimal 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 treating these two separately can give significant improvements in the analysis, see e.g. [19], where a loss-tolerance of up to 50% is shown for a given protocol with only around 15% error-tolerance [17], 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.

Contributions. 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 [16] can be applied to the *lossy-and-constrained* version, and that there exists a hierarchy of SDPs converging to the optimal 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 an-

alyze them in their lossy-and-constrained version. By computing the corresponding semidefinite programs, we show a way to verify some previously known results by solely computing an SDP. Moreover, we find new tighter and new tight results for those games. It is worth to highlight 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 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 [20], using *cvxpy* [7]. These programs can be modified and adapted to analyze other games.

Finally, we study applications to quantum cryptography, 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 executed using only the description of the game. Using our analysis, we provide tighter security bounds. First, we study a relativistic bit commitment protocol originally introduced by Kent [21], where n-BB84 states [22] are used in the protocol. In [23], security was shown for large n, a result that was tightened in [24] that applied for every n. Here, we show that the security of this protocol can be reduced to an extended non-local game, and we provide tighter bounds by computing the corresponding SDPs for small values of n. Second, we use a constrained extended non-local game to show security of device-independent quantum key distribution [22], solving SDPs for small n, where n is the number qubits used in the protocol. Third, we use lossy-and-constrained extended non-local games to study security for certain protocols in quantum position verification (QPV) in the presence of photon loss. For the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol with loss, we obtain, in an easier way, the results shown in [19], 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 [19] for an extension of the above protocol, and we show that they are tight. We finally apply our results to show security of the 2-fold parallel repetition of $\mathrm{QPV}_{\mathrm{BB84}}$ with loss.

2 Preliminaries

For $n \in \mathbb{N}$, we will denote $[n] := \{0, \dots, n-1\}$. Let $\mathcal{H}$, $\mathcal{H}'$ be finite-dimensional Hilbert spaces, we denote by $\mathcal{B}(\mathcal{H}, \mathcal{H}')$ the set of bounded operators from $\mathcal{H}$ to $\mathcal{H}'$ and $\mathcal{B}(\mathcal{H}) = \mathcal{B}(\mathcal{H}, \mathcal{H})$. For $A, B \in \mathcal{B}(\mathcal{H})$, we denote $A \succeq B$ if $A - B$ is positive semidefinite. Denote by $\mathcal{S}(\mathcal{H})$ the set of quantum states on $\mathcal{H}$, i.e. $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \geq 0, \mathrm{Tr}[\rho] = 1)\}$. A pure state will be denoted by a ket $|\psi\rangle \in \mathcal{H}$. A maximally entangled state or EPR pair is the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We will refer to basis 0 and 1 to denote the computational and Hadamard basis, respectively. The Hadamard transformation will be denoted by $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. For bit strings $x, a \in \{0,1\}^n$ we denote

$$|a^x\rangle\langle a^x| := |a_0^{x_0}\rangle\langle a_0^{x_0}| \otimes \cdots \otimes |a_{n-1}^{x_{n-1}}\rangle\langle a_{n-1}^{x_{n-1}}|, \tag{1}$$

where $|a_i^{x_i}\rangle\langle a_i^{x_i}| = H^{x_i}|a_i\rangle\langle a_i|H^{x_i}$. The Hamming distance d_H between two bit strings $x, y \in \{0,1\}^n$ is the number of positions at which they differ, i.e.

$$d_H(x, y) := \{i \in [n] \mid x_i \neq y_i\}. \tag{2}$$

For a set $\mathcal{X}$, we denote $\mathcal{X}^{\times n} := \mathcal{X} \times \cdots \times \mathcal{X}$, where the Cartesian product is taken n times.

3 Lossy-and-constrained extended non-local games

Following [16], 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 $m \in \mathbb{N}$ for all $(z, v) \in \mathcal{Z} \times \mathcal{V}$ and let $V := \{V_v^z\}_{z,v}$. 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.

Definition 3.1. *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*

$$\mathcal{G} = (q, V, W), \tag{3}$$

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* m*, i.e. the reduced state* $\rho_R \in \mathcal{S}(\mathcal{H}_R)$*, for* $\mathcal{H}_R \cong \mathbb{C}^m$*.*

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*

$$\sum_{z,x,y,v,a,b \in W} q(z, x, y) \mathrm{Tr}\left[V^z_v \rho^{x,y}_{R_{a,b}}\right]. \tag{4}$$

See Fig. 1 for a schematic representation of an extended non-local game.

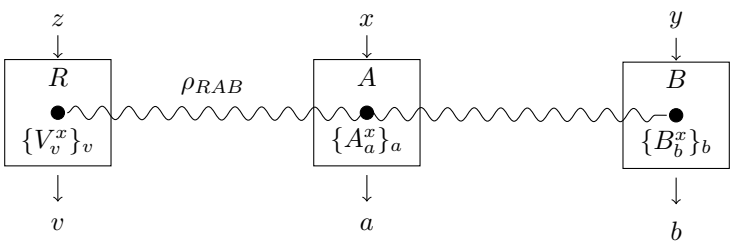


Figure 1: Schematic representation of an extended non-local game. The undulated line represents the tripartite quantum state ρ_{RAB} shared amongst the three parties.

Definition 3.2. *A* monogamy-of-entanglement game *[17] is an extended non-local game where* $x = y = z$*, i.e. all the parties get the same question, and the referee performs the measurement* $\{V^x_a\}$*. The winning set is given by* $W = \{(x, v, a, b) \mid v = a = b\}$*. Then, a monogamy-of-entanglement game will be denoted by the tuple*

$$\mathcal{G} = (q, V). \tag{5}$$

To illustrate the concept of extended non-local games, consider the following example introduced in [17].

Example 3.3. *The* BB84 monogamy-of-entanglement game *is described as follows. Alice and Bob prepare a quantum state and give a qubit to the referee, who, uniformly at random, choses to measure it 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*

$$\mathcal{G}^{BB84} = \left(q(x) = \frac{1}{|\mathcal{X}|}, V = \{V^x_a = H^x|a\rangle\langle a|H^x\}_{x,a}, W = \{(x, v, a, b) \mid v = a = b\}_{x,v,a,b}\right), \tag{6}$$

with $\mathcal{X} = \mathcal{V} = \mathcal{A} = \mathcal{B} = \{0, 1\}$*.*

The most general thing that Alice and Bob can do using quantum mechanics is to perform POVMs $\{A^x_a\}$ and $\{B^y_b\}$ on their local registers to answer a and b, respectively. A *quantum strategy* S_Q is defined by the tuple $\{\rho_{RAB}, A^x_a, B^y_b\}_{x,y,a,b}$, and the quantum winning probability of the extended non-local game $\mathcal{G}$ is defined as

$$\omega_Q(\mathcal{G}) := \sup \sum_{(z,x,y,v,a,b) \in W} q(z, x, y) \mathrm{Tr}[(V^z_v \otimes A^x_a \otimes B^y_b)\rho_{RAB}], \tag{7}$$

where the supremum (sup) is taken over all quantum states ρ_{RAB}, 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 work will be taken over the same conditions. A particular case of quantum strategies that will appear in this work are the *unentangled* strategies. These correspond to quantum strategies 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:

$$\mathrm{Tr}[(V_v^z \otimes A_a^x \otimes B_b^y)\rho_{RAB}] = \sum_\lambda p_\lambda \mathrm{Tr}\big[V_v^z \rho_R^\lambda\big] \mathrm{Tr}\big[A_a^x \rho_A^\lambda\big] \mathrm{Tr}\big[B_b^y \rho_B^\lambda\big]. \tag{8}$$

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

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

where $p(a|x)$ and $p(b|y)$ are the (classical) probabilities to output a and b, given x and y, respectively. For $\mathcal{G}^{BB84}$, it was shown [17] that $\omega_Q(\mathcal{G}^{BB84}) = \cos^2\big(\frac{\pi}{8}\big)$, which is attained by the unentangled strategy $S_Q^{BB84} = \{|\phi\rangle\langle\phi|, A_a^x = \delta_{a0}, B_a^x = \delta_{a0}\}$, where $|\phi\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$.

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 $\mathcal{H}$ such that $[A_a^x, B_b^y] = 0$, i.e. they commute, and a joint tripartite state ρ_{RAB}. The respective commuting winning probability of a non-local game $\mathcal{G}$ is defined as

$$\omega_{comm}(\mathcal{G}) := \sup \sum_{(z,x,y,v,a,b)\in W} q(z,x,y) \mathrm{Tr}[(V_v^z \otimes A_a^x B_b^y)\rho_{RAB}]. \tag{9}$$

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 $\mathcal{G}$,

$$\omega_Q(\mathcal{G}) \leq \omega_{comm}(\mathcal{G}). \tag{10}$$

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 [17], 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.

Example 3.4. *Consider the $\mathcal{G}^{BB84}$ game, described in Example 3.3.*

1. Constrained version (see Section 4.1 for more details): *Motivated by security of quantum cryptographic protocols, this game is used to reduce their security where Alice and Bob pretend to mimic the action of an honest prover in a given protocol, see Section 5 for more details. In such a case, Alice and Bob have to coordinate their actions, and a natural imposition is given by forbidding them to answer differently. This is done by imposing that for every strategy* $S_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,

$$\sum_{x,a,a'\neq b'} q(x)\mathrm{Tr}[(V_a^x \otimes A_{a'}^x \otimes B_{b'}^x)\rho_{RAB}] = 0. \tag{11}$$

2. Lossy version (see Section 4.4 for more 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* $S_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,

$$\sum_{x} q(x)\mathrm{Tr}[(\mathbb{I}_R \otimes A_\perp^x \otimes B_\perp^y)\rho_{RAB}] = 1-\eta. \tag{12}$$

We now formalize these concepts with the following definitions.

Definition 3.5. *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 $c_\ell^0 \leq c_\ell^1$. We say that an extended non-local game is* constrained, *and we denote it by $\mathcal{G}_C$, if for every strategy* $S_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,

$$c_\ell^0 \leq \sum_{z,x,y,v,a,b} \alpha_\ell(v,a,b|z,x,y)\mathrm{Tr}[(V_v^z \otimes A_a^x \otimes B_b^y)\rho_{RAB}] \leq c_\ell^1 \quad \forall \ell \in \{1,\dots,L\}. \tag{13}$$

See Section 4 for examples of how to encode other problems as such a game.

Definition 3.6. *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 $b \in \mathcal{B}\cup\{\perp\}$,*

$$\sum_{x,y} q(x,y)\mathrm{Tr}[(\mathbb{I}_R \otimes A_\perp^x \otimes B_\perp^y)\rho_{RAB}] = 1-\eta. \tag{14}$$

See more examples in Section 4. 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., $\mathrm{Tr}[(\mathbb{I}_R \otimes A_\perp^x B_\perp^y)\rho_{RAB}] = 1-\eta\ \forall x,y \in \mathcal{X}\times\mathcal{Y}$ 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.

Remark 3.7. (The guessing strategy). *Consider a monogamy-of-entanglement game where the referee performs projective measurements $\{V_v^x\}$. If the distribution of the questions $x \in \mathcal{X}$ is uniform, Alice and Bob can make a guess $\tilde{x}$ for x that will be correct with probability $\frac{1}{|\mathcal{X}|}$. 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 $V_a^{\tilde{x}}$ projects onto, i.e. $V_a^{\tilde{x}}|\psi\rangle = |\psi\rangle$. Then, if they receive $x = \tilde{x}$, they answer a and otherwise, they answer $\perp$. This strategy based on guessing x is such that Alice and Bob are going to be correct with probability $\frac{1}{|\mathcal{X}|}$ and will answer $\perp$ with probability $1-\frac{1}{|\mathcal{X}|}$; they will never give a wrong answer.*

If the distribution is not uniform, then Alice and Bob guess $\tilde{x}$ with the highest probability, which will be at least $\frac{1}{|\mathcal{X}|}$, and then they will be correct with probability at least $\frac{1}{|\mathcal{X}|}$.

Because of the general strategy described in Remark 3.7, throughout this paper we will consider the range $\eta \geq \frac{1}{|\mathcal{X}|}$, unless explicitly stated otherwise.

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 $\omega_{comm}(\mathcal{G}_{C,\eta})$, respectively.

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

In [16], it was shown that similar ideas as in [13] 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 [16] 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 [16], consider the set

$$\Sigma = (\mathcal{X} \times \mathcal{A}) \sqcup (\mathcal{Y} \times \mathcal{B}), \tag{15}$$

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,

$$\begin{aligned}
&\Sigma^{\leq 0} = \{\varepsilon\},\\
&\Sigma^{\leq 1} = \Sigma^{\leq 0} \cup \{(x,a),(y,b)\}_{(x,a,y,b)\in\mathcal{X}\times\mathcal{A}\times\mathcal{Y}\times\mathcal{B}},\\
&\Sigma^{\leq 2} = \Sigma^{\leq 1} \cup \{(x,a,x',a'),(y,b,y',b'),(x,a,y,b),(y,b,x,a)\}_{(x,x',a,a',y,y',b,b')\in\mathcal{X}^{\times 2}\times\mathcal{A}^{\times 2}\times\mathcal{Y}^{\times 2}\times\mathcal{B}^{\times 2}}.
\end{aligned} \tag{16}$$

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

$$\Sigma^{\leq \text{`}1+AB\text{'}} = \Sigma^{\leq 1} \cup \{(x,a,y,b)\}_{(x,a,y,b)\in\mathcal{X}\times\mathcal{A}\times\mathcal{Y}\times\mathcal{B}} \subset \Sigma^{\leq 2}. \tag{17}$$

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 $\sigma_B \in \mathcal{Y}\times\mathcal{B}$, $s\sigma_A\sigma_B t \sim s\sigma_B\sigma_A t$.

Definition 3.8. (Admissible function [16]). *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 $(x,y) \in \mathcal{X}\times\mathcal{Y}$,*
$$\sum_{a\in\mathcal{A}} \phi(s(x,a)t) = \phi(s,t) = \sum_{b\in\mathcal{B}} \phi(s(y,b)t). \tag{18}$$
2. *For every $s,t \in \Sigma^*$, every $(x,y) \in \mathcal{X}\times\mathcal{Y}$, and every $a \neq a' \in \mathcal{A}$, $b \neq b' \in \mathcal{B}$,*
$$\phi(s(x,a)(x,a')t) = 0 = \phi(s(y,b)(y,b')t). \tag{19}$$
3. *For every $s,t \in \Sigma^*$ such that $s \sim t$,*
$$\phi(s) = \phi(t). \tag{20}$$

A function $\phi : \Sigma^{\leq k} \to \mathbb{C}$ is said to be admissible if and only if (18)-(20) hold, given that the arguments' length is such that ϕ is defined.

We extend the definition of kth order admissible matrices in [16].

Definition 3.9. *For every $1 \leq k \in \mathbb{Z}$, let $M^{(k)}$ be a block matrix of the form*

$$M^{(k)} = \begin{pmatrix} M^{(k)}_{1,1} & \cdots & M^{(k)}_{1,m} \\ \vdots & \ddots & \vdots \\ M^{(k)}_{m,1} & \cdots & M^{(k)}_{m,m} \end{pmatrix} \tag{21}$$

where $M^{(k)}_{i,j} : \Sigma^{\leq k} \times \Sigma^{\leq k} \to \mathbb{C}$ for every $i,j \in \{1,\ldots,m\}$. 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 $i,j \in \{1,\dots,m\}$, there exists an admissible function $\phi_{i,j} : \Sigma^{2k} \to \mathbb{C}$ such that for every $s,t \in \Sigma^{\leq k}$,*
$$M^{(k)}_{i,j}(s,t) = \phi_{i,j}(s^R t). \tag{22}$$

2. *The following holds*
$$\mathrm{Tr}\Big[M^{(k)}(\varepsilon,\varepsilon)\Big] = 1. \tag{23}$$

3. *For all $\ell \in \{1,\dots,L\}$,*
$$c^0_\ell \leq \sum_{z,x,y,v,a,b} \alpha_\ell(v,a,b|z,x,y)\mathrm{Tr}\Big[V^z_v M^{(k)}((x,a),(y,b))\Big] \leq c^1_\ell, \tag{24}$$
and
$$\sum_{x,y} q(x,y)\mathrm{Tr}\Big[M^{(k)}((x,\perp),(y,\perp))\Big] = 1-\eta. \tag{25}$$

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

The definition of a kth order admissible matrix defined in [16] is the same, except without condition 3.

For a lossy-and-extended kth order admissible matrix for $\mathcal{G}_{C,\eta}$ with constraints $C = \{\alpha_\ell(z,x,y|v,a,b), c^0_\ell, c^1_\ell\}_{(\ell,z,x,y,v,a,b)}$, consider
$$\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) := \sup \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}\Big[V^z_v M^{(k)}((x,a),(y,b))\Big]. \tag{26}$$

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 (14).

Remark 3.10. *The value $\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta})$ can be computed by the following SDP:*
$$\begin{aligned} &\max \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}\Big[V^z_v M^{(k)}((x,a),(y,b))\Big] \\ &\textit{subject to the linear constraints given by (22)-(25),} \\ &\textit{and } M^{(k)} \succeq 0. \end{aligned} \tag{27}$$

Recall that semidefinite programs (SDPs) can be solved in polynomial time to any fixed prescribed precision, see e.g. [25, 26].

Lemma 3.11. *For all $k \geq k' \geq 1$,*
$$\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) \geq \omega^{(k')}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) \geq \omega_{comm}(\mathcal{G}_{\mathcal{C},\eta}). \tag{28}$$

Proof. The function K defined as $K(a,b|x,y) = \mathrm{Tr}_{AB}[(\mathbb{I}_R \otimes A^x_a B^y_b)\rho_{RAB}]$ is said to be a *commuting measurement assemblage*. Then, (7) can be rewritten as
$$\omega_{comm}(\mathcal{G}) = \sup \sum_{(z,x,y,v,a,b)\in W} q(z,x,y)\mathrm{Tr}[V^z_v K(a,b|x,y)]. \tag{29}$$

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 $S_{comm} = \{|\psi\rangle, A^x_a, B^y_b\}$ for $\mathcal{G}_{C,\eta}$, with $|\psi\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ and A^x_a, B^y_b 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 $|\psi\rangle = \sum_{i=1}^m \lambda_i |i\rangle_R |\psi_i\rangle_{AB}$, 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
$$\Pi^z_c := \begin{cases} A^z_c \text{ if } (c,z) \in \mathcal{A}\times\mathcal{X}, \\ B^z_c \text{ if } (c,z) \in \mathcal{B}\times\mathcal{Y}. \end{cases} \tag{30}$$

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

$$M^{(k)}_{i,j}(s,t) = \phi_{i,j}(s^R t)\ \forall i,j \in \{1,\dots,m\}, \tag{31}$$

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

$$\phi_{i,j}((z_1,c_1)\dots(z_l,c_l)) = \langle\tilde{\psi}_j|\Pi^{z_1}_{c_1}\cdots\Pi^{z_l}_{c_l}|\tilde{\psi}_i\rangle. \tag{32}$$

The functions $\phi_{i,j}$ fulfill (18)-(20), and thus they are admissible functions. Notice that

$$\begin{aligned} 1 = \mathrm{Tr}[|\psi\rangle\langle\psi|] &= \mathrm{Tr}\left[\sum_{i,j=1}^{m}|i\rangle|\tilde{\psi}_i\rangle\langle\tilde{\psi}_j|\langle j|\right] = \sum_{i,j=1}^{m}\langle i|j\rangle\langle\tilde{\psi}_i|\tilde{\psi}_j\rangle \\ &= \sum_{i=1}^{m}\langle\tilde{\psi}_i|\tilde{\psi}_i\rangle = \sum_{i=1}^{m}\phi_{i,i}(\varepsilon,\varepsilon) = \sum_{i=1}^{m}M^{(k)}_{i,i}(\varepsilon,\varepsilon) = \mathrm{Tr}\big[M^k(\varepsilon,\varepsilon)\big], \end{aligned} \tag{33}$$

and therefore (23) is fulfilled. Moreover, S_{comm} is such that equations (24) and (25) 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

$$\begin{aligned} K(a,b|x,y) &= \mathrm{Tr}_{AB}\left[(\mathbb{I}_R\otimes A^x_a B^y_b)\sum_{i,j=1}^{m}\lambda_i\lambda_j|j\rangle|\psi_j\rangle\langle\psi_i|\langle i|\right] \\ &= \sum_{k=1}^{\dim\mathcal{H}}\langle\psi_k|(\mathbb{I}_R\otimes A^x_a B^y_b)\sum_{i,j=1}^{m}\lambda_i\lambda_j|j\rangle|\psi_j\rangle\langle\psi_i|\langle i|)|\psi_k\rangle = \sum_{i,j=1}^{m}|i\rangle\langle j|\lambda_j\langle\psi_j|A^x_a B^y_b|\psi_i\rangle\lambda_i \\ &= \sum_{i,j=1}^{m}|i\rangle\langle j|\langle\tilde{\psi}_j|A^x_a B^y_b|\tilde{\psi}_i\rangle = \sum_{i,j=1}^{m}|i\rangle\langle j|M^{(k)}_{i,j}((x,a),(y,b)), \end{aligned} \tag{34}$$

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. □

Lemma 3.12. *(Lemma 5.2. in [27]). Let $M^{(k)}$ be as in (21). Then, for all $i,j \in \{1,\dots,m\}, s,t \in \Sigma^{\leq k}$,*

$$|M^{(k)}_{i,j}(s,t)| \leq 1. \tag{35}$$

Lemma 3.13. (Banach–Alaoglu theorem for separable spaces [28]). *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 $\mu \in X^*$: $\lim_{k\to\infty}\mu_{n_k} = \mu$.*

Theorem 3.14. *The following holds*

$$\lim_{k\to\infty}\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) = \omega_{comm}(\mathcal{G}_{\mathcal{C},\eta}). \tag{36}$$

In summary, for a given game $\mathcal{G}_{\eta,C}$, Lemma 3.11 shows us that computing the SDP (27) will provide an upper bound to the value $\omega_Q(\mathcal{G}_{\eta,C})$. Moreover, Theorem 3.14 tells us that the upper bounds will actually converge to the optimal value of $\omega_{comm}(\mathcal{G}_{\eta,C})$.

Proof. From Lemma 3.11 we have a non-increasing sequence $\{\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta})\}$ that for every k, $\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta}) \geq \omega_{comm}(\mathcal{G}_{\mathcal{C},\eta})$. We will first show the convergence of $\omega^{(k)}_{admiss}(\mathcal{G}_{\mathcal{C},\eta})$, and finally that it converges to $\omega_{comm}(\mathcal{G}_{\mathcal{C},\eta})$.

By Lemma 3.12, we have that $|M_{i,j}^{(k)}(s,t)| \leq 1$ $\forall i,j \in \{1,\dots,m\}, s,t \in \Sigma^{\leq k}$. By the Banach-Alaoglu theorem for separable spaces (Lemma 3.13), there exists a subsequence $\{M_{i,j}^{(k_l)}(s,t)\}_{l\in\mathbb{N}}$ and $M_{i,j}(s,t)$ such that $\lim_{l\to\infty} = M_{i,j}(s,t)$. Let

$$M = \begin{pmatrix} M_{1,1} & \cdots & M_{1,m} \\ \vdots & \ddots & \vdots \\ M_{m,1} & \cdots & M_{m,m} \end{pmatrix}, \tag{37}$$

then, by construction $M^{(k_l)} \to M$. The $M_{i,j}$ are such that

1. For every $i,j \in \{1,\dots,m\}$, there exists an admissible function $\phi_{i,j} : \Sigma^* \to \mathbb{C}$ such that for every $s,t \in \Sigma^{\leq k}$,
$$M_{i,j}^{(k)}(s,t) = \phi_{i,j}(s^R t). \tag{38}$$
2. Equation (23) holds,
3. For all $\ell \in \{1,\dots,L\}$, equations (24), and (25) hold.
4. The matrix M is positive semidefinite.

We want to see that M defines a commuting measurement strategy $S_{comm} = \{|\psi\rangle, A_a^x, B_b^y\}$. Since M is positive semidefinite, there exists vectors $|\psi_{i,s}\rangle \in \mathcal{H}$ for $i \in \{1,\dots,m\}$ and $s \in \Sigma^*$, for a separable Hilbert space $\mathcal{H}$, such that

$$M_{i,j}(s,t) = \langle \psi_{j,s}|\psi_{i,t}\rangle. \tag{39}$$

Assume $\mathcal{H}$ is spanned by $\{|\psi_{i,s}\rangle\}$, otherwise let $\mathcal{H} = \text{span}\{|\psi_{i,s}\rangle\}$.

- Consider the state
$$|\psi\rangle = \sum_{j=1}^{m} |j\rangle|\psi_{j,\varepsilon}\rangle \in \mathcal{H}_R \otimes \mathcal{H}, \tag{40}$$
which is normalized, since
$$\||\psi\rangle\|^2 = \langle\psi|\psi\rangle = \sum_{j=1}^{m}\langle j|j\rangle\langle\psi_{j,\varepsilon}|\psi_{j,\varepsilon}\rangle = \sum_{j=1}^{m}\langle\psi_{j,\varepsilon}|\psi_{j,\varepsilon}\rangle = \sum_{j=1}^{m} M_{j,j}(\varepsilon,\varepsilon) = 1, \tag{41}$$
where we used (39) and (23).
- For all $(z,c) \in \Sigma$, let Π_c^z be the projection operator onto the following space
$$\text{span}\{|\psi_{j,(z,c)s}\rangle : j \in \{1,\dots,m\}, s \in \Sigma^*\}. \tag{42}$$
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 (42) is the image of Π_c^z, which we denote by $\text{Im}(\Pi_c^z)$. For all $j \in \{1,\dots,m\}$ and $s \in \Sigma^*$,
$$\begin{aligned}\langle\psi_{j,(z,c)t}|\psi_{j,s}\rangle &= M_{i,j}((z,c)t,s) = \phi_{i,j}(t^R(z,c)s) = \phi_{i,j}(t^R(z,c)(z,c)s) \\ &= M_{i,j}((z,c)t,(z,c)s) = \langle\psi_{j,(z,c)t}|\psi_{i,(z,c)s}\rangle.\end{aligned} \tag{43}$$
By linearity, for every $|\varphi_1\rangle \in \text{Im}(\Pi_c^z)$,
$$\langle\varphi_1|\psi_{j,s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle. \tag{44}$$
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,
$$\langle\varphi_1|\psi_{j,s}\rangle = \langle\varphi_1|(\Pi_c^z + (\Pi_c^z)^\perp)\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle + \langle\varphi_1|(\Pi_c^z)^\perp|\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle, \tag{45}$$

where we used that $(\Pi_c^z)^\perp|\psi_{j,s}\rangle \in \mathrm{Im}(\Pi_c^z)^\perp$ and therefore, $\langle\varphi_1|(\Pi_c^z)^\perp|\psi_{j,s}\rangle = 0$. Using (44), we have that

$$\langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle. \tag{46}$$

Take an arbitrary $|\varphi\rangle \in \mathcal{H}$, then $|\varphi\rangle = |\varphi_1\rangle + |\varphi_1^\perp\rangle$, for $|\varphi_1\rangle \in \mathrm{Im}(\Pi_c^z)$ and $|\varphi_1^\perp\rangle \in \mathrm{Im}(\Pi_c^z)^\perp$. Then,

$$\langle\varphi|\Pi_c^z|\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle + \langle\varphi_1^\perp|\Pi_c^z|\psi_{j,s}\rangle = \langle\varphi_1|\Pi_c^z|\psi_{j,s}\rangle, \tag{47}$$

$$\langle\varphi|\psi_{j,(z,c)s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle + \langle\varphi_1^\perp|\psi_{j,(z,c)s}\rangle = \langle\varphi_1|\psi_{j,(z,c)s}\rangle, \tag{48}$$

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 (47), for all $|\varphi\rangle \in \mathcal{H}$, 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,

$$\Pi_c^z|\psi_{j,s}\rangle = |\psi_{j,(z,c)s}\rangle. \tag{49}$$

Then, for all $i,j \in \{1,\dots,m\}$, $s,t \in \Sigma^*$, for $(z,c_1),(z,c_2) \in \Sigma$ with $c_1 \neq c_2$,

$$\langle\psi_{j,t}|\Pi_{c_1}^z\Pi_{c_2}^z|\psi_{i,s}\rangle = \langle\psi_{j,(z,c_1)t}|\psi_{i,(z,c_2)s}\rangle = M_{i,j}((z,c_1)t,(z,c_2)t) = \phi_{i,j}(t^R(z,c_1)(z,c_2)s) = 0. \tag{50}$$

Therefore, we have that

$$\Pi_{c_1}^z\Pi_{c_2}^z = 0. \tag{51}$$

Moreover, for all $i,j \in \{1,\dots,m\}$, $s,t \in \Sigma^*, x \in \mathcal{X}$,

$$\sum_{a\in\mathcal{A}}\langle\psi_{i,s}|\Pi_a^x|\psi_{j,t}\rangle = \sum_{a\in\mathcal{A}}\langle\psi_{i,s}|\psi_{j,(x,a)t}\rangle = \sum_{a\in\mathcal{A}}\phi_{i,j}(s^R(x,a)t) = \phi_{i,j}(s^Rt) = \langle\psi_{i,s}|\psi_{j,t}\rangle, \tag{52}$$

and thus,

$$\sum_{a\in\mathcal{A}}\Pi_a^x = \mathbb{I}. \tag{53}$$

Analogously, one finds that for all $y \in \mathcal{Y}$,

$$\sum_{b\in\mathcal{B}}\Pi_b^y = \mathbb{I}. \tag{54}$$

For all $i,j \in \{1,\dots,m\}, s,t \in \Sigma^*, x \in \mathcal{X}, y \in \mathcal{Y}, a \in \mathcal{A}, b \in \mathcal{B}$,

$$\begin{aligned}\langle\psi_{i,s}|\Pi_a^x\Pi_b^y|\psi_{j,t}\rangle &= \langle\psi_{i,(x,a)s}|\psi_{j,(y,b)t}\rangle = \phi_{i,j}(s^R(x,a)(y,b)t) = \phi_{i,j}(s^R(y,b)(x,a)t)\\ &= \langle\psi_{i,(y,b)s}|\psi_{j,(x,a)t}\rangle = \langle\psi_{i,s}|\Pi_b^y\Pi_a^x|\psi_{j,t}\rangle,\end{aligned} \tag{55}$$

and therefore

$$[\Pi_a^x,\Pi_b^y] = 0. \tag{56}$$

Lastly, we see that, from (49),

$$M_{i,j}((x,a),(y,b)) = \langle\psi_{j,(x,a)}|\psi_{i,(y,b)}\rangle = \langle\psi_{j,\varepsilon}|A_a^xB_b^y|\psi_{i,\varepsilon}\rangle, \tag{57}$$

and, thus,

$$\begin{aligned}K(a,b\mid x,y) &= \mathrm{Tr}_{\mathcal{H}}[(\mathbb{I}_R\otimes A_a^xB_b^y)|\psi\rangle\langle\psi|] = \sum_{l,k}\langle\psi_{l,k}|(\mathbb{I}_R\otimes A_a^xB_b^y)\sum_{i,j}|i\rangle|\psi_{i,\varepsilon}\rangle\langle\psi_{j,\varepsilon}|\langle j||\psi_{l,k}\rangle\\ &= \sum_{i,j}\langle\psi_{j,\varepsilon}|A_a^xB_b^y|\psi_{i,\varepsilon}\rangle|i\rangle\langle j| = \sum_{i,j}M_{i,j}((x,a),(y,b))|i\rangle\langle j| = M((x,a),(y,b)).\end{aligned} \tag{58}$$

□

4 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 4.4. For a reader interested in applications in quantum cryptography, the games analyzed in this section will be used in Section 5 to prove security for cryptographic primitives.

4.1 Constrained BB84 monogamy-of-entanglement game

In [17], the following extended non-local game (the BB84 *monogamy-of-entanglement game)* was introduced

$$\mathcal{G}^{BB84} = \left(q(x) = \frac{1}{|\mathcal{X}|}, V = \{V^x_a = H^x|a\rangle\langle a|H^x\}_{x,a}, W = \{(x,v,a,b) \mid v = a = b\}_{x,v,a,b}\right), \quad (59)$$

with $\mathcal{X} = \mathcal{V} = \mathcal{A} = \mathcal{B} = \{0,1\}$. In this game, Alice and Bob prepare a quantum state and give a qubit to the referee, who measures it either in the computational or the Hadamard basis. The task of Alice and Bob is to guess the measurement outcome. In [17], it was shown that $\omega_Q(\mathcal{G}^{BB84}) = \cos^2\left(\frac{\pi}{8}\right)$, which is attained by the strategy $S^{BB84}_Q = \{|\phi\rangle\langle\phi|, A^x_a = \delta_{a0}, B^x_a = \delta_{a0}\}$, where $|\phi\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$.

We will consider the constrained version of $\mathcal{G}^{BB84}$ given by imposing that Alice and Bob never answer differently, i.e. imposing that their probability of answering different is 0. There are settings in quantum cryptography, for example in bit-commitment and quantum-position verification, where this constraint can be added naturally – see Section 5.1 and Section 5.3. In this case, the set of constraints C is given by: for every strategy $S_Q = \{\rho_{RAB}, A^x_a, B^y_b\}_{x,y,a,b}$,

$$\sum_{x,a,a'\neq b'} q(x)\mathrm{Tr}[(V^x_a \otimes A^x_{a'} \otimes B^x_{b'})\rho_{RAB}] = 0. \quad (60)$$

From Section 3.1, we have that

$$\omega_Q(\mathcal{G}^{BB84}_C) \leq \omega_{comm}(\mathcal{G}^{BB84}_C) \leq \omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_C). \quad (61)$$

Solving the SDP (27) to obtain the value of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_C)$, see code [20], we find

$$\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_C) = 0.8535533905 \simeq \cos^2\left(\frac{\pi}{8}\right), \quad (62)$$

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 [17] it was shown that the strategy S^{BB84}_Q, see above, gives the optimal value for $\mathcal{G}^{BB84}$. This strategy fulfills the constraints C, and therefore it is also optimal for $\mathcal{G}^{BB84}_C$.

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

$$\sum_{x,a,a'\neq b'} q(x)\mathrm{Tr}[(V^x_a \otimes A^x_{a'} \otimes B^x_{b'})\rho_{RAB}] \geq \varepsilon, \quad (63)$$

for $\varepsilon \geq 0$, thus imposing that the probability that Alice and Bob answer inconsistently is at least ε, the upper bounds obtained by $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$ for different values of $\varepsilon > 0$ are lower than $\cos^2\left(\frac{\pi}{8}\right)$, see Fig. 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 [29].

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 ($\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$) are *tight*, up to numerical precision. See the continuous black line in Fig. 2 for the values of the

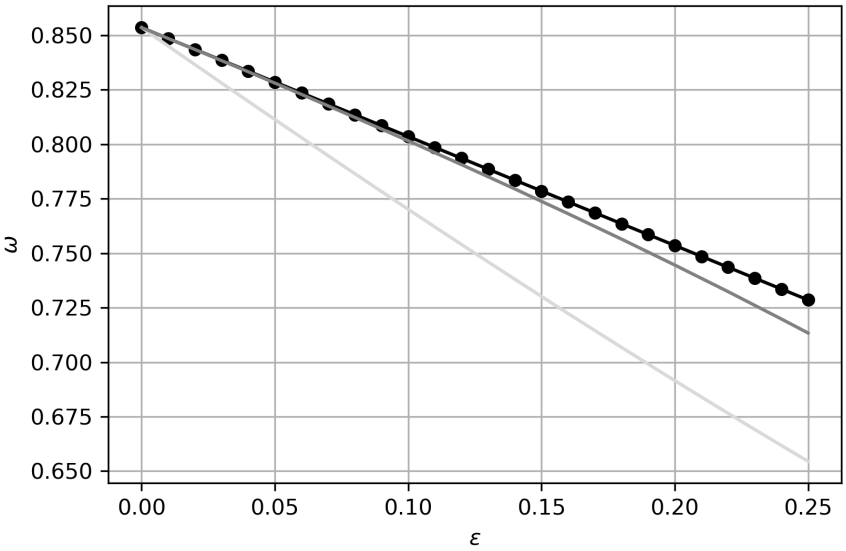


Figure 2: Values of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$ (black dots), optimal winning probability using unentangled strategies (light gray continuous line), 2-qubit state (dark gray continuous line) and 3-qubit state (black continuous line) for different values of ε.

numerical optimization, which match the values of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$ (black dots), and see [20] 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 (63) 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 (63), see [20], shows that the optimal values are significantly lower than $\omega^{(k=1)}_{admiss}(\mathcal{G}^{BB84}_{C_\varepsilon})$, see light gray line in Fig. 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 Fig. 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.

Remark 4.1. *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.*

4.2 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:

$$\mathcal{G}^{\mathrm{A}\ n\ \mathrm{guess}} := \left(q(x) = \frac{1}{|\mathcal{X}|}, V = \{V^x_a = |a^x\rangle\langle a^x|\}_{x,a}, W = \{(x,v,a,b) \mid a = v\}_{x,v,a,b}\right), \tag{64}$$

with $\mathcal{X} = \mathcal{V} = \mathcal{A} = \mathcal{B} = \{0,1\}^n$. Then,

$$\omega_Q(\mathcal{G}^{\mathrm{A}\ n\ \mathrm{guess}}) = \frac{1}{2^n}\sum_{x,a}\mathrm{Tr}\left[\left(V^x_v \otimes A^x_a \otimes (\sum_b B^x_b)\right)\rho_{RAB}\right] = \frac{1}{2^n}\sum_{x,a}\mathrm{Tr}[(V^x_v \otimes A^x_a \otimes \mathbb{I})\rho_{RAB}]. \tag{65}$$

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:

$$\omega_Q(\mathcal{G}^{\mathrm{A}\ n\ \mathrm{guess}}) = 1. \tag{66}$$

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 will be motivated by device-independent QKD, see Section 5.2. In such a case, the set of constraints $C_{p_{err}}$ is described as: for every strategy $S_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$,

$$\sum_{x,a} q(x)\mathrm{Tr}[(V_v^x \otimes A_a^x \otimes B_b^x)\rho_{RAB}] \leq p_{err}^{d_H(v,b)} \qquad \forall v, b. \tag{67}$$

In order to find an upper bound on the winning probability, we find the values of $\omega_{admiss}^{(k=1)}(\mathcal{G}_C^{\mathrm{A}\ n\ \mathrm{guess}})$ for $n = 1, 2$ computing the corresponding SDPs, see Fig. 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 $n = 1$ and $n = 2$, respectively, which can be obtained by the strategy where Alice and Bob send $|\Phi^+\rangle_{RB}^{\otimes n}$, Bob measures V_b^x and Alice and makes the random guess $a = 0\ldots0$, which will be correct with probability $\frac{1}{2^n}$. On the other hand, if $p_{err} \geq \frac{1}{2}$, Bob can answer randomly and Alice can share $|\Phi^+\rangle_{RA}^{\otimes n}$ with the referee and perform the same measurement, in which case Alice's outcomes will be perfectly correlated with the referee's outcomes.

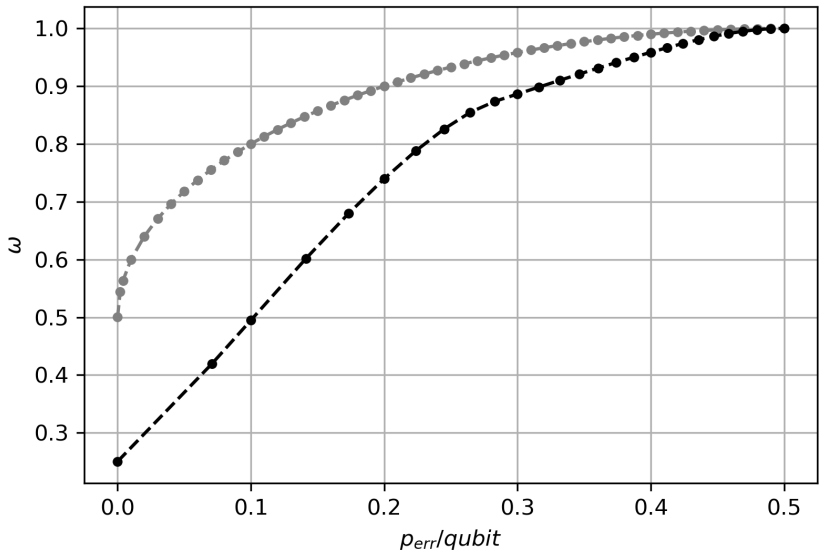


Figure 3: Upper bounds for $\omega_Q(\mathcal{G}_{C_{p_{err}}}^{\mathrm{A}\ n\ \mathrm{guess}})$ obtained from solving the SDP giving the value of $\omega_{admiss}^{(k=1)}(\mathcal{G}_C^{\mathrm{A}\ n\ \mathrm{guess}})$ for $n = 1$ (in grey) and $n = 2$ (in black).

4.3 Local guessing game

Let $n \in \mathbb{N}$, and consider the extended non-local game where Alice and Bob receive input $x \in \{0, 1\}$ and the referee chooses $z \in \{0, 1\}^n$, all uniformly at random. The referee's measurements (on a system of n qubits) are $V_v^z = |v_0^{z_0}\rangle\langle v_0^{z_0}| \otimes \ldots \otimes |v_{n-1}^{z_{n-1}}\rangle\langle v_{n-1}^{z_{n-1}}|$, for $v \in \{0, 1\}^n$. Alice and Bob have to answer $a, b \in \{0, 1\}^n$, 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

$\mathcal{G}^{n-\text{local guessing}}$, and, in the above notation,

$$\mathcal{G}^{n-\text{local guessing}} := \left(q(z,x,y) = \frac{\delta_{x,y}}{2}\frac{1}{2^n}, V = \{V_v^z\}_{z,v}, W = \{(z,x,v,a,b) \mid a = b \text{ and } \forall i \text{ s.t. } z_i = x, a_i = v_i\}\right). \tag{68}$$

Proposition 4.2. *The optimal average winning probability of $\mathcal{G}^{n-\text{local guessing}}$ for $n = 1$ is given by*

$$\omega_Q(\mathcal{G}^{1-\text{local guessing}}) = \frac{1+\cos^2\left(\frac{\pi}{8}\right)}{2}. \tag{69}$$

Moreover, this value is attained by the strategy $S_Q^{BB84} = \{|\phi\rangle\langle\phi|, A_a^x = \delta_{a0}, B_a^x = \delta_{a0}\}$, where $|\phi\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$.

Proof. The strategy $S_Q^{BB84} = \{|\phi\rangle\langle\phi|, A_a^x = \delta_{a0}, B_a^x = \delta_{a0}\}$ 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 $\mathcal{S} = \{\rho_{RAB}, A_a^x, B_b^x\}$, then

$$\begin{aligned}
\omega_Q(\mathcal{G}^{1-\text{local guessing}})\big|_{\mathcal{S}} &= \frac{1}{2^2}\sum_{(z,x,v,a,b)\in W} \mathrm{Tr}[(V_v^z \otimes A_a^x \otimes B_b^x)\rho_{RAB}] \\
&= \frac{1}{2^2}\sum_{x,v,a} \mathrm{Tr}\big[(V_v^x \otimes A_a^{1-x} \otimes B_a^{1-x})\rho_{RAB}\big] + \frac{1}{2^2}\sum_{x,a} \mathrm{Tr}[(V_a^x \otimes A_a^x \otimes B_a^x)\rho_{RAB}] \\
&= \frac{1}{2^2}\sum_{x,v} \mathrm{Tr}\left[\big(V_v^x \otimes (\sum_a A_a^{1-x} \otimes B_a^{1-x})\big)\rho_{RAB}\right] + \frac{1}{2^2}\sum_{x,a} \mathrm{Tr}[(V_a^x \otimes A_a^x \otimes B_a^x)\rho_{RAB}] \\
&\leq \frac{1}{2^2}\mathrm{Tr}\left[\left(\sum_{x,v} V_v^x\right)\rho_{RAB}\right] + \frac{1}{2}\omega(\mathcal{G}^{BB84}) = \frac{1}{2^2}\mathrm{Tr}[2\rho_{RAB}] + \frac{1}{2}\omega(\mathcal{G}^{BB84}) = \frac{1+\cos^2\left(\frac{\pi}{8}\right)}{2},
\end{aligned} \tag{70}$$

where we split the first sum in $x = z$ and $x \neq z$, then we used $\sum_a A_a^{1-x} \otimes B_a^{1-x} \preceq \mathbb{I}$ 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 n-fold parallel repetition of the strategy $\mathcal{S}_Q^{BB84}$, denoted by $(\mathcal{S}_Q^{BB84})^{\times n}$ does not provide the optimal value for $\mathcal{G}^{n-\text{local guessing}}$ for all n. To see this, notice that on the one hand, this strategy has average winning probability

$$\omega(\mathcal{G}^{n-\text{local guessing}})\big|_{(S_Q^{BB84})^{\times n}} = \left(\frac{1}{4}\left(3 + \frac{1}{\sqrt{2}}\right)\right)^n. \tag{71}$$

On the other hand, consider the strategy $\mathcal{S}_{n-0} = \{|0\rangle^{\otimes n}, A_a^x = \delta_{a,0\ldots0}, B_b^y = \delta_{b,0\ldots0}\}$. This strategy is such that

$$\omega(\mathcal{G}^{n-\text{local guessing}})\big|_{\mathcal{S}_{n-0}} = \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^n. \tag{72}$$

To see this, let $\mathcal{T}_{xz} := \{i \mid z_i = x\}$, 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,

$$\begin{aligned}
\omega(\mathcal{G}^{n-\text{local guessing}})\big|_{\mathcal{S}_{n-0}} &= \frac{1}{2^{n+1}} \sum_{(z,x,v,a,b)\in W} \mathrm{Tr}\big[(|0\rangle\langle 0|)^{\otimes n}|v^z\rangle\langle v^z|\delta_{a,0}\big] \\
&= \frac{1}{2^{n+1}} \sum_{z,x} \mathrm{Tr}\left[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}| \otimes |0_{\mathcal{T}^c_{xz}}\rangle\langle 0_{\mathcal{T}^c_{xz}}|)(|0^{x\ldots x}_{\mathcal{T}_{xz}}\rangle\langle 0^{x\ldots x}_{\mathcal{T}_{xz}}| \otimes \sum_{v\in\mathcal{T}^c_{xz}} |v^{1-x\ldots 1-x}_{\mathcal{T}^c_{xz}}\rangle\langle v^{1-x\ldots 1-x}_{\mathcal{T}^c_{xz}}|)\right] \\
&= \frac{1}{2^{n+1}} \sum_{z,x} \mathrm{Tr}\big[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0^{x\ldots x}_{\mathcal{T}_{xz}}\rangle\langle 0^{x\ldots x}_{\mathcal{T}_{xz}}| \otimes |0_{\mathcal{T}^c_{xz}}\rangle\langle 0_{\mathcal{T}^c_{xz}}|\mathbb{I}\big] \\
&= \frac{1}{2^{n+1}} \left(\sum_{z,x-0} \mathrm{Tr}[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|] + \sum_{z,x=1} \mathrm{Tr}\big[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0^{1\ldots 1}_{\mathcal{T}_{xz}}\rangle\langle 0^{1\ldots 1}_{\mathcal{T}_{xz}}|\big] \right) \\
&= \frac{1}{2^{n+1}} \left(\sum_{z} 1 + \sum_{t=0}^{n} \binom{n}{t} 2^{-t} \right) = \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^n,
\end{aligned} \tag{73}$$

where we used that $\mathrm{Tr}\big[(|0_{\mathcal{T}_{xz}}\rangle\langle 0_{\mathcal{T}_{xz}}|0^{1\ldots 1}_{\mathcal{T}_{xz}}\rangle\langle 0^{1\ldots 1}_{\mathcal{T}_{xz}}|\big] = |\langle 0_{\mathcal{T}_{xz}}|0^{1\ldots 1}_{\mathcal{T}_{xz}}\rangle| = 2^{-t}$. Similarly, one can see (71).

We see that for $n \geq 8$, the strategy $\mathcal{S}_{n-0}$ outperforms $(\mathcal{S}_Q^{BB84})^{\times n}$. Not only this, but the strategy $(\mathcal{S}_Q^{BB84})^{\times n}$ decays exponentially in n, whereas $\mathcal{S}_{n-0}$ has an average winning value of at least $\frac{1}{2}$. Therefore, we can conclude that

$$\omega_Q(\mathcal{G}^{n-\text{local guessing}}) \geq \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^n. \tag{74}$$

In [24] an upper bound was shown that can be directly transformed in an upper bound for $\mathcal{G}^{n-\text{local guessing}}$, which we state in the below proposition:

Proposition 4.3. *For every $n \in \mathbb{N}$, the following bound holds*

$$\omega_Q(\mathcal{G}^{n-\textit{local guessing}}) \leq \frac{1}{2} + \frac{1}{2}\left(\frac{1+1/\sqrt{2}}{2}\right)^n. \tag{75}$$

The proof in [24] is based on similar techniques as in the proof of Theorem 3. in [17]. For completeness, we show the proof in terms of extended non-local games in the Appendix.

In order to verify tightness of (75), we compute the SDPs providing the values of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{n-\text{local guessing}})$ for $n = 1, 2, 3, 4, 5$, see Fig. 4. We see that using SDPs, we obtain tighter upper bounds for the above mentioned values of n.

4.4 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 $S_Q = \{\rho_{RAB}, A^x_a, B^y_b\}_{x,y,a,b}$,

$$\sum_{x,a,a'\neq b'} q(x)\mathrm{Tr}[(V^x_a \otimes A^x_{a'} \otimes B^x_{b'})\rho_{RAB}] = 0. \tag{76}$$

In [19] tight results for the optimal winning probability of this lossy-and-constrained game were found by an *ad hoc* method combining the '$1 + AB$' level of the NPA hierarchy [13] with extra linear constraints derived from bounding operator norms. We show that solving the SDP (27) for $k =$ '$1+AB'$ for $\mathcal{G}^{BB84}_{C,\eta}$, see code [20], it confirms the results in [19], showing that the optimal value is achieved by the strategy given by the convex combination of S_Q^{BB84} and $S_Q^{guess} = \{|0\rangle\langle 0|, A^0_a = \delta_{a0}, A^1_a = \delta_{a\perp}, B^0_a = \delta_{a0}, B^1_a = \delta_{a\perp}\}$, which is the strategy where Alice and Bob make the guess

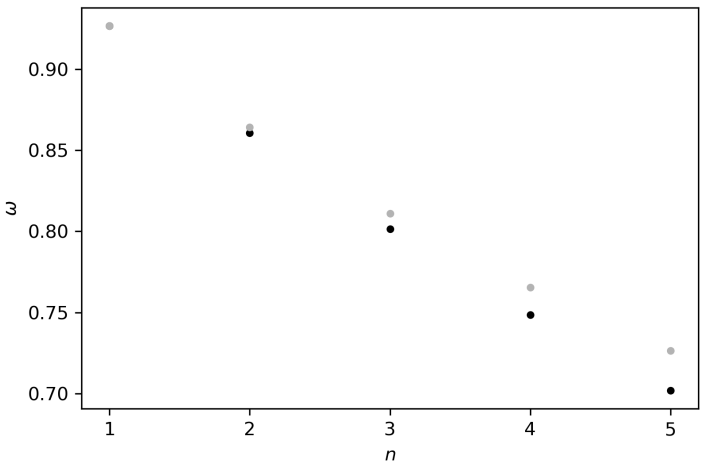


Figure 4: Upper bounds in Proposition 4.3, given by (75), (gray dots) and upper bounds obtained by $\omega^{(k=1)}_{admiss}(\mathcal{G}^{n-\text{local guessing}})$ (black dots).

$x = 0$ for the referee's measurement, and they answer 0 if the guess was right, and they answer $\perp$ if their guess was wrong. See Fig. 5 for a plot of the results. We see that level 1, $\omega^{(k=1)}_{admiss}$, provides a good approximation, whereas level 1 in [19] 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 $\omega^{(k)}_{admiss}$ will converge to the true value, whereas it was not necessarily the case in the *ad hoc* method in [19]. This becomes more clear in the following case.

Consider the extended non-local game $\mathcal{G}^{3-bases}$ described by

$$\mathcal{G}^{3-bases} := \left(q(x) = \frac{1}{|\mathcal{X}|}, V = \{V^x_a = |a_x\rangle\langle a_x|\}_{x,a}, W = \{(x,v,a,b) \mid v = a = b\}_{x,v,a,b}\right), \tag{77}$$

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, $\mathcal{G}^{3-bases}_{C,\eta}$, where C is given by forbidding different answers from Alice and Bob, was analyzed in [19] with the *ad hoc* method providing upper bounds on $\omega_Q(\mathcal{G}^{3-bases}_{\eta})$ for $\forall \eta \in [0,1]$. Nevertheless, it was open if those were tight. Here we show that solving the SDPs for $\omega^{k}_{admiss}(\mathcal{G}^{3-bases}_{C,\eta})$ gives better upper bounds, see Fig. 6. In addition, we will see that they are tight. Moreover, we computed the values for $\omega^{k=1}_{admiss}(\mathcal{G}^{3-bases}_{\eta})$, 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 lead us to think of strategies that always coordinate the answers of Alice and Bob, consisting on preparing a concrete qubit and pre-agreeding a fix answer regardless the question they receive.

Consider the strategies

$$S^{3-guess}_Q = \{|0\rangle\langle 0|, A^0_a = \delta_{a0}, A^1_a = A^2_a = \delta_{a\perp}, B^0_a = \delta_{a0}, B^1_a = B^2_a = \delta_{a\perp}\}, \tag{78}$$

which consists on guessing $x = 0$ and answering $\perp$ (photon loss) if the guess was wrong,

$$S^{3-BB84}_Q = \{|\phi\rangle\langle\phi|, A^0_a = A^1_a = \delta_{a0}, A^2_a = \delta_{a\perp}, B^0_a = B^1_a = \delta_{a0}, B^2_a = \delta_{a\perp}\}, \tag{79}$$

consisting on using S^{BB84}_Q if $x \in \{0,1\}$ and claiming photon loss if $x = 2$, and

$$S^{3-bases}_Q = \{|\phi_3\rangle\langle\phi_3|, A^x_a = \delta_{a0}, B^x_a = \delta_{a0}\}, \tag{80}$$

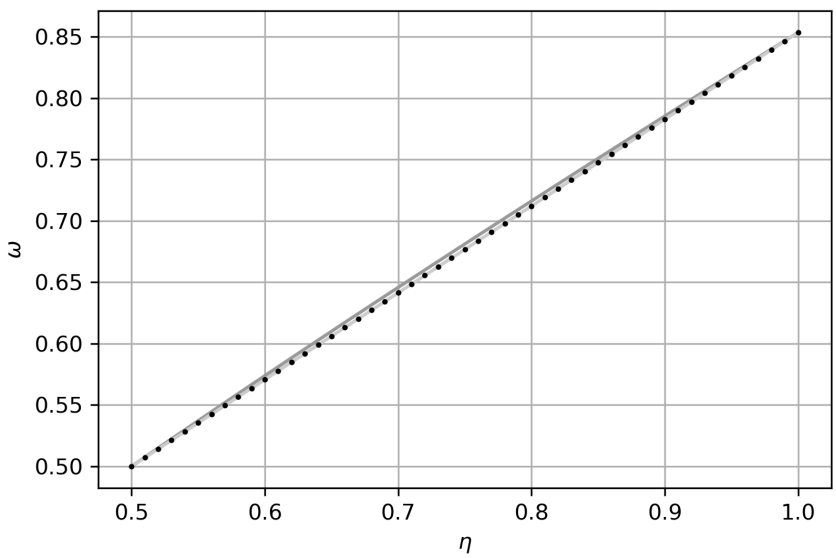


Figure 5: Solutions of $\omega_{admiss}^{(k=1)}(\mathcal{G}_{C,\eta}^{BB84})$ and $\omega_{admiss}^{(k=`1+AB')}(\mathcal{G}_{C,\eta}^{BB84})$, represented by dark grey continuous line and black dots, respectively, together with the winning probability of the strategy given by the convex combination of the strategies S_Q^{BB84} and S_Q^{guess}, represented by a light grey continuous line.

where $|\phi_3\rangle = \cos\left(\frac{\tan^{-1}(\sqrt{2})}{2}\right)|0\rangle + e^{i\frac{\pi}{4}}\sin\left(\frac{\tan^{-1}(\sqrt{2})}{2}\right)|1\rangle$. Notice that $|\phi_3\rangle$ is the state that has simultaneous maximum overlap with $|0\rangle, |+\rangle$ and $|i\rangle$, i.e.

$$\max_{|\varphi\rangle}\left\{|\langle 0|\varphi\rangle|^2 + |\langle +|\varphi\rangle|^2 + |\langle i|\varphi\rangle|^2\right\} = |\langle 0|\phi_3\rangle|^2 + |\langle +|\phi_3\rangle|^2 + |\langle i|\phi_3\rangle|^2. \tag{81}$$

Result 4.4. *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

$$\omega_Q(\mathcal{G}_\eta^{3-bases}) = \begin{cases} \frac{1}{3} + \frac{1}{\sqrt{2}}(\eta - \frac{1}{3}) \text{ if } \eta \in [\frac{1}{3}, \frac{2}{3}), \\ \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}}\right) + \frac{1-\sqrt{2}+\sqrt{3}}{2}\eta \text{ if } \eta \in [\frac{2}{3}, 1]. \end{cases} \tag{82}$$

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 Fig. 6.

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:

Observation 4.5. *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.*

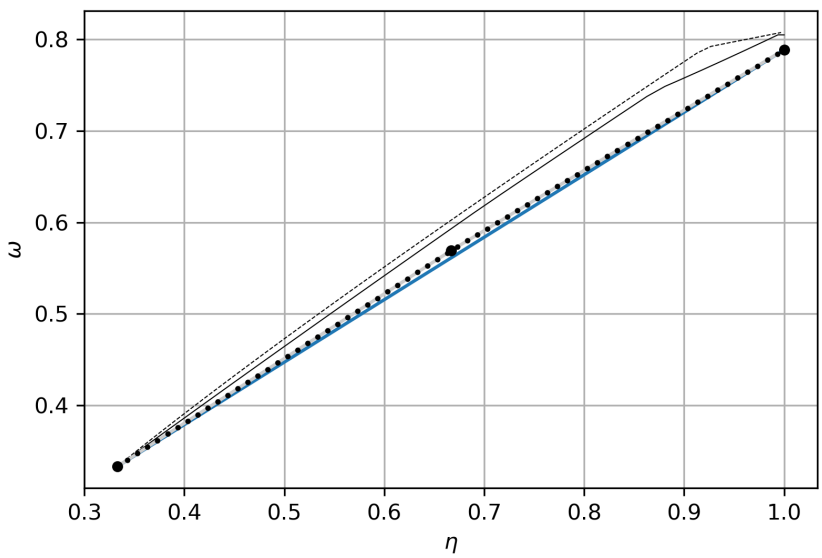


Figure 6: The dotted and continuous lines correspond to the upper bounds obtained in [19] with the *ad hoc* method using the 1st and 2nd levels of the NPA hierarchy, respectively. The black dots correspond to the values of $\omega^{(k)}_{admiss}(\mathcal{G}^{3-bases}_{\eta})$, where $k =$ '$1 + AB'$ 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 $\mathcal{S}^{3\eta}_{Q}$, the blue line corresponds to the winning value of the strategy given by the convex combination of $S^{3-guess}_{Q}$ and $S^{3-bases}_{Q}$, and the big black dots correspond to the winning probabilities of the strategies $S^{3-guess}_{Q}$, S^{3-BB84}_{Q} and $S^{3-bases}_{Q}$, respectively.

5 Applications to quantum cryptography

5.1 Application to relativistic Bit Commitment (with loss)

Bit commitment (BC) is a cryptographic two-party primitive where a party Charlie commits to a bit $x \in \{0, 1\}$ relative to another party R in a way that is both binding, in the sense that Charlie can not change the value of x afterward, and hiding, in the sense that R cannot know the value of x before Charlie unveils it. The standard description of bit commitment protocols consist of the following phases: commit (Charlie commits to x), wait (no information is shared between parties), and open (Charlie unveils x to R). In [30, 31] the impossibility of unconditional security of bit commitment was shown, even for protocols constructed using quantum information.

In [21], Kent introduced a BC protocol, which we denote by BC^{n-BB84}, in which Charlie is forced by the spacetime constraints in a Minkowski spacetime to commit x at a given spacetime point. Unconditional security in the asymptotic limit (in n, see below) was proven in [23], with tighter results for every n in [24]. In this section, we show that security of this protocol can be reduced to an extended non-local game and, by computing upper bounds as in Section 3.1, we find tighter results (for small values of n). We show security for small instances of n when loss is taken into consideration.

The BC^{n-BB84} protocol is described as follows: let (s, t) be a set of coordinates for $(1 + 1)$-dimensional Minkowski spacetime and consider the points $P = (0, 0)$, $Q_0 = (-1, 1)$ and $Q_1 = (1, 1)$. Notice no information sent from $P_t = (0, t)$ for $t > 0$ can reach both Q_0 and Q_1. The referee R prepares the state $|\psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$, where $|\psi_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ are BB84 states, and sends $|\psi\rangle$ to Charlie, who, at P, commits the bit x by measuring each qubit he received in basis $x \in \{0, 1\}$, obtaining $b \in \{0, 1\}^n$. Charlie sends x, b to two agents, Alice and Bob, who unveil x (and b) at Q_0 and Q_1, respectively. The referee checks if both x, b from Q_0 and Q_1 are the same and are consistent with the states he prepared.

Security for dishonest referee and honest Charlie follows from the fact that the referee cannot learn anything about x by no-signalling.

In order to study security for honest referee and dishonest Charlie (and his agents), we introduce a purified version of BC^{n-BB84}, in a similar way as in [23], described as follows:

1. R prepares n EPR pairs $\otimes_{i=1}^{n}|\Phi^+\rangle_{R_iC_i}$ and sends one half of each pair to Charlie (C), i.e. registers $C_1 \dots C_n$ and keeps the other halves (registers $R_1 \dots R_n$).

2. Charlie (C) commits to a bit x by measuring the qubits he received in basis $x \in \{0,1\}$, obtaining $b \in \{0,1\}^n$ (committing phase), and broadcasts x and b to two non-communicating agents Alice (A) and Bob (B).

3. Alice and Bob send x and b to R (opening phase).

4. R picks a uniformly random bit string $z \in \{0,1\}^n$ and measures the qubit in register R_i in the basis z_i for all $i \in [n]$, obtaining $r \in \{0,1\}^n$.

5. R checks if

   - he received the same x and b from Alice and Bob,
   - for all i such that $z_i = x$, it should hold that $r_i = b_i$. We will denote (x, z, r, b) such that the above hold as W, the *winning set*.

   If the checks pass, the opening is accepted.

The only difference with the purification of BC^{n-BB84} in [23] is that, in our case, the referee measures each qubit in a uniformly random basis $z_i \in \{0,1\}$ instead of measuring half of the n qubits in the computational basis and the other half in the Hadamard basis. Our purification corresponds to Kent's protocol [21], since all the BB84 states are in a uniformly random basis, instead of half in computational and half in Hadamard as in the variation in [23].

The average probability of accepting the commitment is given by

$$\omega_{accept} = \frac{1}{2}(p_0 + p_1), \tag{83}$$

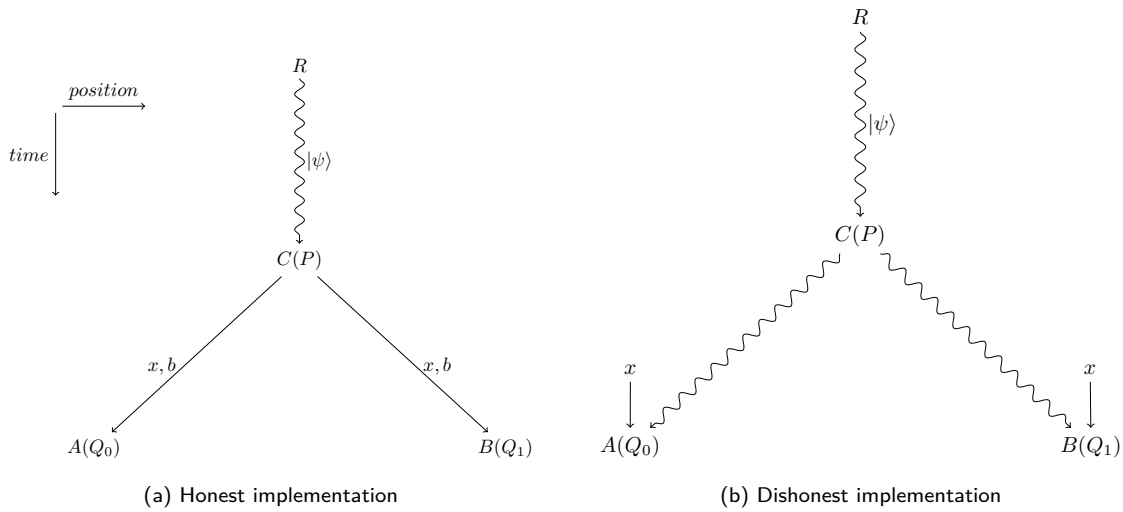
where p_0 and p_1 denote the probability of accepting the commitment $x = 0$ and $x = 1$, respectively. For an honest (and perfect) implementation of the protocol,

$$p_x = \frac{1}{2^n} \sum_{(x,z,r,b)\in W} \mathrm{Tr}\Big[(V_{r_0}^{z_0} \otimes \cdots \otimes V_{r_{n-1}}^{z_{n-1}}) \otimes (V_{b_0}^{x} \otimes \cdots \otimes V_{b_{n-1}}^{x})(|\Phi^+\rangle\langle\Phi^+|)^{\otimes n}\Big], \text{ for } x \in \{0,1\}, \tag{84}$$

where $V_a^y = H^y|a\rangle\langle a|H^y$ for $a, y \in \{0,1\}$. Then, the average probability of accepting is

$$\omega_{accept}^{honest} = \frac{1}{2}\sum_x p_x = 1. \tag{85}$$

See Fig. 7 (a) for a schematic representation of BC^{n-BB84}. In Fig. 7, we place R in the same location as B' in the past, but R can be anywhere in the past of C.



(a) Honest implementation (b) Dishonest implementation

Figure 7: Scheme of an honest (a) and dishonest (committer) implementation (b) of the $\mathrm{BC}^{n\text{-}BB84}$ protocol.

When transmitting the quantum information from R to C, for example, by sending it through a quantum channel connecting R to C, or by R 'delivering' it to C such that C has to keep it in a quantum memory till the committing phase, a certain fraction of qubits might be lost. Let η denote the transmission rate per qubit, then with probability $1-\eta$, in the commitment phase Charlie will obtain $b_i = \perp$ for all $i \in [n]$. We introduce $\mathrm{BC}_\eta^{n-BB84}$ as the lossy version of BC^{n-BB84} with transmission rate per qubit η, where the difference is that $b \in \{0,1,\perp\}^n$ and the check that R performs consists of

- verifying that he received the same x and b from Alice and Bob,
- verifying consistency with the measurement outcomes, i.e.

$$\text{for all } i \text{ such that } z_i = x, \text{ and } b_i \neq \perp,\ r_i = b_i, \tag{86}$$

- verifying consistency with the transmission rate, i.e.

$$|\{i \mid b_i \neq \perp\}| \in [n\eta - \sigma_\eta, n\eta + \sigma_\eta], \tag{87}$$

  for a certain $\sigma_\eta > 0$.

If the checks pass, the opening is accepted. The set of tuples (x, z, r, b) that pass the test (winning set) is given by

$$W_\eta = \{(x,z,r,b) \in \{0,1\} \times \{0,1\}^n \times \{0,1\}^n \times \{0,1,\perp\}^n \mid \text{ eqs. (86) and (87) hold.}\}, \tag{88}$$

i.e., if the answers she received are such that $(x, z, r, b) \in W_\eta$, the bit x is accepted.

For an honest execution of the protocol, we consider the lossy channel that acts on each qubit by leaving it invariant with probability η, and losing it with probability $1-\eta$. The honest average winning probability can be expressed as

$$\omega_{accept}^{honest} = \frac{1}{2}\frac{1}{2^n} \sum_{(x,z,r,b)\in W_\eta} \mathrm{Tr}\big[(V_r^z \otimes M_b^x)(|\Phi^+\rangle\langle\Phi^+|)^{\otimes n}\big], \tag{89}$$

where $M_b^x = M_{b_0}^x \otimes \cdots \otimes M_{b_{n-1}}^x$, for

$$M_{b_i}^x = \begin{cases} \eta H^x |b_i\rangle\langle b_i| H^x & \text{if } b \in \{0,1\}, \\ (1-\eta)\mathbb{I}_2 & \text{if } b = \perp\,. \end{cases} \quad \forall i \in [n], \tag{90}$$

i.e. in each qubit Charlie either performs the same measurement as the referee with probability η, or the photon is lost with probability $1-\eta$. For n large enough, by the central limit theorem, the

commitment will be accepted with probability arbitrarily close to 1 (with the value determined by σ_η).

Moreover, in an experimental implementation, an honest Charlie will have a certain error. Let ε be the error per qubit that he is assumed to have. Then, taking this into account, we introduce the loss-and-error version of BC^{n-BB84} as $\mathrm{BC}_\eta^{n-BB84}$ where the check that R performs consists of the same check as in the lossy version and, in addition, she verifies the consistency with the error, i.e.,

$$\varepsilon - \sigma_\varepsilon \leq \frac{|\{i \mid z_i = x \text{ and } b_i \neq \perp \text{ and } b_i \neq r_i\}|}{|\{i \mid z_i = x \text{ and } b_i \neq \perp\}|} \leq \varepsilon + \sigma_\varepsilon, \tag{91}$$

for a certain $\sigma_\varepsilon > 0$.

5.1.1 Security for dishonest Charlie

We analyze security in the *global command model* [23], where an external agent dictates the bit that should be unveiled to Alice and Bob at latest at $t = 1$. The most general thing a dishonest Charlie can do is, during the commit phase, to apply an arbitrary completely positive trace-preserving (CPTP) map to his halves of EPR pairs and possibly some ancillary qubits and send a register to Alice and another register to Bob. Then, upon receiving the bit x dictated by an external agent, Alice and Bob perform POVMs $\{A_a^x\}$ and $\{B_b^x\}$ to answer x, a and x, b, respectively.

Security of $\mathrm{BC}_\eta^{n-BB84}$ can be reduced to the winning probability of the extended non-local game 'Local guessing game' $\mathcal{G}^{n-\text{local guessing}}$, described in Section 4.3, where the referee, Alice and Bob share a tripartite state ρ_{RAB}, and Alice and Bob answer x, a and x, b such that $a = b$. Upon the choice of measurement $z \in \{0,1\}^n$ with outcome $r \in \{0,1\}^n$, they win the game if the tuple $(x, z, r, b) \in W_\eta$. The optimal winning probability is given by

$$\omega_Q = \sup \frac{1}{2}\frac{1}{2^n} \sum_{(x,z,r,b)\in W_\eta} \mathrm{Tr}[(V_r^z \otimes A_b^x \otimes B_b^x)\rho_{RAB}] = \frac{1}{2}(p_0^{attack} + p_1^{attack}) =: \omega_{accept}^{attack}, \tag{92}$$

where $V_r^z = |r_0^{z_0}\rangle\langle r_0^{z_0}| \otimes \cdots \otimes |r_{n-1}^{z_{n-1}}\rangle\langle r_{n-1}^{z_{n-1}}|$, and $p_x^{attack} = \frac{1}{2^n}\sum_{(x,z,r,b)\in W} \mathrm{Tr}[(V_r^z \otimes A_b^x \otimes B_b^x)\rho_{RAB}]$ denotes the probability that R accepts the commit x (sent by the attackers).

Notice that a dishonest implementation of the protocol will always have average winning probability of at least $\frac{1}{2}$, since a dishonest Charlie can pick x, measure all the qubits he received at P in basis x (as in an honest implementation) and broadcast the outcome to Alice and Bob. If the external agent picks the same value x, the commitment will be accepted, thus,

$$\omega_{accept}^{attack} = \frac{1}{2} + \xi, \tag{93}$$

for a certain bias $\xi \geq 0$. Phrasing the attack in terms of an extended non-local game, the strategy $\mathcal{S}_{n-0} = \{|0\rangle^{\otimes n}, A_a^x = \delta_{a,0\ldots0}, B_b^y = \delta_{b,0\ldots0}\}$ introduced in Section 4.3 is such that

$$\omega_{accept}^{attack}\big|_{\mathcal{S}_{n-0}} = \frac{1}{2}(p_{x_0}^{attack} + p_{1-x_0}^{attack}) = \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^n. \tag{94}$$

Therefore, we have that

$$\omega_{accept}^{attack} \geq \frac{1}{2} + \frac{1}{2}\left(\frac{3}{4}\right)^n. \tag{95}$$

In [23], security was shown with

$$\omega_{accept}^{attack} \leq \frac{1}{2} + \inf_{\delta\in(0,\frac{1}{2})} 2^{-n(1-h(\delta))} + e^{-\frac{1}{2}n\delta^2}, \tag{96}$$

which decays exponentially for $n \to \infty$. This result was tightened in [24], showing that, from Proposition 4.3,

$$\omega_{accept}^{attack} \leq \frac{1}{2} + \frac{1}{2}\left(\frac{1 + 1/\sqrt{2}}{2}\right)^n. \tag{97}$$

We analyze security for small values of n by computing upper bounds of (92) solving the SDP that gives us the upper bound $\omega^{(1)}_{admiss}$ for fixed values of n, see code [20].

For the lossless and error-free case, we have the bounds plotted in Fig. 4, where we find tighter bounds than in [24] for small values of n.

Now, for small n, we consider the scenario where a certain number of photon loss answers are accepted. Since the acceptance criterion will be based on a few qubits, we only consider the error-free case. We analyze the following cases:

(i) $n = 1$. The referee has to either accept or reject the commitment based on a single bit. In such a case, we consider the error-free case where only non no-photon answers are accepted, i.e. $W = \{(x, z, r, b) \mid \text{ if } z = x, \text{ then } r = b \neq \perp\}$. Then,

$$\omega_{Charlie} = \eta \qquad \text{and} \qquad \omega^{(1)}_{admiss} = 0.926776695 \simeq \frac{1 + \cos^2 \frac{\pi}{8}}{2}. \tag{98}$$

From Section 4.3, we know that the result $\omega^{(1)}_{admiss}$ is tight. In this case, an honest Charlie would pass the test with higher probability than potential attackers as long as $\eta > 0.926776695$. There is no point in considering accepting photon loss as a valid answer for $n = 1$, since the attackers can then always claim photon loss and be accepted with probability 1.

(ii) $n = 2$. The referee has to either accept or reject the commitment based on two bits. In such a case, we consider two possible winning sets W given by

- the set of two answers such that do not contain $\perp$ (no photon loss answers accepted), then
$$\omega_{Charlie} = \eta^2 \qquad \text{and} \qquad \omega^{(1)}_{admiss} = 0.8607577. \tag{99}$$
In this case, an honest Charlie would pass the test with higher probability than potential attackers as long as $\eta > 0.92777$.
- the set of two answers such that at least one is not $\perp$. In such a case, $\omega^{(1)}_{admiss} = 1.000$ provides a trivial upper bound.

(iii) $n = 3$. The referee has to either accept or reject the commitment based on three bits. In such a case, we consider two possible winning sets W given by

- the set of two answers such that do not contain $\perp$ (no photon loss answers accepted), then
$$\omega_{Charlie} = \eta^3 \qquad \text{and} \qquad \omega^{(1)}_{admiss} = 0.8014794 \tag{100}$$
In this case, an honest Charlie would pass the test with higher probability than potential attackers as long as $\eta > 0.928892$.
- the set of two answers such that at least one is not $\perp$, then
$$\omega_{Charlie} = (3 - 2\eta)\eta^2 \qquad \text{and} \qquad \omega^{(1)}_{admiss} = 0.927699 \tag{101}$$
In this case, an honest Charlie would pass the test with higher probability than potential attackers as long as $\eta > 0.835472$.

5.2 Application to device-independent quantum key distribution

In [17], security of one-sided device-independent quantum key distribution (DIQKD) BB84 [22] was proven using a monogamy-of-entanglement game. In order to reduce an attack on the protocol to a monogamy-of-entanglement game, we consider an entanglement-based variant of the original BB84 protocol, which implies security of the latter [32].

We consider a simplified version omitting information reconciliation and privacy amplification, in which two parties, a referee (usually in the literature, Alice) and Bob want to establish a secret key, tolerating a measurement error p_{err} per qubit:

- The referee prepares n EPR pairs, keeps one half and sends the other half to Bob from each EPR pair. Bob confirms he received the n qubits.
- The referee picks a random basis x_i, either computational or Hadamard, to measure each qubit, sends $x_0, \ldots, x_{n-1}$ to Bob and both measure, obtaining $a = a_0 \ldots a_{n-1}$ and $b = b_0 \ldots b_{n-1}$, respectively.

The key is successfully generated, up to information reconciliation and privacy amplification, if $d_H(a, b) \leq np_{err}$.

The security of this protocol for untrusted Bob's measurement device, which could behave maliciously, can be reduced to the monogamy-of-entanglement game where Alice's goal is to guess the value of the referee's raw key a [17], where it is proven that the protocol can tolerate a noise up to 1.5% asymptotically.

Here we consider a similar approach by first fixing the error p_{err} and then seeing what is the probability that Alice guesses x, with the condition that Bob's answers must be at a relative Hamming distance at most p_{err} from x. This security can be reduced to the constrained extended non-local game $\mathcal{G}^{\text{A } n \text{ guess}}_{C_{p_{err}}}$ described in Section 4.2.

Obtaining the values of $\omega^{(k=1)}_{admiss}(\mathcal{G}^{n-QKD}_{C})$ for $n = 1, 2$, see Fig. 3, we find nontrivial upper bounds for the winning probability $\mathcal{G}^{\text{A } n \text{ guess}}_{C_{p_{err}}}$, which translate to security for QKD. Notice that if the error per qubit is at least $\frac{1}{2}$, the eavesdropper can use the strategy consisting of sharing n EPR pairs with the referee, performing the same measurement, and manipulating Bob's device so that it answers random bits (which each are going to be correct with probability $\frac{1}{2}$), therefore, the eavesdropper's outcomes will be perfectly correlated with the referee's outcomes so that she guesses perfectly the raw key and for $p_{err} \geq \frac{1}{2}$, $\omega_Q(\mathcal{G}^{\text{A } n \text{ guess}}_{C_{p_{err}}}) = 1$, this confirms the that the results for $p_{err} \geq \frac{1}{2}$ obtained via $\omega^{(k=1)}_{admiss}(\mathcal{G}^{\text{A } n \text{ guess}}_{C_{p_{err}}})$ are tight, see Fig. 3.

In order to prove security for an arbitrary n and a given laboratory error p_{err}, one would need to solve the corresponding SDP $\omega^{(k=1)}_{admiss}(\mathcal{G}^{\text{A } n \text{ guess}}_{C_{p_{err}}})$ (or larger k). However, the downside is that larger values of n take considerably more computational resources.

5.3 Application to quantum position verification

Securely finding out a party's location (position verification) or writing messages that can only be read at a certain location are potentially-impactful tasks part of the field of *position-based cryptography* (PBC). An important building block for PBC is so-called Position Verification (PV), where, in a 1-dimensional setup, an untrusted prover P wants to convince verifiers V_0, and V_1, placed left and right of P, respectively, that she is at a certain given position. In [33] it was proven that no secure classical protocol for position verification can exist, since there exists a general attack based on copying classical information.

Due to the no-cloning theorem [34] the general classical attack does not apply if quantum information is used instead [35, 36], however, a general quantum attack exists which requires exponential entanglement [37, 38]. This means that hope for protocols secure against reasonable amounts of entanglement is alive, and indeed there has been much analysis on attacks on specific protocols [39, 35, 40, 41, 42, 43, 44, 45, 46, 47]. Also of note is recent work performing the first experiment that implements QPV in a lab setting [48].

One of the simplest and best-studied QPV protocols [39, 35] is based on BB84 states, denoted by QPV_{BB84}. The protocol consists of one verifier (V_0) sending a BB84 state $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to the prover, and the other verifier (V_1) sending classical information $x \in \{0, 1\}$ describing in which basis the prover has to measure, either the computational basis ($x = 0$) or the Hadamard basis ($x = 1$). The prover then has to broadcast the measurement outcome $a \in \{0, 1\}$ to both verifiers, with all communication happening at the speed of light.

The most general attack on any 1-dimensional QPV protocol is to place an adversary between V_0 and the prover, Alice, and another adversary between the prover and V_1, Bob, such that the adversaries intercept the messages coming from their closest verifiers, have one round of simultaneous communication, and reply to their closest verifier.

For security analysis, we will consider the purified version of QPV_{BB84}, which is equivalent to the defined version above. In the purified version, V_0, instead of sending a BB84 state, prepares

the EPR pair $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and sends one qubit to P and at some later point, V_0 measures their register in basis x. In particular, it makes it easy to delay the choice of basis x to a later point in time, which makes it clear that the attackers' actions are independent of the basis choice.

In [37] it was proven that $\mathrm{QPV}_{\mathrm{BB84}}$ is secure if the attackers do not pre-share entanglement before to intercept the information. 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 [17], it was shown that security of $\mathrm{QPV}_{\mathrm{BB84}}$ 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. Therefore, 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 $S_Q = \{\rho_{RAB}, A_a^x, B_b^y\}_{x,y,a,b}$ given by

$$\sum_{x,a,a'\neq b'} q(x)\mathrm{Tr}[(V_a^x \otimes A_{a'}^x \otimes B_{b'}^x)\rho_{RAB}] = 0. \tag{102}$$

This corresponds to the constrained $\mathcal{G}^{BB84}$ game analyzed in Section 4.1, 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.

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 $\mathrm{QPV}_{\mathrm{BB84}}$, 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 $\mathrm{QPV}_{\mathrm{BB84}}$ will be denoted by $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$. In [19] it was shown that the security of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$ could be reduced to the lossy-and-constrained extended non-local game $\mathcal{G}^{BB84}_{C,\eta}$, which we analyzed in Section 4.4, with $\omega_Q(\mathcal{G}^{BB84}_{C,\eta}) = \frac{1}{\sqrt{2}}\eta + \sin^2\left(\frac{\pi}{8}\right)$. 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

$$\eta(1-p_{err}) > \frac{1}{\sqrt{2}}\eta + \sin^2\left(\frac{\pi}{8}\right). \tag{103}$$

Since the results were tight, the above inequality provides the optimal relation with the error. We saw that using our new methodology, the results of [19] 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 4.4 in QPV not only verifies in a different way preveously known results but improves some providing tight results. Consider the extension of $\mathrm{QPV}_{\mathrm{BB84}}$ consisting on V_0 sending a uniformly random state from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ and V_1 sending in which basis to measure (Hadamard, computational or $\{|\pm i\rangle\}$), introduced in [35]. The security of this protocol can be reduced to the winning probability of the extended non-local game $\mathcal{G}^{3-bases}$, as shown in [19]. This game was analyzed in Section 4.4, 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 Result 4.4. 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 Result 4.4 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 $\eta \in [\frac{1}{3}, \frac{2}{3})$,

$$\eta(1-p_{err}) > \frac{1}{3} + \frac{1}{\sqrt{2}}(\eta - \frac{1}{3}), \tag{104}$$

(ii) if $\eta \in [\frac{2}{3}, 1]$,

$$\eta(1-p_{err}) > \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}}\right) + \frac{1-\sqrt{2}+\sqrt{3}}{2}\eta. \tag{105}$$

5.3.1 Security for 2-fold parallel repetition of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

The security of the n-fold parallel repetition of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, given that the attackers do not pre-share entanglement, can can be reduced to the n-fold parallel repetition of the lossy extended non-local game $\mathcal{G}_{\eta}^{BB84\times n}$, with $\mathcal{X} = \mathcal{Y} = \{0,1\}^n$ and $\mathcal{A} = \mathcal{B} = \{0,1,\perp\}^n$.

In this section, we analyze the case $n = 2$ and we show security for the 2-fold parallel repetition of $\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$, given that the attackers do not pre-share entanglement. Imposing the same loss rate for both qubits, i.e.,

$$\sum_{x_0x_1} q(x_0x_1)\mathrm{Tr}[(\mathbb{I}_R \otimes \mathbb{I}_R \otimes A^{x_0x_1}_{\perp\perp} B^{x_0x_1}_{\perp\perp})\rho_{RAB}] = (1-\eta)^2, \tag{106}$$

for all $a_0, a_0' \in \{0,1\}$,

$$\sum_{x_0x_1} q(x_0x_1)\mathrm{Tr}\Big[(\mathbb{I}_R \otimes \mathbb{I}_R \otimes A^{x_0x_1}_{a_0\perp} B^{x_0x_1}_{a_0'\perp})\rho_{RAB}\Big] = \frac{1}{2}\eta(1-\eta), \tag{107}$$

and for all $a_1, a_1' \in \{0,1\}$,

$$\sum_{x_0x_1} q(x_0x_1)\mathrm{Tr}\Big[(\mathbb{I}_R \otimes \mathbb{I}_R \otimes A^{x_0x_1}_{\perp a_1} B^{x_0x_1}_{\perp a_1'})\rho_{RAB}\Big] = \frac{1}{2}\eta(1-\eta), \tag{108}$$

we obtain an upper bound solving the SDP that gives the value $\omega^{(k=1)}_{admiss}(\mathcal{G}_{\eta}^{BB84\times 2})$. The obtained values, see [20] for the code, are plotted in Fig. 8, together with the winning value of the parallel repetition of the optimal strategy for $\mathcal{G}_{\eta}^{BB84}$. 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 $\omega_Q(\mathcal{G}_{\eta}^{BB84\times 2})$, for all $\eta > \frac{1}{2}$. In addition, if the 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

$$\eta^2(1-p_{err}) > \omega^{(k=1)}_{admiss}(\mathcal{G}_{\eta}^{BB84\times 2}). \tag{109}$$

Security for the n-fold parallel repetition for a given n can be computed analogously. Since our techniques do run into a practical limit when increasing n, we leave the open problem to create a more efficient program that computes the parallel repetition faster.

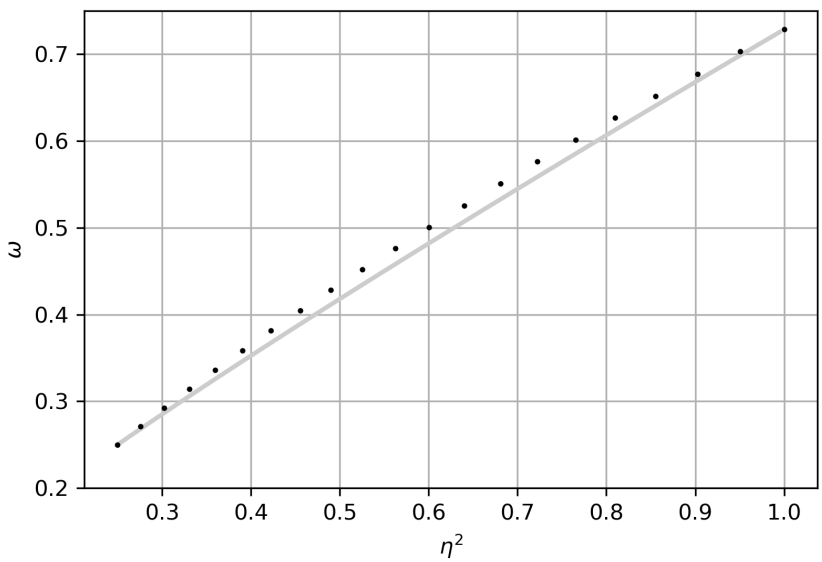


Figure 8: Values of $\omega_{admiss}^{(k=1)}(\mathcal{G}_\eta^{BB84\times 2})$ (black dots) and winning values for the parallel repetition of the optimal strategy for $\mathcal{G}_\eta^{BB84}$ (gray continuous line).

6 Discussion and open problems

We give an approach using SDP hierarchies to extend security proofs of quantum cryptographic protocols to realistic scenarios. A first natural extension of this work, could be to apply our techniques to other problems in quantum cryptography, especially when proving security of near-term experimental setups. A possible future task could be optimizing the code provided in this work, making it feasible to compute SDP solutions for larger instances of n in some of the above analyzed games. In addition, since the solutions of the solved SDPs provide tighter results than Proposition 4.3, it would be interesting to find either a tighter version of that proposition or the optimal value for all n. In our application to relativistic bit commitment, we show partial loss tolerance of the protocol without having to adjust the communication pattern. A different way to make the protocol loss tolerant could be to introduce an extra round of communication, where the committer announces immediately which qubits arrived successfully.

7 Acknowledgments

This work was supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme. We would like to thank an anonymous referee for pointing out a mistake in the SDP solutions of Section 4.1 in an earlier version of this work — thanks to their observation we were able to correct a typo in the code for the corresponding game [20], and could also find strategies that matched the bounds provided by the (correct) SDP solutions.

References

[1] J. S. Bell. "On the Einstein Podolsky Rosen paradox". Physics Physique Fizika **1**, 195–200 (1964).

[2] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. "Device-independent security of quantum cryptography against collective attacks". Physical Review Letters **98**, 230501 (2007).

[3] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. "Random numbers certified by Bell's theorem". Nature **464**, 1021–1024 (2010).

[4] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. "Nonlocality and communication complexity". Reviews of Modern Physics **82**, 665–698 (2010).

[5] Dominic Mayers and Andrew Yao. "Self testing quantum apparatus". Quantum Info. Comput. **4**, 273–286 (2004).

[6] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". Quantum **4**, 337 (2020).

[7] Janet Anders and Dan E. Browne. "Computational power of correlations". Physical Review Letters **102**, 050502 (2009).

[8] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. "Proposed experiment to test local hidden-variable theories". Phys. Rev. Lett. **23**, 880–884 (1969).

[9] Richard Cleve, Peter Hoyer, Ben Toner, and John Watrous. "Consequences and limits of nonlocal strategies" (2010). arXiv:quant-ph/0404076.

[10] Stephanie Wehner. "Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities". Physical Review A**73** (2006).

[11] Yeong-Cherng Liang and Andrew C. Doherty. "Bounds on quantum correlations in bell-inequality experiments". Phys. Rev. A **75**, 042103 (2007).

[12] Miguel Navascués, Stefano Pironio, and Antonio Acín. "Bounding the set of quantum correlations". Phys. Rev. Lett. **98**, 010401 (2007).

[13] Miguel Navascués, Stefano Pironio, and Antonio Acín. "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations". New Journal of Physics **10**, 073013 (2008).

[14] Oded Regev and Thomas Vidick. "Quantum XOR games" (2012). arXiv:1207.4939.

[15] T. Cooney, M. Junge, C. Palazuelos, and D. Pérez-García. "Rank-one quantum games" (2013). arXiv:1112.3563.

[16] 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**, 20160003 (2016).

[17] 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**, 103002 (2013).

[18] Vincent Russo and John Watrous. "Extended nonlocal games from quantum-classical games" (2017). arXiv:1709.01837.

[19] Llorenç Escolà-Farràs and Florian Speelman. "Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers". Physical Review Letters**131** (2023).

[20] Llorenç Escolà-Farràs. "`https://github.com/llorensescola/LossyAndConstrainedGames`".

[21] Adrian Kent. "Unconditionally secure bit commitment by transmitting measurement outcomes". Physical Review Letters**109** (2012).

[22] 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).

[23] Jedrzej Kaniewski, Marco Tomamichel, Esther Hanggi, and Stephanie Wehner. "Secure bit commitment from relativistic constraints". IEEE Transactions on Information Theory **59**, 4687–4699 (2013).

[24] Damián Pitalúa-García and Iordanis Kerenidis. "Practical and unconditionally secure spacetime-constrained oblivious transfer". Physical Review A**98** (2018).

[25] Monique Laurent and Franz Rendl. "Semidefinite programming and integer programming". In K. Aardal, G.L. Nemhauser, and R. Weismantel, editors, Discrete Optimization. Volume 12 of Handbooks in Operations Research and Management Science, pages 393–514. Elsevier (2005).

[26] Stephen Boyd and Lieven Vandenberghe. "Convex optimization". Cambridge University Press. (2004).

[27] Vincent Russo. "Extended nonlocal games" (2017). arXiv:1704.07375.

[28] Leon Alaoglu. "Weak topologies of normed linear spaces". Annals of Mathematics **41**, 252–267 (1940).

[29] Anne Broadbent and Eric Culf. "Rigidity for Monogamy-Of-Entanglement Games". In Yael Tauman Kalai, editor, 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.

[30] Hoi-Kwong Lo and H. F. Chau. "Is quantum bit commitment really possible?". Phys. Rev. Lett. **78**, 3410–3413 (1997).

[31] Dominic Mayers. "Unconditionally secure quantum bit commitment is impossible". Phys. Rev. Lett. **78**, 3414–3417 (1997).

[32] Charles H. Bennett, Gilles Brassard, and N. David Mermin. "Quantum cryptography without Bell's theorem". Phys. Rev. Lett. **68**, 557–559 (1992).

[33] 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).

[34] W. K. Wootters and W. H. Zurek. "A single quantum cannot be cloned". Nature **299**, 802–803 (1982).

[35] Adrian Kent, William J. Munro, and Timothy P. Spiller. "Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints". Physical Review A**84** (2011).

[36] Robert A. Malaney. "Location-dependent communications using quantum entanglement". Phys. Rev. A **81**, 042319 (2010).

[37] 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**, 150–178 (2014).

[38] Salman Beigi and Robert König. "Simplified instantaneous non-local quantum computation with applications to position-based cryptography". New Journal of Physics **13**, 093036 (2011).

[39] Adrian Kent, William Munro, Timothy Spiller, and Raymond Beausoleil. "Tagging systems. us patent nr 2006/0022832" (2006).

[40] Hoi-Kwan Lau and Hoi-Kwong Lo. "Insecurity of position-based quantum-cryptography protocols against entanglement attacks". Physical Review A**83** (2011).

[41] Jérémy Ribeiro and Frédéric Grosshans. "A tight lower bound for the BB84-states quantum-position-verification protocol" (2015).

[42] Kaushik Chakraborty and Anthony Leverrier. "Practical position-based quantum cryptography". Physical Review A**92** (2015).

[43] Florian Speelman. "Instantaneous Non-Local Computation of Low T-Depth Quantum Circuits". In Anne Broadbent, editor, 11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016). Volume 61 of Leibniz International Proceedings in Informatics (LIPIcs), pages 9:1–9:24. Dagstuhl, Germany (2016). Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[44] Kfir Dolev. "Constraining the doability of relativistic quantum tasks" (2022). arXiv:1909.05403.

[45] Kfir Dolev and Sam Cree. "Non-local computation of quantum circuits with small light cones" (2022). arXiv:2203.10106.

[46] Alvin Gonzales and Eric Chitambar. "Bounds on instantaneous nonlocal quantum computation". IEEE Transactions on Information Theory **66**, 2951–2963 (2020).

[47] Joy Cree and Alex May. "Code-routing: a new attack on position verification". Quantum **7**, 1079 (2023).

[48] 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). arXiv:2502.04125.

Appendix A Proof of Proposition 4.3

We show the proof of Proposition 4.3 [24]. For that, we need the following Definition and Lemmas.

Definition A.1. *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 $i \in [n]$.*

Lemma A.2. (Lemma 2 in [17]) *Let $\Pi^1, \ldots, \Pi^n$ be projectors acting on a Hilbert space $\mathcal{H}$. Let $\{\pi_k\}_{k\in[n]}$ be a set of mutually orthogonal permutations. Then,*

$$\left\| \sum_{i\in[n]} \Pi^i \right\| \leq \sum_{k\in[n]} \max_{i\in[n]} \left\| \Pi^i \Pi^{\pi_k(i)} \right\|. \tag{110}$$

Remark A.3. *There always exists a set of n permutations of $[n]$ that are mutually orthogonal, an example is the n cyclic shifts.*

Lemma A.4. *(Lemma 1 in [17]) Let $A, B, L \in \mathcal{B}(\mathcal{H})$ such that $AA^\dagger \succeq B^\dagger B$. Then it holds that $\|AL\| \geq \|BL\|$.*

Now, we are in position to prove Proposition 4.3, which uses similar ideas as in the proof of Theorem 3 in [17]. Let $\mathcal{S} = \{\rho_{RAB}, A_a^x, B_b^x\}$ be an arbitrary strategy. As above, let $\mathcal{T}_{xz} := \{i \mid z_i = x\}$, and 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

$$\begin{aligned}
\omega_Q(\mathcal{G}^{n-\text{local guessing}})\big|_{\mathcal{S}} &= \frac{1}{2^{n+1}} \sum_{(z,x,v,a,b)\in W} \mathrm{Tr}[(V_v^z \otimes A_a^x \otimes B_b^x)\rho_{RAB}] \\
&= \frac{1}{2^{n+1}} \sum_{z,x} \sum_{v\in\mathcal{T}_{zx}^c, a} \mathrm{Tr}\Big[\big(|a_{\mathcal{T}_{zx}}^{x\ldots x}\rangle\langle a_{\mathcal{T}_{zx}}^{x\ldots x}| \otimes |v_{\mathcal{T}_{zx}^c}^{1-x\ldots 1-x}\rangle\langle v_{\mathcal{T}_{zx}^c}^{1-x\ldots 1-x}| \otimes A^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}} \otimes B^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}}\big)\rho_{RAB}\Big] \\
&\leq \frac{1}{2^{n+1}} \left\| \sum_{z,x} \sum_{v\in\mathcal{T}_{zx}^c, a} |a_{\mathcal{T}_{zx}}^{x\ldots x}\rangle\langle a_{\mathcal{T}_{zx}}^{x\ldots x}| \otimes |v_{\mathcal{T}_{zx}^c}^{1-x\ldots 1-x}\rangle\langle v_{\mathcal{T}_{zx}^c}^{1-x\ldots 1-x}| \otimes A^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}} \otimes B^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}} \right\| \\
&= \frac{1}{2^{n+1}} \left\| \sum_{z,x} \sum_{v\in\mathcal{T}_{zx}^c, a} |a_{\mathcal{T}_{zx}}^{x\ldots x}\rangle\langle a_{\mathcal{T}_{zx}}^{x\ldots x}| \otimes \mathbb{I}_{\mathcal{T}_{zx}^c} \otimes A^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}} \otimes B^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}} \right\| \\
&= \frac{1}{2^{n+1}} \left\| \sum_{z,x} \Pi^{zx} \right\| \leq \frac{1}{2^{n+1}} \sum_k \max_{xz} \|\Pi^{zx}\Pi^{\pi_k(zx)}\|,
\end{aligned} \tag{111}$$

where we used $\sum_{v\in\mathcal{T}_{zx}^c} |v_{\mathcal{T}_{zx}^c}^{1-x\ldots 1-x}\rangle\langle v_{\mathcal{T}_{zx}^c}^{1-x\ldots 1-x}| = \mathbb{I}_{\mathcal{T}_{zx}^c}$ where $I_{\mathcal{T}_{zx}^c}$ is the identity in the systems T_{zx}^c, in the last equality we defined $\Pi^{zx} := \sum_a |a_{\mathcal{T}_{zx}}^{x\ldots x}\rangle\langle a_{\mathcal{T}_{zx}}^{x\ldots x}| \otimes \mathbb{I}_{\mathcal{T}_{zx}^c} \otimes A^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}} \otimes B^x_{a_{\mathcal{T}_{zx}} a_{\mathcal{T}_{zx}^c}}$, and we used Lemma A.2 in the last inequality, for a set of mutually orthogonal permutations $\{\pi_k\}$. Fix

k, let $z'x' := \pi_k(zx)$, let $\mathcal{I} := \mathcal{T}_{zx} \cap \mathcal{T}_{z'x'}$, let $i = |\mathcal{I}|$ and denote $\mathcal{I}^c = [n] \setminus \mathcal{I}$. We define

$$\begin{aligned} P^{zx} &:= \sum_a |a_{\mathcal{I}}^{x\ldots x}\rangle\langle a_{\mathcal{I}}^{x\ldots x}| \otimes \mathbb{I}_{\mathcal{I}^c} \otimes A_a^x \otimes \mathbb{I}_B, \\ Q^{z'x'} &:= \sum_{a'} |a_{\mathcal{I}}'^{x'\ldots x'}\rangle\langle a_{\mathcal{I}}'^{x'\ldots x'}| \otimes \mathbb{I}_{\mathcal{I}^c} \otimes \mathbb{I}_A \otimes B_{a'}^x. \end{aligned} \tag{112}$$

Note that $\Pi^{zx} \preceq P^{zx}$ and $\Pi^{z'x'} \preceq Q^{z'x'}$, then, by Lemma A.4, $\|\Pi^{zx}\Pi^{z'x'}\| \leq \|P^{zx}Q^{z'x'}\| = \|P^{zx}Q^{z'x'}Q^{z'x'}P^{zx}\|^{\frac{1}{2}} = \|P^{zx}Q^{z'x'}P^{zx}\|^{\frac{1}{2}}$. We compute the last product of matrices:

$$\begin{aligned} P^{zx}Q^{z'x'}P^{zx} &= \sum_{a,a',a''} |a_{\mathcal{I}}^{x\ldots x}\rangle\langle a_{\mathcal{I}}^{x\ldots x}|a_{\mathcal{I}}'^{x'\ldots x'}\rangle\langle a_{\mathcal{I}}'^{x'\ldots x'}|a_{\mathcal{I}}''^{x\ldots x}\rangle\langle a_{\mathcal{I}}''^{x\ldots x}| \otimes \mathbb{I}_{\mathcal{I}^c} \otimes A_a^x A_{a''}^x \otimes B_{a'}^{x'} \\ &= \sum_{a,a'} |\langle a_{\mathcal{I}}^{x\ldots x}|a_{\mathcal{I}}'^{x'\ldots x'}\rangle|^2 |a_{\mathcal{I}}^{x\ldots x}\rangle\langle a_{\mathcal{I}}^{x\ldots x}| \otimes \mathbb{I}_{\mathcal{I}^c} \otimes A_a^x \otimes B_{a'}^{x'}, \end{aligned} \tag{113}$$

where we used that $A_a^x A_{a'}^x = \delta_{aa'} A_a^x$. We distinguish two cases:

(i) if $x \neq x'$, we have that $|\langle a_{\mathcal{I}}^{x\ldots x}|a_{\mathcal{I}}'^{x'\ldots x'}\rangle|^2 = 2^{-i}$, and then,

$$P^{zx}Q^{z'x'}P^{zx} = \sum_a 2^{-i}|a_{\mathcal{I}}^{x\ldots x}\rangle\langle a_{\mathcal{I}}^{x\ldots x}| \otimes \mathbb{I}_{\mathcal{I}^c} \otimes A_a^x \otimes \sum_{a'} B_{a'}^{x'} = \sum_a 2^{-i}|a_{\mathcal{I}}^{x\ldots x}\rangle\langle a_{\mathcal{I}}^{x\ldots x}| \otimes \mathbb{I}_{\mathcal{I}^c} \otimes A_a^x \otimes \mathbb{I}_B,$$

therefore

$$\|P^{zx}Q^{z'x'}P^{zx}\| \leq 2^{-i}. \tag{114}$$

(ii) If $x = x'$, then $|\langle a_{\mathcal{I}}^{x\ldots x}|a_{\mathcal{I}}'^{x'\ldots x'}\rangle|^2 = \delta_{aa'}$ and we use the trivial bound

$$\|P^{zx}Q^{z'x'}P^{zx}\| \leq 1. \tag{115}$$

Therefore, we have that

$$\|\Pi^{zx}\Pi^{z'x'}\| \leq \begin{cases} \sqrt{2^{-i}} & \text{if } x \neq x', \\ 1 & \text{if } x = x'. \end{cases} \tag{116}$$

In order to apply it in the bound (111), consider the set of permutations given by $\pi_k(zx) = zx \oplus k$, where $zx, k \in \{0,1\}^{n+1}$ (they are such that they have the same Hamming distance). Notice that exactly half of the permutations (i.e. 2^n) are such that $x = x'$ and the other half are such that $x \neq x'$. For the latter case, there are $\binom{n}{i}$ permutations with Hamming distance i. Then,

$$\begin{aligned} \omega_Q(\mathcal{G}^{n-\text{local guessing}})\big|_{\mathcal{S}} &\leq \frac{1}{2^{n+1}}\left\|\sum_{z,x}\Pi^{zx}\right\| \leq \frac{1}{2^{n+1}}\sum_k \max_{xz}\|\Pi^{zx}\Pi^{\pi_k(zx)}\| \\ &\leq \frac{1}{2^{n+1}}\left(2^n + \sum_{i=0}^n \binom{n}{i}\sqrt{2^{-i}}\right) = \frac{1}{2} + \frac{1}{2}\left(\frac{1+1/\sqrt{2}}{2}\right)^n. \end{aligned} \tag{117}$$