Secure Certification of Mixed Quantum States with Application to Two-Party Randomness Generation

Frédéric Dupuis[3,4](✉), Serge Fehr[1,2], Philippe Lamontagne[5], and Louis Salvail[5]

[1] Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
serge.fehr@cwi.nl
[2] Mathematical Institute, Leiden University, Leiden, The Netherlands
[3] Université de Lorraine, CNRS, Inria, LORIA, 54000 Nancy, France
frederic.dupuis@loria.fr
[4] Faculty of Informatics, Masaryk University, Brno, Czech Republic
[5] Université de Montréal (DIRO), Montréal, Canada
{lamontph,salvail}@iro.umontreal.ca

Abstract. We investigate sampling procedures that certify that an arbitrary quantum state on n subsystems is close to an ideal mixed state $\varphi^{\otimes n}$ for a given reference state φ, up to errors on a few positions. This task makes no sense classically: it would correspond to certifying that a given bitstring was generated according to some desired probability distribution. However, in the quantum case, this is possible if one has access to a prover who can supply a purification of the mixed state.

In this work, we introduce the concept of mixed-state certification, and we show that a natural sampling protocol offers secure certification in the presence of a possibly dishonest prover: if the verifier accepts then he can be almost certain that the state in question has been correctly prepared, up to a small number of errors.

We then apply this result to two-party quantum coin-tossing. Given that strong coin tossing is impossible, it is natural to ask "how close can we get". This question has been well studied and is nowadays well understood from the perspective of the bias of individual coin tosses. We approach and answer this question from a different—and somewhat orthogonal—perspective, where we do not look at individual coin tosses but at the global entropy instead. We show how two distrusting parties can produce a common high-entropy source, where the entropy is an arbitrarily small fraction below the maximum.

1 Introduction

1.1 Background and Motivation

Certifying correctness by means of cut-and-choose techniques is at the core of many – classical and quantum – cryptographic protocols. This goes back as far as Yao's garbled circuits, introduced in the 80s, where cut-and-choose is the

© International Association for Cryptologic Research 2018
A. Beimel and S. Dziembowski (Eds.): TCC 2018, LNCS 11240, pp. 282–314, 2018.
https://doi.org/10.1007/978-3-030-03810-6_11

main technique used to obtain active security. Even more so, cut-and-choose is at the very heart of essentially any quantum-cryptographic protocol, where participants are often asked to prepare states that agree with some specification. Certifying that quantum states satisfy this specification is essential to proving the security of these protocols.

Underlying these techniques is one of the most fundamental tasks in statistics: sampling. It allows one to infer facts about a large set of data by only looking at a small subset of it. For example, one can estimate the number of zeros in an n-bit string with very high accuracy by looking only at a small, randomly selected subset of the bits. This is also true in quantum mechanics: given an n-qubit system, one can infer that it is almost entirely contained in a subspace $\mathrm{span}\{|s\rangle : s \text{ is a bitstring with } (\delta \pm \epsilon)n \text{ 1's}\}$ by measuring a small subset of the qubits and observing that a fraction δ of the bits are ones [6].

One thing that a classical sampling procedure *cannot* do, however, is to infer the probability distribution from which the bitstring was generated. While a sampling procedure might be able to tell us that a bitstring contains roughly $n/2$ zeros and $n/2$ ones, that does not mean that it originally came from n fair coin flips—for all we know, it might be a fixed string that happens to have the right number of zeros and ones. If we were somehow able to do this, it would have interesting consequences for cryptography: for instance, we could get a coin-flipping protocol by getting one party to generate the coin flips, send them to the other party, and have the other party perform this hypothetical sampling procedure to certify that most of the bits indeed came from fair coin flips.

While this is clearly impossible in the classical case, it turns out that, perhaps surprisingly, this makes sense in the quantum scenario. This is due to the phenomenon of *purification*: given a mixed quantum state ρ_A on system A (which corresponds to a probability distribution on quantum states), it is possible to define a bipartite *pure* (i.e. deterministic) state $|\psi\rangle_{AR}$ which is in the same mixed state as ρ_A when looking at A only. Hence, one can *certify* that A is in the mixed state ρ_A by asking someone to produce the purifying system R and measuring that the combined system AR is indeed in state $|\psi\rangle_{AR}$. To give a more concrete example, suppose ρ_A is a uniformly random qubit, i.e. $\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. Then, the pure state $|\Phi\rangle_{AR} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ purifies it, and checking that AR is in state $|\Phi\rangle$ certifies that A was uniformly distributed in the first place. Note also that one does not need to trust the party who gives us the purification, making this suitable for an adversarial setting.

This leads to the following natural sampling protocol. Consider a sampler Sam who holds an arbitrary quantum state ρ_{A^n} on n subsystems, prepared by a possibly dishonest prover Paul. Sam would like to certify that this state is close to the ideal mixed state $\varphi^{\otimes n}$, possibly with errors on a small number of positions, for a given reference state φ. To do this, he selects a small subset of k positions at random, and he asks the distrusted prover Paul to deliver the purifying systems R^k for these positions. He then measures the POVM $\{|\varphi\rangle\langle\varphi|_{AR}, \mathbb{1} - |\varphi\rangle\langle\varphi|_{AR}\}$ on each of the selected systems in the sample to ensure that all of them are in the state $|\varphi\rangle_{AR}$ which purifies φ_A. He rejects if any errors are detected.

We emphasize that for verifying a *mixed* reference state, interaction with a prover is necessary, as there is no local measurement on Sam's side that can distinguish between the correct state $\varphi^{\otimes n}$ and a state that consists of the eigenvectors of φ in the correct proportions (given by the eigenvalues).

1.2 Our Contribution

In this paper, we investigate this type of sampling procedure in detail. Several challenges arise in the analysis of this protocol. First, defining what we mean when we say that the sampling works is not trivial. In the case of regular quantum sampling, we usually want to say that the state has a very small probability of being outside of a low-error subspace that corresponds to the statistics that we have observed. For mixed states, this definition fails completely: every subspace contains *pure* states, which we would want to exclude since they are very far from the ideal *mixed* state. We might then be tempted to include the purifying systems in the definition of the low-error subspace, but then we have no guarantee that an adversarial prover will respect the structure we want to impose on his part of the state—we don't even know that it consists of n subsystems. A second difficulty comes from the fact that the prover might not necessarily want to provide the state that gives him the best chance of passing the test, even if he has it. If we again look at the case of certifying uniformly random qubits, even if Sam has the ideal state before the sampling begins, Paul might want to bias the outcome, for example by passing the test if he measures $|0\rangle$ on all of the non-sampled qubits, and failing on purpose otherwise. Because of these difficulties, our main result does not follow from traditional sampling theorems.

We overcome these challenges and present a general class of mixed state certification protocols which contains the natural protocol described above. We show that any protocol that fits this class, and that satisfies the simple criteria of being invariant under permutations and performing well on i.i.d. states, allows us to control the post-sampling state in a meaningful way. A positive consequence of this modular analysis is that previous results on *pure state* certification also fit our framework, and thus fall under a special case of our analysis – just as pure states are a special case of mixed states. Because pure state certification has already found many applications in cryptography [6,10–12,29], the fact that we recover it as a special case positions our result as a powerful tool for quantum cryptography.

Another part of the paper is devoted to applying this result to coin tossing—or *randomness generation*. Given that strong coin tossing is known to be impossible, it is natural to ask "how close can we get?". This question has been well studied and is nowadays well understood from the perspective of the bias of individual coin tosses (see Sect. 1.3 below). We approach and answer this question from a different—and somewhat orthogonal—perspective, where we do not optimize individual coin tosses but the global entropy instead. From this entropic perspective, we show that "the next best" after strong coin tossing is possible. We show that the coin-flipping protocol loosely described above allows two distrusting parties to produce a common high-entropy source, where the entropy is an arbitrarily small fraction below the maximum (except with negligible probability).

Our protocol for the task of two party randomness generation outperforms any classical protocol in the information theoretical setting. The trivial classical protocol—where each party tosses $n/2$ unbiased coins and the output is the result of the n tosses—is optimal for this task [15].

The paper is organized as follows. First, in the next subsections, we discuss some previous work in the area and the relevance of our work for cryptography. In Sect. 2, we introduce the notation and recall some useful facts. Section 3 presents the main result in more detail. The coin-flipping protocol described above is presented in Sect. 4, and the proof of our main result then follows in Sect. 5.

1.3 Previous Work

Classical sampling results have been around since the foundations of modern probability theory, dating back to the work of Bernstein, Hoeffding and Chernoff on concentration of measure in the 1920s and 1930s. More recently, several quantum generalizations of these classics have been proven. These generalizations include, for instance, Ahlswede and Winter's operator Chernoff bound [1] and the quantum Chernoff bound of [4]. However, these generalizations are not easily amenable to giving results about sampling, unlike their classical counterparts. Other quantum results can be used to analyze sampling in certain contexts, such as quantum de Finetti theorems for quantum key distribution [9,23,24].

But perhaps the most direct analogues of the classical sampling results are those of [6]. There, the authors give a generic way to transpose classical sampling procedures to the quantum case. Roughly speaking, they show that if a classical sampling protocol says that a string of random variables $X_1, \cdots, X_n$ is contained in some "good" subset $\mathcal{X}_{\text{good}}$ except with negligible probability, then the quantum version of the same sampling procedure (defined in a precise way in [6]) would say that the final state $\rho_{X_1,\ldots,X_n}$ is almost entirely contained in the good subspace $\text{span}\{|x_1\rangle \otimes \cdots \otimes |x_n\rangle : x_1, \cdots, x_n \in \mathcal{X}_{\text{good}}\}$, except with negligible probability. This "good" set would normally correspond to strings that are consistent with what was observed in the sample. Our main result can be viewed as extending this to the case of mixed state sampling.

Our main application, coin flipping, also has a long history. The basic task was first defined in 1981 by Manuel Blum [5]. Since the early 2000's, it has received a lot of attention in the quantum cryptography community, as it is one of the most natural tasks for which quantum protocols can perform something that is impossible classically. There are two versions of coin flipping: *strong* coin flipping, in which we require the protocol to be equivalent to a black box that produces the coin flip and distributes the result, and *weak* coin flipping, in which each participant has a known preferred outcome and must be prevented from biasing the outcome in that direction. Several quantum protocols for strong coin flipping have been developed with various biases [3,27], but a fundamental lower bound of $(\frac{1}{\sqrt{2}} - \frac{1}{2})$ on the bias of such protocols was proven in [17] (see also [13]). Finally, a protocol with a bias matching the lower bound was proven in [7]. For weak

coin flipping, we have had several protocols [16,18,19,28], again with various biases, but this time culminating in a protocol with arbitrarily small bias [20]. Quantum coin flipping has even been implemented in the lab [22]. Here, we go in a somewhat different direction: we show that even though strong coin flipping with negligible bias is impossible without assumptions, two distrustful parties can produce a common string of min-entropy arbitrarily close to maximum.

A strong quantum coin tossing protocol using ideas similar to that of the protocol described in Sect. 4 has been previously considered by Høyer and Salvail (unpublished) for achieving in a slightly simpler way the same $\frac{1}{4}$ bias than the one in [2]. Alice prepares two EPR pairs and sends one half of each to Bob. Bob picks at random one qubit out of the two and verifies that Alice holds the corresponding purification register of an EPR pair by asking her to measure it in a random BB84 basis before comparing the result with his own. If this test succeeds, Bob gets some evidence that the remaining pair of qubits can be used as a coin toss after measuring it in the canonical basis. Our protocol extends this test to a random sample of a population of N qubits, increasing the confidence that Bob has about the remaining qubits being "close" to ideal coin tosses when the test is successful.

1.4 Applications to Cryptography

Sampling with a Pure Reference State. Previous results on sampling from a quantum population have dealt with *pure* reference states. In this case, the sampler can choose its sample and perform local measurements on the sampled positions without any help from the prover. This setting allows for standard classical tools such as Hoeffding's inequality to be used to derive the probability that the sampled positions' proximity to the reference state is not a good indicator for the unsampled positions' proximity to the same reference state.

Since pure states are a special case of mixed states, a natural property that we would want for our mixed state sampling result is to recover a statement similar to the one for pure state sampling in the framework of [6]. This is indeed the case when we restrict our attention to the task of certification, i.e. when we do not tolerate any error in the sample. Although our results do not use the same tools, and are expressed in terms of a *post-selected* operator instead of in terms of proximity to an ideal state (see Sect. 3), we recover a statement equivalent to that of [6], albeit with slightly worse parameters, when we apply our results to pure reference states. Since most applications [6,11,12,29] of pure state sampling has been in the setting of certification, our results can also be used to prove those applications.

Sampling with a Distributed Pure Reference State. Our mixed state sampling result is also applicable to an instance of pure state certification that falls outside the framework of [6] and which was presented and analyzed in an ad hoc way in [10]. Their sampling algorithm was used as part of a protocol for leakage resilient computation.

The sampling task considered in [10] is as follows: spacially separated Alice and Bob want to certify that their joint registers – which was prepared by an untrusted third party – is of the form $|\varphi\rangle_{AB}^{\otimes n}$ for some entangled state $|\varphi\rangle$ where Alice holds the A part of each of the n states and Bob the B part. The fact that the state is distributed between Alice and Bob means that the techniques of [6] do not apply: the two samplers cannot perform a projective measurement to check that their shared registers are in the reference state $|\varphi\rangle_{AB}$.

Our results of Sect. 5 only requires that the sampling protocol's verification procedures is invariant under the permutation of the quantum population, and that it aborts when performed on an *obviously bad* state. Since the pure state certification protocol of [10] satisfies these properties, our techniques readily apply and can be used to analyze their protocol.

Application to Two-Party Computation. In [26], the power of quantum communication for secure unconditional two-party computation is investigated. Among other results, it was shown that *correct* quantum implementations of two-party classical cryptographic primitives must leak at least some minimal amount of information to one of the parties. For example, randomized variants[1] of one-out-of-two OT and secure AND sharing must leak at least $\frac{1}{2}$ bit on average. Protocols exist in the quantum honest-but-curious model that minimize the amount of leakage for a given primitive. The simplest such protocol consists of an adversary preparing and distributing an *embedding* of the primitive. An embedding of a cryptographic primitive is a pure state that yields the correct outcomes when measured in the computational basis, i.e. from each party's point of view, the state shared before the final measurement is a purification of the probability distribution for this party's output.

A protocol that achieves minimal leakage against *active* adversaries under the sole assumption that the parties have access to strong coin-tosses is easily obtained from mixed-state certification. One of the parties would generate many copies of the embedding of the primitive that minimizes leakage and the other party certifies correctness using our sampling procedure. They then choose one of the remaining embeddings, the target embedding, and measure it; the outcome acts as the output of the protocol. If the sampling succeeds, the unsampled positions are close to ideal embeddings from the sampler's perspective and randomly picking the target embedding would then have close to minimal leakage with good probability. However, without additional resources, an adversary (the sampler say) could measure its part of a few embeddings before choosing the target embedding as one that produces the output the adversary wants to see. Coin-tosses are therefore required to pick the target embedding without bias.

[1] Variants where the primitives considered are applied to random inputs.

2 Preliminaries

2.1 Notation

Let $\mathcal{H}_A, \mathcal{H}_B$ be two Hilbert spaces, we write $L(\mathcal{H}_A, \mathcal{H}_B)$ for the set of linear operators from $\mathcal{H}_A$ to $\mathcal{H}_B$ and we write $L(\mathcal{H}_A)$ for $L(\mathcal{H}_A, \mathcal{H}_A)$. Let $\mathcal{D}_{\leq}(\mathcal{H})$ be the set of positive semi-definite operators with trace less than or equal to 1, and let $\mathcal{D}(\mathcal{H})$ be the set of density operators on $\mathcal{H}$. The set of isometries from $\mathcal{H}_A$ to $\mathcal{H}_B$ is denoted $U(\mathcal{H}_A, \mathcal{H}_B)$. We use the notation $U_{A\to B}$ to illustrate that $U_{A\to B} \in U(\mathcal{H}_A, \mathcal{H}_B)$. When there is no ambiguity from doing so, we write U_A instead of $U_{A\to B}$. For an arbitrary isometry U, we sometimes write $[U](\rho)$ as shorthand for $U\rho U^\dagger$. For a pure state $|\psi\rangle$, we write ψ as shorthand for $|\psi\rangle\langle\psi|$ when this creates no ambiguity. For a linear operator A, $\|A\|_1 := \mathrm{tr}(\sqrt{A^\dagger A})$ denotes the *trace norm*. We denote $\mathbb{1}_A$ as the identity operator on $\mathcal{H}_A$ and id_A as the CPTP map that acts trivially on register A.

We let $[n] := \{1, \ldots, n\}$ denote the set of the first n positive integers for $n \in \mathbb{N}$. For a fixed finite set Y and any subset $X \subseteq Y$, $\bar{X}$ denotes the complement of X in Y, i.e. $\bar{X} = Y \backslash X$. Let $h(p) := -p\log_2(p) - (1-p)\log_2(1-p)$ be the binary entropy function; we make use of the fact that $\binom{n}{\beta n} \leq 2^{h(\beta)n}$ for $0 < \beta < 1$.

Let A be a quantum register, we use the notation A^n to denote n identical copies of A and label them $A_1, \ldots, A_n$ when the need arises to distinguish individual registers. For $t \subseteq [n]$, we write A_t as the composite register containing registers A_i for each $i \in t$.

2.2 Permutation Invariance and the Symmetric Subspace

Let $\mathcal{S}_n$ denote the symmetric group on n elements and let $A_1, \ldots, A_n$ be n quantum registers with identical state space $\mathcal{H}$. For $\pi \in \mathcal{S}_n$, we use the same symbol to denote the unitary operation that acts on $\mathcal{H}^{\otimes n}$ by

$$\pi(|\phi_1\rangle_{A_1} \otimes \cdots \otimes |\phi_n\rangle_{A_n}) = \left|\phi_{\pi^{-1}(1)}\right\rangle_{A_1} \otimes \cdots \otimes \left|\phi_{\pi^{-1}(n)}\right\rangle_{A_n}. \tag{1}$$

Definition 1. *The* symmetric subspace *of* $\mathcal{H}^{\otimes n}$*, denoted* $\mathrm{Sym}^n(\mathcal{H})$*, is the space spanned by all vectors* $|\phi\rangle \in \mathcal{H}^{\otimes n}$ *with* $\pi|\phi\rangle = |\phi\rangle$ *for any* $\pi \in \mathcal{S}_n$*. A pure state* $|\phi\rangle \in \mathrm{Sym}^n(\mathcal{H})$ *is referred to as a* symmetric state*.*

A density operator $\rho \in \mathcal{D}(\mathcal{H}^{\otimes n})$ *is called* permutation invariant *if* $\pi\rho\pi^\dagger = \rho$ *for all* $\pi \in \mathcal{S}_n$*.*

Remark 1 ([8,23]). Although not all permutation invariant operators have support in the symmetric subspace, the next lemma asserts that they have a purification that does: for any permutation invariant density operator ρ_{A^n} on $\mathcal{H}_A^{\otimes n}$ there exists a pure state $|\rho_{A^nB^n}\rangle \in \mathrm{Sym}^n(\mathcal{H}_A \otimes \mathcal{H}_B)$ where $\mathcal{H}_A \simeq \mathcal{H}_B$, such that $\mathrm{tr}_{B^n}(\rho_{A^nB^n}) = \rho_{A^n}$.

Remark 2 ([23,25]). Let $\mathcal{H}$ be a d-dimensional Hilbert space. The projector onto the symmetric subspace $\mathrm{Sym}^n(\mathcal{H})$ can be expressed as

$$c_{n,d} \int |\theta\rangle\langle\theta|^{\otimes n} d|\theta\rangle$$

where $d|\theta\rangle$ is the measure on the set of pure states of $\mathcal{H}$ induced by the Haar measure on the set of unitaries acting on $\mathcal{H}$ and where $c_{n,d} := \binom{n+d-1}{n} \leq (n+1)^{d-1}$ is the dimension of $\mathrm{Sym}^n(\mathcal{H})$.

2.3 Mathematical Tools and Definitions

We say that an operator $\tilde{\rho}_B$ is *post-selected* from register A of ρ_{AB} if there exists a POVM element $0 \leq E_A \leq \mathbb{1}_A$ such that $\tilde{\rho}_B = \mathrm{tr}_A((E_A \otimes \mathbb{1}_B)\rho_{AB})$. The following remark on relation between the reduced operator of a joint system before and after a post-selected measurement takes place will be useful.

Remark 3. Let ρ_{AB} be an arbitrary positive semi-definite operator on registers AB. Let $0 \leq E_A \leq \mathbb{1}_A$ be a positive semidefinite operator acting on register A. Then it holds that

$$\mathrm{tr}_A\left((E_A \otimes \mathbb{1}_B)\rho_{AB}\right) \leq \mathrm{tr}_A\left(\rho_{AB}\right).$$

The following observation shows that there is a strong relation between post-selected operators and upper-bounded operators.

Proposition 1. *Let $c \geq 0$ and let ρ_Q, σ_Q be two positive semi-definite operators. Then $\rho_Q \leq c \cdot \sigma_Q$ if and only if for any purification $|\sigma_{R_1Q}\rangle$ of σ_Q and $|\rho_{R_2Q}\rangle$ of ρ_Q, there exists a linear operator $A_{R_1 \to R_2}$ such that $A^\dagger_{R_1} A_{R_1} \leq \mathbb{1}_{R_1}$ and*

$$|\rho_{R_2Q}\rangle = \sqrt{c} \cdot (A_{R_1 \to R_2} \otimes \mathbb{1}_Q)|\sigma_{R_1Q}\rangle. \tag{2}$$

Proof. Let's start with the easier direction of the proof. Let $|\sigma_{R_1Q}\rangle$ be a purification of σ_Q, let $|\rho_{R_2Q}\rangle$ be a purification of ρ_Q and let $A_{R_1 \to R_2}$ be as in (2). Then by Remark 3, ρ_Q is equal to

$$\mathrm{tr}_{R_2}\left(\rho_{R_2Q}\right) = c \cdot \mathrm{tr}_{R_1}\left((A^\dagger_{R_1 \to R_2} A_{R_1 \to R_2} \otimes \mathbb{1}_Q)\sigma_{R_1Q}\right) \leq c \cdot \mathrm{tr}_{R_1}\left(\sigma_{R_1Q}\right) = c \cdot \sigma_Q.$$

For the other direction, write σ_Q as $\sigma_Q = \frac{1}{c}(\rho_Q + \tilde{\sigma}_Q)$ where $\tilde{\sigma}_Q := c \cdot \sigma_Q - \rho_Q \geq 0$. Let $|\rho_{R_2Q}\rangle$ be an arbitrary purification of ρ_Q and let $|\tilde{\sigma}_{R_2Q}\rangle$ be a purification of $\tilde{\sigma}_Q$ that lives in the same space. Then consider the following purification of σ_Q: $|\sigma_{R'R_2Q}\rangle := \sqrt{\frac{1}{c}}(|0\rangle_{R'}|\rho_{R_2Q}\rangle + |1\rangle_{R'}|\tilde{\sigma}_{R_2Q}\rangle)$. Let $|\sigma_{R_1Q}\rangle$ be an arbitrary purification of σ_Q and let $A_{R_1 \to R_2} := (\langle 0|_{R'} \otimes \mathbb{1}_{R_2})V_{R_1 \to R'R_2}$ where $V_{R_1 \to R'R_2}$ is an isometry that maps $|\sigma_{R_1Q}\rangle$ to $|\sigma_{R'R_2Q}\rangle$. Then

$$(A_{R_1 \to R_2} \otimes \mathbb{1}_Q)|\sigma_{R_1Q}\rangle = (\langle 0|_{R'} \otimes \mathbb{1}_R)|\sigma_{R'R_2Q}\rangle = \sqrt{\frac{1}{c}}|\rho_{R_2Q}\rangle.$$

□

The following proposition is a simple corollary of the *pinching inequality* [14, Lemma 9]. A direct consequence of this is that a superposition of a few states can be *approximated* by a mixture of the same few states.

Proposition 2. *Let $\{|\psi_i\rangle\}_{i\in\mathcal{J}}$ be a family of vectors living on a Hilbert space $\mathcal{H}$ indexed by some finite set $\mathcal{J}$. Define operators*

$$\rho = \sum_{i,j\in\mathcal{J}} |\psi_i\rangle\langle\psi_j| \text{ and } \rho^{\text{mix}} = \sum_{i\in\mathcal{J}} |\psi_i\rangle\langle\psi_i|.$$

Then, $\rho \leq |\mathcal{J}| \cdot \rho^{\text{mix}}$.

Definition 2 (Quantum "Hamming Ball"). *Let $|\Psi\rangle \in \mathcal{H}^{\otimes n}$ for $n \in \mathbb{N}$ and let $r \in [n]$. We define the quantum* Hamming ball *of radius r around $|\Psi\rangle$, denoted $\Delta_r(|\Psi\rangle)$, as the space spanned by all vectors of the form $U|\Psi\rangle$ where U is a unitary that acts as the identity on at least $n-r$ subsystems.*

For the special case where $|\Psi\rangle = |\nu\rangle^{\otimes n}$,

$$\Delta_r(|\nu\rangle^{\otimes n}) = \text{span}\{\pi(|\nu\rangle^{\otimes n-r} \otimes |u\rangle) \ : \ |u\rangle \in \mathcal{B}, \pi \in \mathcal{S}_n\}$$

where $\mathcal{B}$ is an orthonormal basis of $\mathcal{H}^{\otimes r}$.

The projector onto the quantum Hamming ball of radius r around an i.i.d. state $|\nu\rangle^{\otimes n} \in \mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_n}$ can be written as

$$\mathbb{P}^{r,|\nu\rangle}_{A^n} = \sum_{E\subseteq[n]\,:\,|E|\leq r} \left(\bigotimes_{i\in E} (\mathbb{1} - |\nu\rangle\langle\nu|)_{A_i} \bigotimes_{i\notin E} |\nu\rangle\langle\nu|_{A_i} \right).$$

The following Lemma says that n i.i.d. copies of a state close to $|\nu\rangle$ is almost entirely contained in a Hamming ball around $|\nu\rangle^{\otimes n}$.

Lemma 1. *Let $|\nu\rangle, |\theta\rangle \in \mathcal{H}$ be such that $|\langle\theta|\nu\rangle|^2 \geq 1-\epsilon$. Then, for any $\alpha > 0$,*

$$\text{tr}\left(\mathbb{P}^{r,|\nu\rangle} \cdot |\theta\rangle\langle\theta|^{\otimes n}\right) \geq 1 - \exp(-2\alpha^2 n)$$

where $\mathbb{P}^{r,|\nu\rangle}$ is the projector onto $\Delta_r(|\nu\rangle^{\otimes n})$ for $r = (\epsilon+\alpha)n$.

Proof. Observe that

$$\text{tr}\left(\mathbb{P}^{r,|\nu\rangle}|\theta\rangle\langle\theta|^{\otimes n}\right) = \Pr[wt(X_\theta) \leq r] = \Pr[wt(X_\theta) - \epsilon n \leq \alpha n]$$

where X_θ is a random variable obtained by measuring n copies of $|\theta\rangle$ with observables $M_0 = |\nu\rangle\langle\nu|$ and $M_1 = \mathbb{1} - |\nu\rangle\langle\nu|$ and where $wt(\cdot)$ is the Hamming weight function, i.e. the number of ones. Since X_θ consists of n i.i.d. Bernoulli trials with parameter $1 - F(\nu,\theta)^2 \leq \epsilon$, Hoeffding's inequality allows us to lower-bound the above quantity: $\text{tr}(\mathbb{P}^{r,|\nu\rangle}\, |\theta\rangle\langle\theta|^{\otimes n}) \geq 1 - \exp(-2\alpha^2 n)$. □

3 Certification of Mixed States

The task we analyze can be understood as an interactive game between two participants: a *prover* Paul, and a *sampler* Sam. Paul is supposed to prepare multiple copies of some *reference state* φ before sending them to Sam, and the purpose of the game is for Sam to detect when the state produced by Paul is (close to) what it is supposed to be, no matter how maliciously Paul behaves. Here, the reference state φ may be an arbitrary but known *mixed* state. A canonical example of such a quantum sampling protocol is depicted in Fig. 1. It consists of Sam asking Paul to deliver the purification registers of k randomly chosen positions. Sam then measures these purifications in order to learn if they were in the right state.[2]

Purification-Based Sampling

1. Paul prepares N copies of the purification $|\varphi_{PS}\rangle$ of φ_S, he sends N registers in state φ_S labeled S_1 to S_N to Sam and keeps the corresponding purification registers P_1 to P_N.
2. Sam picks a subset $t \subseteq [N]$ of size k uniformly at random.
3. Sam sends t to Paul and asks him to send him the purification registers P_i for $i \in t$.
4. Sam measures each register P_iS_i for $i \in t$ using projective measurement $\{|\varphi\rangle\langle\varphi|_{PS}, \mathbb{1}_{PS} - |\varphi\rangle\langle\varphi|_{PS}\}$. Sam accepts if he observed $|\varphi\rangle\langle\varphi|^{\otimes k}$, otherwise, he rejects.

Fig. 1. The purification-based mixed state quantum sampling protocol with reference state φ_S. Paul and Sam need to have previously agreed on a purification $|\varphi_{PS}\rangle$ of φ_S.

In the extreme case of a reference state that is empty on Paul's side, and thus pure on Sam's side (and so there is no purification for Paul to provide in step 2), the sampling protocol of Fig. 1 pretty much coincides with the pure-state sampling procedure considered and analyzed in [6]. For a true mixed reference state, however, it is significantly harder to prove that the sampling protocol "does its job" because of the additional freedom that Paul has in preparing the purification registers that may depend on the choice of t. This very much renders the techniques from [6] useless. Indeed, the idea of the analysis in [6] was to assume, for the sake of the argument, that the positions outside of t are measured as well, and then to delay the choice of t to after the measurement so as to reduce to a classical sampling procedure. Because of Paul's freedom in choosing the purifications dependent on t, it makes no sense to speak about the

[2] Note that there is no loss in generality in announcing the positions that Sam wants to check *in one go* as is done in Fig. 1, compared to announcing them *one-by-one*; doing it the latter way only makes it harder for Paul.

outcome of the reference measurement $\{|\varphi\rangle\langle\varphi|, \mathbb{1} - |\varphi\rangle\langle\varphi|\}$ *before* t is chosen, or about the measurement being applied to a position *outside* of t. As such, we need an entirely different approach.

Before worrying about analyzing the mixed-state sampling protocol of Fig. 1, we first need to specify what it should actually mean for it to "do its job"; this is not entirely obvious. Intuitively, we want that after the sampling, if Sam accepts then his part of the state should be "somehow close" to what it is supposed to be, namely $\varphi^{\otimes n}$ where we set $n = N - k$. However, Paul can obviously cheat in a small number of positions, i.e., start off with a state that consists of i.i.d. copies of $|\varphi\rangle$ except for a small number of positions where the state may deviate arbitrarily, and he still has a fair chance of not being caught. Of course, the same holds for a mixture of such states, and therefore, by purification, also for a superposition of such states. This motivates the definition below of an "ideal state", which captures the best we can hope for. The formal statement of what the sampling protocol of Fig. 1 achieves is then in terms of controlling Sam's part of the state after the protocol by means of Sam's part of such an ideal state. This is somewhat similar in spirit as the approach in [6] for pure-state sampling, though there are some technical differences.

Definition 3 (Ideal States). *For $\epsilon > 0$, a state $\psi_{S^n} \in \mathcal{D}_{\leq}(\mathcal{H}_S^{\otimes n})$ is said to be* ϵ–ideal *if there exists a purification $|\psi_{RP^nS^n}\rangle$ of ψ_{S^n} such that*

$$|\psi\rangle_{RP^nS^n} \in \mathcal{H}_R \otimes \Delta_{\epsilon n}(|\varphi\rangle_{P^nS^n}^{\otimes n}).$$

We loosely say that ψ_{S^n} is ideal *when it is ϵ–ideal for* small *ϵ.*

This basically means that an ideal state is one where Paul could transform his system into one where he holds n systems P^n and an additional purifying R system, and where the P^nS^n part of the state lives in a low-error subspace.

Our analysis of the sampling protocol described in Fig. 1 (and some variants of it) preserves many aspects of the operational interpretation provided in [6] when sampling with respect to a pure reference state. We establish that Sam's *subnormalized* final state of register S^n upon acceptance can be controlled by an ideal state. The subnormalized state is simply the state Sam is left with when he accepts scaled down by the probability of acceptance (i.e. its trace corresponds to the probability for Sam to accept). Let $d := \dim(\mathcal{H}_S)$ be the size of the register holding φ_S and let $\epsilon > 0$ be a parameter. Informally, our main theorem (Theorem 2 and Corollary 2) establishes that Sam's subnormalized final state upon acceptance $\rho_{S^n}^{\text{acc}} \in \mathcal{D}_{\leq}(\mathcal{H}_S^{\otimes n})$ is such that

$$\rho_{S^n}^{\text{acc}} \leq (N+1)^{d^2-1}\psi_{S^n} + \sigma_{S^n}, \tag{3}$$

where ψ_{S^n} is ideal and $\|\sigma_{S^n}\|_1$ is negligible in N.

Any state $\rho_{S^n}^{\text{acc}}$ that satisfies (3) can be considered to be an ideal state in many applications. Let $\mathcal{Q}$ be a completely positive trace non-increasing superoperator modelling a task that we would like to apply upon $\rho_{S^n}^{\text{acc}}$. Suppose that $\mathcal{Q}$ behaves nicely when it is executed from an ideal state ψ_{S^n}. That is, the bad

event represented by a POVM element E_{bad} has negligible probability on the ideal state $p^{\text{id}}_{\text{bad}} := \text{tr}(E_{\text{bad}}\mathcal{Q}(\psi_{S^n})) \leq 2^{-\alpha N}$ for $\alpha > 0$. Running $\mathcal{Q}$ upon $\rho^{\text{acc}}_{S^n}$ instead produces the state $\mathcal{Q}(\rho^{\text{acc}}_{S^n}) \leq \mathcal{Q}((N+1)^{d^2-1}\psi_{S^n} + \sigma_{S^n})$. We then have that the probability of the bad event in the real case is $p^{\text{real}}_{\text{bad}} := \text{tr}(E_{\text{bad}}\mathcal{Q}(\rho^{\text{acc}}_{S^n})) \leq (N+1)^{d^2-1}p^{\text{id}}_{\text{bad}} + \|\sigma_{S^n}\|_1$, which remains negligible when $p^{\text{id}}_{\text{bad}}$ is negligible and d is small enough (i.e. a constant). In other words, any negligible upper bound on the probability of some "bad" event occurring when processing the ideal state translates to a negligible upper bound on the "bad" event when processing the real state instead. In these cases, it is good enough to analyze the ideal state, for which an analysis is typically simpler because of the specific form of the state as given by Definition 3.

Our main result can also be interpreted as a statement about Paul and Sam's joint state when Sam accepts. To do so, we invoke Proposition 1 upon (3). For the sake of simplicity, assume that $\rho^{\text{acc}}_{S^n} \leq c \cdot \psi_{S^n}$, which is essentially what (3) means for $c := (N+1)^{d^2-1}$. Proposition 1 then establishes the existence of a linear operator A acting upon registers RP^n for which $A^\dagger A \leq \mathbb{1}$ such that

$$|\rho^{\text{acc}}\rangle_{RP^nS^n} = \sqrt{c}(A \otimes \mathbb{1}_{S^n})|\psi\rangle_{RP^nS^n}, \tag{4}$$

where $|\rho^{\text{acc}}\rangle_{RP^nS^n}$ and $|\psi\rangle_{RP^nS^n}$ are purifications of $\rho^{\text{acc}}_{S^n}$ and ψ_{S^n}, respectively. The operator $E := AA^\dagger$ can be viewed as the outcome of a POVM applied upon registers RP^n implemented by the detection operator A. It follows from (4) that $\rho^{\text{acc}}_{RP^nS^n}$ can be obtained with a non-negligible probability of success $1/c$ by applying a measurement upon an ideal state $\psi_{RP^nS^n}$. Therefore, any application having a negligible probability for Paul to generate a *bad* shared state from an ideal one has also a negligible probability to generate a *bad* shared state from the real one.

We now state our main result in the special case of the basic protocol given in Fig. 1. To do so, we define $\mathcal{E}^{\text{acc}}_{RS^N\to S^n}$ as a completely positive, trace non-increasing map that represents the execution of the protocol in the accepting case, meaning that given an initial state ρ_{RS^n}, $\mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho_{RS^n})$ will be a subnormalized density matrix representing the output given that the verifier accepted, and $\text{tr}[\mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho)]$ will be the probability of acceptance on that input state. The statement is the following:

Theorem 1. *Let $\mathcal{E}^{\text{acc}}_{RS^N\to S^n}$ be defined as above, and let $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$ be an arbitrary input state. For any $\epsilon > 0$, there exist a subnormalized ϵ-ideal operator $\psi_{S^n} \in \mathcal{D}_{\leq}(\mathcal{H}_S^{\otimes n})$ and σ_{S^n} such that*

$$\mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho_{RS^N}) \leq c_{N,d^2} \cdot \psi_{S^n} + \sigma_{S^n}$$

where $\|\sigma_{S^n}\|_1 \leq \exp(-\Omega(N))$.

The proof is deferred to Sect. 5 (Theorem 2 and Corollary 2), where it will be a corollary of a more general statement.

3.1 Sampling Protocol Using LOCC only

Our analysis of mixed state sampling protocols is not limited to the protocol of Fig. 1. In Sect. 5, we show that any sampling protocol that satisfy certain criteria can be analyzed using our techniques. One such protocol is the one depicted in Fig. 2. It is a protocol for certifying that Paul prepares—and purifies—halves of EPR pairs that requires only local operations and classical communication (LOCC) after the initial state preparation and distribution phase. EPR pairs are states of the form $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ that have the unique property that measurements in both the computational and diagonal bases are perfectly correlated. The protocol exploits this fact in the following way: for each position in the sample, Sam asks Paul for the result of measuring his purifying register in a random basis, and checks that this result corresponds to his own measurement in the same basis.

EPR-LOCC Sampling

1. Paul prepares N EPR pairs and sends half of each to Sam.
2. Sam chooses a sample $t \subset [N]$ of size k and a basis $c \in \{+, \times\}^k$ both uniformly at random, and sends both to Paul.
3. Upon reception of t and c, Paul measures each qubit of the sample in the corresponding basis c_i. He sends the outcome $\hat{X} \in \{0,1\}^k$ back to Sam.
4. Sam measures each of his sampled qubit in the corresponding basis c_i, let $X \in \{0,1\}^k$ be the outcome. He rejects if $\hat{X} \neq X$.

Fig. 2. The sampling protocol with local measurements for sampling halves of EPR pairs, i.e. with reference state $\varphi = \frac{1}{2}$.

4 Two-Party Randomness Generation

Before we prove our main result, we first apply the protocol in Fig. 1 to a two-party randomness generation problem.

4.1 The Protocol

The protocol for randomness generation is depicted in Fig. 3. The protocol works as follows: Alice first has to generate N EPR pairs and send half of each to Bob. Bob then uses our sampling protocol of Fig. 1 to certify that the state Alice sent him is (close to) the prescribed state. If Bob's check succeeds, then our quantum sampling result says that Alice basically prepared the right state, up to a few errors. Bob's measurement outcome will then have very high min-entropy (arbitrarily close to the maximum n).

1. Alice prepares the state $|\Phi^+\rangle^{\otimes N}_{A^N B^N}$ for $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends the system B^N to Bob.
2. Alice and Bob perform protocol **Purification-Based Sampling** from Fig. 1 with Alice as the prover and Bob as the sampler and with $k = \beta N$ for $\beta > 0$ such that βN is an integer. Let $\rho_{A^n B^n} \in \mathcal{D}((\mathcal{H}_2 \otimes \mathcal{H}_2)^{\otimes n})$ be the resulting normalized joint state of $n = N - k$ pairs of qubits.
3. Alice and Bob respectively measure their n qubits in the computational basis and output their respective measurement outcomes X_A and X_B.

Fig. 3. The randomness generation protocol. N is the security parameter, β determines the size of the sample.

4.2 Entropy of Alice and Bob's Outputs

Since Alice is the preparer of the N EPR pairs, her output will have high min-entropy. The tricky part of the following proof is showing that Bob's freedom in choosing t and accepting or refusing the sampling outcome cannot influence too much the distribution of Alice's measurement outcome.

Lemma 2 (Entropy of Alice's output). *If Alice follows the protocol, then for any $\gamma > 0$, her output $X_A \in \{0,1\}^n$ satisfies*

$$\mathrm{H}_\infty(X_A) \geq (1-\gamma)n,$$

except with probability negligible in n.

Proof. Let $\rho_{A^N B^N}$ be the joint state of Alice and Bob before the sampling phase. As the preparer of the quantum state, Alice prepares N perfect EPR pairs (i.e. $\rho_{A^N B^N} = |\Phi^+\rangle\langle\Phi^+|^{\otimes N}$), so her measurement outcome would have maximal min-entropy for the n remaining qubits were it not for Bob's actions. Bob can bias the outcome of Alice's measurement in two possible ways: (1) he can measure his register B^N *before* choosing t and make t depend on this measurement outcome and (2) he can make the sampling abort even though Alice was honest. We analyze both possibilities separately, showing that each cannot reduce the min-entropy by more than a small linear amount, except with negligible probability.

For (1), suppose Bob performs some measurement on his register B^N that yields sample choice $t \subset [N]$ with probability p_t and results in the reduced density operator $\rho^t_{A^N}$ on Alice's side. Suppose also that Alice was to measure her whole state at this point, resulting in a measurement outcome $X_A \in \{0,1\}^N$. Observe that by the law of total probability,

$$2^{-N} = 2^{-\mathrm{H}_\infty(X_A)_\rho} = \sum_t p_t \cdot 2^{-\mathrm{H}_\infty(X_A|T=t)_{\rho^t}},$$

where $2^{-\mathrm{H}_\infty(X_A|T=t)_{\rho^t}}$ gives the maximal probability of guessing X_A given $T=t$ when X_A was obtained by measuring $\rho^t_{A^N}$. It holds by Markov's inequality that

$$\sum_t p_t \cdot [\mathrm{H}_\infty(X_A \mid T=t)_{\rho^t} \leq N - (\alpha N)] \leq 2^{-\alpha N}$$

where $[\cdot]$ is the Iverson bracket which evaluates to 1 if the contents is true and to 0 otherwise. In other words, the values of t for which $\mathrm{H}_\infty(X_A \mid T=t)_{\rho^t}$ is less than $(1-\alpha)N$ have combined probability less than $2^{-\alpha N}$. Now, Alice does not measure her whole state, but instead only those positions that do not belong to t, so let $X_A^{\bar{t}}$ be the outcome of measuring the qubits outside of t and let X_A^t be the outcome for the positions in t. The following holds except with negligible probability over the choice of t:

$$\mathrm{H}_\infty(X_A^{\bar{t}} \mid T=t) \geq \mathrm{H}_\infty(X_A \mid T=t, X_A^t) \geq (1-\alpha-\beta)N \tag{5}$$

where the last inequality follows from the chain rule for the min-entropy with $\mathrm{H}_0(X_A^t) = \beta N$.

To deal with (2), observe that

$$2^{-\mathrm{H}_\infty(X_A^{\bar{t}}|T=t,\mathrm{acc})} \leq 2^{-\mathrm{H}_\infty(X_A^{\bar{t}}|T=t)} / \Pr[\mathrm{acc}] \leq 2^{-\mathrm{H}_\infty(X_A^{\bar{t}}|T=t)+\alpha N} \tag{6}$$

whenever $\Pr[\mathrm{acc}] \geq 2^{-\alpha N}$.

We can conclude that, except with negligible probability upper bounded by $2 \cdot 2^{-\alpha N}$, the min-entropy of Alice's output is

$$\mathrm{H}_\infty(X_A^{\bar{t}} \mid T=t, \mathrm{acc}) \geq (1-2\alpha-\beta)N$$

by combining the bounds (5) and (6) and the respective probabilities that these bounds hold. The statement is satisfied by choosing α and β such that $\gamma = 2\alpha+\beta$ and noting that $N > n$. □

We rely on the next Lemma to lower-bound the amount of min-entropy in the measurement outcome of Bob. It says that if the joint state of Alice and Bob lives in a quantum Hamming ball of small radius around n copies of an EPR pair, then Bob's reduced density operator has high min-entropy.

Lemma 3. *Let $\epsilon > 0$ and $|\sigma_{RP^nS^n}\rangle \in \mathcal{H}_R \otimes \Delta_{\epsilon n}(|\Phi^+\rangle^{\otimes n}_{P^nS^n})$. It holds that*

$$\mathrm{H}_\infty(S^n)_\sigma \geq (1-\epsilon-h(\epsilon))n.$$

Proof. Let $\Pi_\epsilon = \{E \subseteq [n] : |E| \leq \epsilon n\}$ and let $\mathbb{P}^{\epsilon n, |\Phi^+\rangle}_{P^nS^n} = \sum_{E \in \Pi_\epsilon} \mathbb{P}^E_{P^nS^n}$ be the projector onto $\Delta_{\epsilon n}(|\Phi^+\rangle^{\otimes n}_{P^nS^n})$ where

$$\mathbb{P}^E_{P^nS^n} = \bigotimes_{i \in E} (\mathbb{1} - |\Phi^+\rangle\langle\Phi^+|)_{P_iS_i} \bigotimes_{i \notin E} |\Phi^+\rangle\langle\Phi^+|_{P_iS_i}.$$

Define $|\tilde{\sigma}^E_{RP^nS^n}\rangle = (\mathbb{1}_R \otimes \mathbb{P}^E_{P^nS^n})|\sigma_{RP^nS^n}\rangle$ for each $E \in \Pi_\epsilon$. It holds by Proposition 2 that

$$\sigma_{RP^nS^n} = \sum_{E,E' \in \Pi_\epsilon} |\tilde{\sigma}^E_{RP^nS^n}\rangle\langle\tilde{\sigma}^{E'}_{RP^nS^n}| \leq 2^{h(\epsilon)n} \sum_{E \in \Pi_\epsilon} |\tilde{\sigma}^E_{RP^nS^n}\rangle\langle\tilde{\sigma}^E_{RP^nS^n}|$$

because the set Π_ϵ contains at most $2^{h(\epsilon)n}$ elements. Furthermore, we know by the definition of $|\tilde{\sigma}^E_{RP^nS^n}\rangle$ that

$$\frac{\tilde{\sigma}^E_{S^n}}{\|\tilde{\sigma}^E_{S^n}\|_1} = \left(\bigotimes_{i \notin E} \frac{\mathbb{1}_{S_i}}{2}\right) \otimes \psi_{S_E} \leq 2^{-n+|E|}\mathbb{1}_{S^n}$$

for some normalized state ψ_{S_E} living on register $S_E = \bigotimes_{i \in E} S_i$. Since $|E| \leq \epsilon n$, it directly follows that

$$\sigma_{S^n} \leq 2^{h(\epsilon)n} \sum_{E \in \Pi_\epsilon} \tilde{\sigma}^E_{S^n} \leq 2^{-(1-\epsilon-h(\epsilon))n}\mathbb{1}_{S^n}$$

and we can thus conclude that $\mathrm{H}_\infty(S^n)_\sigma \geq (1-\epsilon-h(\epsilon))n$. □

Lower-bounding Bob's output min-entropy is essentially applying Lemma 3 to Bob's state after the sampling step of protocol of Fig. 3 which can be approximated by an ideal state by means of our main result (Theorem 1).

Lemma 4 (Entropy of Bob's output). *If Bob follows the protocol, for any $\gamma > 0$, his output $X_B \in \{0,1\}^n$ satisfies*

$$\mathrm{H}_\infty(X_B) \geq (1-\gamma)n,$$

except with probability negligible in n.

Proof. The security of the protocol against dishonest Alice is almost a direct consequence of our quantum sampling result (Theorem 1). Let $\rho_{B^n} \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$ be the normalized state of Bob after step 2 of the protocol of Fig. 3 given that Bob did not reject and let P_{acc} be the probability that he did not reject the sampling. By Theorem 1, it holds that for any $\epsilon > 0$ there exists an ideal ψ_{B^n} and an operator σ_{B^n} with negligible norm such that

$$\rho_{B^n} \leq P_{\mathrm{acc}}^{-1}(c_{N,d^2}\psi_{B^n} + \sigma_{B^n}). \tag{7}$$

Let $\tilde{\psi}_{B^n} = \frac{c_{N,d^2}}{P_{\mathrm{acc}}} \cdot \psi_{B^n}$. Then

$$\left\| \frac{c_{N,d^2}}{P_{\mathrm{acc}}}(\psi_{B^n} + \sigma_{B^n}) - \tilde{\psi}_{B^n} \right\|_1 = \frac{1}{P_{\mathrm{acc}}}\|\sigma_{B^n}\|_1,$$

which is negligible in N whenever P_{acc} is non-negligible. It follows that except with negligible probability, the right-hand side of (7) will behave exactly like

$\tilde{\psi}_{B^n}$, in which case their min-entropy will be equal. This min-entropy is bounded below by

$$\mathrm{H}_\infty(\tilde{\psi}_{B^n}) = \mathrm{H}_\infty(\psi_{B^n}) - \log \frac{c_{N,d^2}}{P_{\mathrm{acc}}} \geq (1 - \epsilon - h(\epsilon))n - \log \frac{c_{N,d^2}}{P_{\mathrm{acc}}} \tag{8}$$

by Lemma 3.

Using the bound of (8), we can claim that the min-entropy of ρ_{B^n} is lower-bounded by

$$(1 - \epsilon - h(\epsilon) - \alpha)n$$

unless one of two negligible probability events occurred. The first event is that ρ_{B^n} behaves like σ_{B^n} instead of $\tilde{\psi}_{B^n}$ and the second event is that Bob accepted the outcome of a sampling that had probability $P_{\mathrm{acc}} \leq c_{N,d^2} \cdot 2^{-\alpha n}$ of being accepted. We can conclude that the result X_B of measuring ρ_{B^n} in the computational basis will have min-entropy at least $(1 - \epsilon - h(\epsilon) - \alpha)n$, except with negligible probability. The statement follows by choosing ϵ and α in the above such that $\gamma = \epsilon + h(\epsilon) + \alpha$. □

5 Proof of Our Main Result

We now turn to the proof of our main result. In this section, we present the techniques that allow to analyze sampling protocols similar to that of Fig. 1. The key property of the sampling protocol that makes the tools of this section applicable is that it is invariant under the permutation of the sampler's register, up to an adjustment of the adversary's attack and of the output state. In order to make this more explicit, we actually consider and analyze a general class of sampling protocols that are permutation invariant and perform well on i.i.d. states, and we then show (1) that the protocol of Fig. 1 falls into that class and (2) that any protocol from that class allows us to control the post-sampling state the way we want. As an additional bonus of this modular analysis is that we can then easily extend our results to other sampling protocols. For instance, the sampling protocol of Fig. 2 for certifying EPR pairs presented in Sect. 3.1 also falls into the class of protocols that we consider. In that protocol, Paul is not asked to provide his respective parts of the EPR pairs from within the sampled subset, but he is instead asked to provide the *measurement outcome* of those, when measured in a random basis chosen and announced by Sam, and Sam compares with the corresponding measurement outcomes on his side.

5.1 Mixed State Sampling Protocols and Permutation Invariance

The general form of the sampling protocols we consider is depicted in Fig. 4. For simplicity, we assume that the protocol always outputs the same number of qudits $n = N - k$, i.e. that it lives in the Hilbert space $\mathcal{H}_S^{\otimes n}$. Note that this means that there is no freedom in the way we choose the sample t; the only permutation invariant probability distribution on the subsets of $[N]$ of size k is the uniform distribution. We also assume that k is of the order of N.

General Mixed State Sampling Protocol

1. Paul prepares $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$ and sends register S^N to Sam.
2. Sam chooses a sample $t \subset [N]$ of size k uniformly at random and a challenge c and sends both to Paul.
3. Upon reception of t and c, Paul sends back a quantum register Q.
4. Sam performs a binary outcome measurement that depends on c and t on the joint system of registers Q and S_i for $i \in t$, and accepts or rejects based on the outcome.

Fig. 4. The general form of a mixed state sampling protocol for sampling a mixed reference state φ.

The obvious example instantiation of such a sampling protocol is the sampling protocol of Fig. 1, where c is empty and Sam's measurement consists of projecting onto $|\varphi\rangle\langle\varphi|^{\otimes k}$. Another example is the one we discuss in Sect. 3.1 for certifying EPR pairs, where c then is a randomly chosen sequence of bases that specifies how Paul is supposed to measure his parts of the EPR pairs.

Clearly, for a given instantiation of the general protocol of Fig. 4, the adversary's attack strategy consists of the choice of ρ_{RS^N} and of the quantum operation (that depends on t and c) that produces Q in step 3.

We now define the notion of permutation invariance that sampling strategies must satisfy for our techniques to apply.

Definition 4 (Permutation Invariance for Sampling Protocols). *A sampling protocol that implements the framework of Fig. 4 is* invariant under the permutation of the sampler's register *if for any adversarial strategy for Paul, the completely positive trace non-increasing map $\mathcal{E}^{\text{acc}}_{RS^N \to S^n}$, which represents the output state of the sampler when he accepts, satisfies*

1. *for any input $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$ there exists $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ such that*

$$\frac{1}{n!} \sum_{\pi \in \mathcal{S}_n} |\pi\rangle\langle\pi|_\Pi \otimes \pi_{S^n} \mathcal{E}^{\text{acc}}_{RS^N \to S^n}(\rho_{RS^N}) \pi^\dagger_{S^n} = \bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}(\bar{\rho}_{P^N S^N}) \tag{9}$$

   for some symmetric purification $|\bar{\rho}_{P^N S^N}\rangle \in \text{Sym}^N(\mathcal{H}_P \otimes \mathcal{H}_S)$ of $\frac{1}{N!}\sum_{\pi \in \mathcal{S}_N} \pi_{S^N} \rho_{S^N} \pi^\dagger_{S^N}$,
2. *for any $\epsilon > 0$, $\|\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}(|\theta\rangle\langle\theta|^{\otimes N})\|_1 \leq \exp(-\Omega(N))$ whenever $F(\theta_S, \varphi_S)^2 < 1 - \epsilon$, and*
3. *$\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ acts trivially on the unsampled systems, up to reordering. Formally, $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ satisfies*

$$\text{tr}_\Pi \left(\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}(|\theta\rangle\langle\theta|^{\otimes N}_{PS}) \right) \leq \theta_S^{\otimes n}.$$

The first criterion effectively requires that any attack against the sampling protocol of Fig. 4 can be transformed into an *equivalent* attack on a symmetric state—up to a random reordering of the positions. The second criterion demands that Bob rejects with overwhelming probability in case of an "obviously bad" state, i.e., in case of i.i.d. copies of a state that is far from the reference state φ. The third criterion simply asks that the sampling protocol (and the corresponding symmetrized map $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^N S^N \to \Pi S^n}$) does not measure registers outside the sample.

From a technical perspective, the first criterion allows us to apply the observations from Sect. 2.2 to the promised symmetric state, so that we can upper bound the latter by a convex linear combination of i.i.d. states, and the second criterion then allows us to control the "bad part" of this convex linear combination (see Sect. 5.3). What then still turns out to be cumbersome to deal with is the random permutation, which got introduced by the first criterion, and to get a bound on the actual state $\mathcal{E}^{\mathrm{acc}}_{RS^N \to S^n}(\rho_{RS^N})$ instead; we show how to do this in Sect. 5.4.

We point out that the "cheap" way to deal with the random permutation would be to simply modify the sampling protocol by *really* permuting the registers at the end of the protocol, so that the permuted state *is* the final state after the sampling protocol. Besides being esthetically less appealing, because it would mean a less natural and more complicated sampling protocol than really necessary, this would also give more freedom to the party who chooses the permutation in choosing it adversarially. For instance, in our application in Sect. 4, where the final state is used to produce a high min-entropy source, we cannot allow that either player can rearrange the registers and so, say, move the zero-outputs into the positions he wants them to be.

5.2 Permutation Invariance of Our Sampling Protocols

As a first step in analyzing the sampling protocol **Purification-Based Sampling** of Fig. 1, we show that it satisfies the above definition of permutation invariance. Given that Sam's actions are obviously symmetric with respect to permuting his registers, this is probably not very surprising; spelling out the details though still turns out to be somewhat cumbersome. We therefore move the proof to Appendix A.1 and simply give a high-level proof sketch below.

Proposition 3. *The protocol* **Purification-Based Sampling** *of Fig. 1 satisfies Definition 4.*

Proof (sketch). For the first criterion, we need to argue that any adversary against the real sampling protocol can be adapted into an adversary against a symmetrized version of the protocol that will yield the same output state, up to a random permutation.

We first observe that when sampling from a permutation invariant operator, it doesn't matter which registers we sample from since the reduced density operator of any subset of k registers is the same, i.e. $\rho_{S_t} = \rho_{S_{t'}}$ for any $t, t' \subseteq [N]$ of size k. Therefore we can make the simplifying assumption that we always sample from the first k registers of S^N.

We construct the symmetric adversary: from the symmetric state $\bar{\rho}_{P^N S^N}$ from the first criterion of Definition 4, the adversary will compute the permutation $\pi \in \mathcal{S}_N$ applied on S^N. This permutation defines the set $t_\pi \subset [N]$ of positions to which π sends positions $1, \ldots, k$. The symmetric adversary will then simulate the real adversary on this sample t_π and will permute the output according to π before sending it to Sam (such that each register sent by the adversary aligns with the corresponding register on Sam's side).

The second criterion follows from the observation that the maximal probability of measuring $|\varphi\rangle\langle\varphi|^{\otimes k}$ in the sampling protocol on input $|\theta\rangle\langle\theta|^{\otimes N}$ is the fidelity between $\theta^{\otimes k}$ and $\varphi^{\otimes k}$ which is negligible in k when $F(\theta_S, \varphi_S)^2 < 1 - \epsilon$.

The third criterion follows from the fact that the unsampled positions are untouched in both the real and the symmetrized protocols. □

The following proposition allows us to apply the techniques of this section to the LOCC sampling protocol presented in Fig. 2. Its proof can be found in Appendix A.2.

Proposition 4. *The sampling protocol* **EPR-LOCC Sampling** *from Fig. 2 satisfies Definition 4.*

Proof (sketch). We need to argue that the protocol is permutation invariant in the sense of Definition 4, and that it performs well on i.i.d. states. The first part follows from the permutation invariance of the choice of t and c and of the measurement on the sampler's qubits. Suppose Sam was to permute his register with $\pi \in \mathcal{S}_N$ before performing the sampling. Then we can modify the adversary such that it attacks the sampling protocol with this new ordering of Sam's register: if Sam chooses sample t, announce $\pi(t)$ to Paul instead, the same goes for c. Let x be Paul's message to Sam, then permute x such that it aligns correctly with the corresponding qubits on Sam's register. The probability of accepting is exactly the same and the output of the protocol will be shuffled according to π's action on the unsampled qubits.

The second criterion follows from the fact that the only state that is perfectly correlated in both the computational and the diagonal bases is the EPR pair $|\Phi^+\rangle$. Therefore if all of Paul and Sam's measurement outcomes are perfectly correlated in the randomly chosen basis, it should hold that they shared states close to perfect EPR pairs. More precisely, if they share a state $|\theta\rangle^{\otimes N}$ where each θ has fidelity at most $1 - \epsilon$ with $|\Phi^+\rangle$, then their outputs cannot be perfectly correlated in at least one of the bases, except with negligible probability. The third criterion follows trivially from the fact that the unsampled qubits are not measured or acted upon. □

5.3 Proof of Sampling Against Symmetric Adversaries

By considering sampling protocols that are permutation invariant in the sense of Definition 4, we can use the specific properties of symmetric states to upper-bound the failure probability of such protocols for symmetric adversaries (adversaries which prepare a state $|\bar{\rho}_{P^N S^N}\rangle$ that lives in the symmetric subspace $\mathrm{Sym}^N(\mathcal{H}_P \otimes \mathcal{H}_S)$).

Lemma 5 below shows that since symmetric states are approximated by a mixture of i.i.d. states, then the output of the sampling executed on such a mixture is approximated by a mixture of states i.i.d. in states that are close to the reference state φ.

Lemma 5. *Let $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}$ be the output of a sampling protocol that satisfies Definition 4 and let $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$. For any $\epsilon > 0$ there exists a subnormalized measure $d\theta_S$ on the set of mixed states $\theta_S \in \mathcal{D}(\mathcal{H}_S)$ which satisfy $F(\theta_S, \varphi_S)^2 \geq 1-\epsilon$ and an operator $\tilde{\sigma}_{S^n}$ such that*

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{S^n}\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n} \leq c_{N,d^2}\cdot\int \theta_{S^n}^{\otimes n} d\theta_S + \tilde{\sigma}_{S^n} \tag{10}$$

and $\|\tilde{\sigma}_{S^n}\|_1 \leq \exp(-\Omega(N))$, where c_{N,d^2} is the dimension of $\mathrm{Sym}^N(\mathcal{H}_P\otimes\mathcal{H}_S)$.

Proof. By Definition 4, there exists $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}$ and $\bar{\rho}_{P^NS^N} \in \mathrm{Sym}^N(\mathcal{H}_P\otimes\mathcal{H}_S)$ such that

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} |\pi\rangle\langle\pi|_\Pi \otimes \pi_{S^n}\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n} = \bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}(\bar{\rho}_{P^NS^N}). \tag{11}$$

Therefore it suffices to prove the statement for $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to S^n}$ obtained by tracing out the register Π from the output of $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}$.

Since $|\bar{\rho}_{P^NS^N}\rangle \in \mathrm{Sym}^N(\mathcal{H}_P\otimes\mathcal{H}_S)$, it holds by Remark 2 that $\bar{\rho}_{P^NS^N} \leq c_{N,d^2}\cdot\int |\theta\rangle\langle\theta|^{\otimes N}_{P^NS^N}\, d|\theta_{PS}\rangle$ where $d|\theta_{PS}\rangle$ is the normalized Haar measure on the set of pure states on $\mathcal{H}_P\otimes\mathcal{H}_S$. It follows that

$$\begin{aligned}
\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to S^n}(\bar{\rho}_{P^NS^N}) &\leq \bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to S^n}\left(c_{N,d^2}\cdot\int |\theta\rangle\langle\theta|^{\otimes N}_{P^NS^N}\, d|\theta\rangle\right)\\
&= c_{N,d^2}\cdot\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to S^n}\Bigg(\int_{\theta_S\approx^\epsilon\varphi_S} |\theta\rangle\langle\theta|^{\otimes N}_{P^NS^N}\, d|\theta\rangle\\
&\qquad\qquad + \int_{\theta_S\not\approx^\epsilon\varphi_S} |\theta\rangle\langle\theta|^{\otimes N}_{P^NS^N}\, d|\theta\rangle\Bigg)\\
&\leq c_{N,d^2}\cdot\int_{\theta_S\approx^\epsilon\varphi_S} \theta_{S^n}^{\otimes n}\, d\theta_S + \tilde{\sigma}_{S^n}
\end{aligned}$$

where $\theta_S \approx^\epsilon \varphi_S$ means that $F(\theta_S,\varphi_S)^2 \geq 1-\epsilon$ and where the operator $\tilde{\sigma}_{S^n} := c_{N,d^2}\cdot\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to S^n}\left(\int_{\theta\not\approx^\epsilon\varphi} |\theta\rangle\langle\theta|^{\otimes N} d|\theta\rangle\right)$ satisfies $\|\tilde{\sigma}_{S^n}\|_1 \leq \exp(-\Omega(N))$ by the second criterion of Definition 4. The last inequality of the above follows from the third criterion of Definition 4 and from Remark 3: since the trace non-increasing map $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to S^n}$ does not act on the unsampled qubits, the state of S^n *after* the application of this map is upper-bounded by the state of the unsampled qubits *before* its application.

Finally, the measure $d\theta_S$ is obtained by taking the partial trace over P on the measure $d|\theta_{PS}\rangle$ on the restricted set of $|\theta_{PS}\rangle$ where $F(\theta_S,\varphi_S)^2 \geq 1-\epsilon$. This corresponds to a measure proportional to the Hilbert-Schmidt measure [25,31] over density operators on $\mathcal{H}_S$ which have fidelity squared at least $1-\epsilon$ with φ_S. □

From the above Lemma, we can conclude that the *permuted* output of the sampling protocol is upper bounded by an ideal state in the spirit of (3).

Corollary 1. *Let $\mathcal{E}^{\text{acc}}_{RS^N\to S^n}$ be the output of a sampling protocol that satisfies Definition 4 and let $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$. For any $\epsilon > 0$, there exist a subnormalized ϵ-ideal operator $\psi_{S^n} \in \mathcal{D}_{\leq}(\mathcal{H}_S^{\otimes n})$ and σ_{S^n} such that*

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{S^n}\mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n} \leq c_{N,d^2}\cdot\psi_{S^n} + \sigma_{S^n} \tag{12}$$

where $\|\sigma_{S^n}\|_1 \leq \exp(-\Omega(N))$.

Proof. Fix $\beta = \epsilon/2$ and let $d\theta_S$ and $\tilde{\sigma}_{S^n}$ be as in Lemma 5 for parameter β, i.e. such that

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{S^n}\mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n} \leq c_{N,d^2}\cdot\int \theta_{S^n}^{\otimes n} d\theta_S + \tilde{\sigma}_{S^n} \tag{13}$$

where $d\theta_S$ is a subnormalized measure on the set of mixed states which satisfy $F(\theta_S,\varphi_S)^2 \geq 1-\beta$ and where $\tilde{\sigma}_{S^n}$ has negligible norm.

Let $\tau_{P^nS^n} := \int |\theta\rangle\langle\theta|^{\otimes n}_{P^nS^n} d\theta_S$ be an extension of $\int \theta^{\otimes n}_{S^n} d\theta_S$ where each $|\theta_{PS}\rangle$ is such that $|\langle\theta_{PS}|\varphi_{PS}\rangle|^2 = F(\theta_S,\varphi_S)^2 \geq 1-\beta$ and let $\tilde{\sigma}_{P^nS^n}$ be an extension of $\tilde{\sigma}_{S^n}$. Then from Lemma 1, we have

$$\operatorname{tr}\left(\left(\mathbb{1} - \mathbb{P}^{2\beta n,|\varphi\rangle}_{P^nS^n}\right)(\tau_{P^nS^n})\right) \leq \exp(-2\beta^2 n). \tag{14}$$

Choose $\psi_{S^n} = \operatorname{tr}_{P^n}(\mathbb{P}^{2\beta n,|\varphi\rangle}_{P^nS^n}\tau_{P^nS^n}\mathbb{P}^{2\beta n,|\varphi\rangle}_{P^nS^n})$. Then, using (13), we have

$$\begin{aligned}\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{S^n}\mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n} &\leq c_{N,d^2}\cdot\int \theta_{S^n}^{\otimes n} d\theta_S + \tilde{\sigma}_{S^n}\\ &= \operatorname{tr}_{P^n}\left(c_{N,d^2}\cdot\tau_{P^nS^n} + \tilde{\sigma}_{P^nS^n}\right) = c_{N,d^2}\cdot\psi_{S^n} + \sigma_{S^n}\end{aligned}$$

where $\sigma_{S^n} := \operatorname{tr}_{P^n}(c_{N,d^2}(\tau_{P^nS^n} - \mathbb{P}^{2\beta n,|\varphi\rangle}_{P^nS^n}\tau_{P^nS^n}\mathbb{P}^{2\beta n,|\varphi\rangle}) + \tilde{\sigma}_{P^nS^n})$ has norm upper bounded by

$$\|\sigma_{P^nS^n}\|_1 \leq c_{N,d^2}\|\tau_{P^nS^n} - \mathbb{P}^{2\beta n,|\varphi\rangle}_{P^nS^n}\ \tau_{P^nS^n}\ \mathbb{P}^{2\beta n,|\varphi\rangle}_{P^nS^n}\|_1 + \|\tilde{\sigma}_{P^nS^n}\|_1 \leq \exp(-\Omega(N))$$

by first applying the triangle inequality and then the Gentle Measurement's Lemma [21,30] with the bound of (14). □

It should be noted that the operator σ_{S^n} from the above Corollary is not positive semidefinite in general, but since its norm is negligible, this shouldn't matter because it can simply be ignored for most applications.

5.4 Proof Against Arbitrary Adversaries: Unpermuting the Output

In order to conclude that the sampling protocol works as intended on an arbitrary input state and adversarial strategy, we need to argue that if we remove the permutation from the contents of (12), then the left-hand side, which becomes the post-sampling state, is still approximated by a state having a purification in a low-error subspace. It turns out that the intuitive statement "if the permuted output is ideal then the non-permuted output is also ideal" that we want to show is quite tricky to prove. We stress that this step is necessary if we want to keep the permutation "under the hood" and have a statement that doesn't require to physically shuffle the systems, which would lead to unnatural sampling protocols.

Lemma 6 below is the first step in this proof, it shows that the property of having a purification in a low-error subspace, i.e. of being *ideal*, does indeed persist after "unpermutation" of the registers.

Lemma 6. *Let $\epsilon > 0$ and let $\sigma_{S^n} \in \mathcal{D}(\mathcal{H}_S^{\otimes n})$ be such that $\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{S^n}\sigma_{S^n}\pi_{S^n}^\dagger$ is ϵ-ideal, then σ_{S^n} is also ϵ-ideal.*

Proof. Let $r = \epsilon n$. We need to show that if $\bar{\sigma}_{S^n} := \frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{S^n}\sigma_{S^n}\pi_{S^n}^\dagger$ has a purification in $\mathcal{H}_R \otimes \Delta_r(|\varphi\rangle_{P^nS^n}^{\otimes n})$ for some register R, then σ_{S^n} also has a purification in $\mathcal{H}_R \otimes \Delta_r(|\varphi\rangle_{P^nS^n}^{\otimes n})$. Let $|\bar{\sigma}_{RP^nS^n}\rangle \in \mathcal{H}_R \otimes \Delta_r(|\varphi\rangle_{P^nS^n}^{\otimes n})$ be the purification of $\bar{\sigma}_{S^n}$ that exists by assumption and let $\sum_i p_i|i_{S^n}\rangle\langle i_{S^n}|$ be the spectral decomposition of σ_{S^n}. Define the pure state

$$|\bar{\sigma}_{\Pi P^nS^n}\rangle = \sqrt{\frac{1}{n!}}\sum_{\pi\in\mathcal{S}_n} |\pi\rangle_\Pi \otimes \left(\sum_i \sqrt{p_i}|i_{P^n}\rangle \otimes \pi_{S^n}|i_{S^n}\rangle\right)$$

where $\{|i_{P^n}\rangle\}_i$ is an orthonormal basis of $\mathcal{H}_{P^n}$. Note that this state is a purification of $\bar{\sigma}_{S^n}$, so there exists an isometry $V_{\Pi P^n\to RP^n}$ such that $V_{\Pi P^n\to RP^n}|\bar{\sigma}_{\Pi P^nS^n}\rangle = |\bar{\sigma}_{RP^nS^n}\rangle \in \mathcal{H}_R \otimes \Delta_r(|\varphi\rangle_{P^nS^n}^{\otimes n})$. We can express $|\bar{\sigma}_{RP^nS^n}\rangle$ as:

$$\begin{aligned}
&|\bar{\sigma}_{RP^nS^n}\rangle = (V_{\Pi P^n\to RP^n} \otimes \mathbb{1}_{S^n})|\sigma_{\Pi P^nS^n}\rangle \\
&= \sum_{\pi,i}\sqrt{\frac{p_i}{n!}}V_{\Pi P^n\to RP^n}|\pi\rangle_\Pi|i_{P^n}\rangle \otimes \pi_{S^n}|i_{S^n}\rangle = \sum_{\pi,i}\sqrt{\frac{p_i}{n!}}|\xi_{\pi,i}\rangle_{RP^n} \otimes \pi_{S^n}|i_{S^n}\rangle
\end{aligned}$$

where the vectors $|\xi_{\pi,i}\rangle_{RP^n} := V_{\Pi P^n\to RP^n}|\pi\rangle_\Pi|i_{P^n}\rangle$ are orthogonal to each other. Then by acting on this state with an isometry that extracts π from registers RP^n and that undoes π on registers P^n and S^n, we get

$$\sum_{\pi,i}\sqrt{\frac{p_i}{n!}}(\mathbb{1}_R \otimes \pi_{P^n}^{-1})|\xi_{\pi,i}\rangle_{RP^n} \otimes |i_{S^n}\rangle$$

Note that both before and after this isometry is applied, the state of registers P^n and S^n has support in $\Delta_r(|\varphi\rangle_{P^nS^n}^{\otimes n})$ because this subspace is invariant under permutation of these registers. The proof is then completed since the above state is a purification of σ_{S^n} that lies in $\mathcal{H}_R \otimes \Delta_r(|\varphi\rangle_{P^nS^n}^{\otimes n})$. □

We now have all the tools we need to prove our main result, Theorem 2 below. Its proof combines the above lemma with Lemmas 1 and 5 to show that the output of the sampling is negligibly close to a state that is post-selected from a purification of an ideal state.

Theorem 2 (Main Result). *Let $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}$ be the output of a sampling protocol that satisfies Definition 4 and let $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$. For any $\epsilon > 0$, there exists a non-normalized vector*

$$\left|\tilde{\psi}_{R'P^nS^n}\right\rangle \in \mathcal{H}_{R'} \otimes \Delta_{\epsilon n}(|\varphi\rangle^{\otimes n}_{P^nS^n})$$

and a completely positive trace non-increasing superoperator $\tilde{\mathcal{K}}_{R'P^n\to\mathbb{C}}$ such that

$$\left\|\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N}) - c_{N,d^2}(\tilde{\mathcal{K}}_{R'P^n} \otimes \mathrm{id}_{S^n})(\tilde{\psi}_{R'P^nS^n})\right\|_1 \leq \exp(-\Omega(N))$$

By means of Proposition 1 and Remark 3, we can express the statement of Theorem 2 in terms of an operator inequality as suggested in (3), rather than by means of post-selection.

Corollary 2. *Let $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}$ be the output of a sampling protocol that satisfies Definition 4 and let $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$. For any $\epsilon > 0$, there exist a sub-normalized ϵ-ideal operator $\psi_{S^n} \in \mathcal{D}_{\leq}(\mathcal{H}_S^{\otimes n})$ and σ_{S^n} such that*

$$\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N}) \leq c_{N,d^2} \cdot \psi_{S^n} + \sigma_{S^n}$$

where $\|\sigma_{S^n}\|_1 \leq \exp(-\Omega(N))$.

Proof (of Theorem 2). Let ψ_{S^n} and σ_{S^n} be as in the statement of Corollary 1, i.e. such that

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{S^n}\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n} \leq c_{N,d^2} \cdot \psi_{S^n} + \sigma_{S^n} \tag{15}$$

and define $\tau_{S^n} := \psi_{S^n} + c^{-1}_{N,d^2} \cdot \sigma_{S^n}$. Since ψ_{S^n} is ϵ-ideal, let $|\psi_{R'P^nS^n}\rangle$ be the purification of ψ_{S^n} that lives in the low error subset $\mathcal{H}_{R'} \otimes \Delta_{\epsilon n}(|\varphi\rangle^{\otimes n}_{P^nS^n})$. Let $|\tau_{R'P^nS^n}\rangle$ be a purification[3] of τ_{S^n} such that $\|\psi_{R'P^nS^n} - \tau_{R'P^nS^n}\|_1 \leq \exp(-\Omega(N))$. From (15) and Proposition 1 we can show that there exists a trace non-increasing completely positive map $\mathcal{K}_{R'P^n\to\Pi}$ that produces a classical register Π from purification registers $R'P^n$ with the property that

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} |\pi\rangle\langle\pi|_\Pi \otimes \pi_{S^n}\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n} = c_{N,d^2}(\mathcal{K}_{R'P^n\to\Pi} \otimes \mathrm{id}_{S^n})(\tau_{R'P^nS^n}).$$

[3] The existence of a purification of τ_{S^n} with this property can be argued by using Uhlmann's Theorem: since τ_{S^n} is close in fidelity to ψ_{S^n}, for any purification $|\psi_{R'P^nS^n}\rangle$ of ψ_{S^n}, there exists a purification $|\tau_{R'P^nS^n}\rangle$ that is also close to $|\psi_{R'P^nS^n}\rangle$.

Suppose now we were to submit both sides of the above equality to the following quantum operation: measure register Π and undo the observed permutation on register S^n. The left-hand side of the above would become $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})$ whereas the right-hand side becomes

$$c_{N,d^2}\cdot\sum_{\pi\in\mathcal{S}_n}(\langle\pi|_\Pi\otimes\pi^{-1}_{S^n})(\mathcal{K}_{R'P^n\to\Pi}\otimes\mathrm{id}_{S^n})(\tau_{R'P^nS^n})(|\pi\rangle_\Pi\otimes(\pi^{-1}_{S^n})^\dagger).$$

We now show how to represent this operator in a way that corresponds to the statement we need to prove, i.e. as post-selected from a rank-one operator living almost entirely in the low-error subspace. To this end, define[4] an isometry $U_{R'P^n\to Z\Pi}$ that purifies the action of $\mathcal{K}_{R'P^n\to\Pi}$, i.e. such that for any $\nu_{R'P^n}$,

$$\mathcal{K}_{R'P^n\to\Pi}(\nu_{R'P^n}):=\mathrm{tr}_Z\left((\mathbb{P}_Z\otimes\mathbb{1}_\Pi)\cdot U_{R'P^n\to Z\Pi}\cdot\nu_{R'P^n}\cdot(U_{R'P^n\to Z\Pi})^\dagger\right)$$

for some projector $\mathbb{P}_Z$. Using this representation, the post-sampling operator can be expressed as

$$\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})=c_{N,d^2}\cdot\mathrm{tr}_Z\left((\mathbb{P}_Z\otimes\mathbb{1}_{S^n})\cdot\sum_{\pi\in\mathcal{S}_n}[U^\pi_{R'P^n\to Z}\otimes\pi^{-1}_{S^n}](\tau_{R'P^nS^n})\right)\tag{16}$$

where $U^\pi_{R'P^n\to Z}:=(\mathbb{1}_Z\otimes\langle\pi|_\Pi)\cdot U_{R'P^n\to Z\Pi}$ and where $[U](\rho)$ is short for $U\rho U^\dagger$.

Define the operator

$$\tilde{\psi}_{ZS^n}:=\sum_{\pi\in\mathcal{S}_n}(U^\pi_{R'P^n\to Z}\otimes\pi^{-1}_{S^n})\psi_{R'P^nS^n}(U^\pi_{R'P^n\to Z}\otimes\pi^{-1}_{S^n})^\dagger.$$

where $\psi_{R'P^nS^n}$ is the purification of ψ_{S^n} defined earlier. It isn't too hard to show that $\tilde{\psi}_{S^n}$ is such that $\psi_{S^n}=\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n}\pi_{S^n}\tilde{\psi}_{S^n}\pi^\dagger_{S^n}$. Since ψ_{S^n} has a purification in the low-error subspace, Lemma 6 implies that $\tilde{\psi}_{S^n}$ itself admits a purification in this subspace. Let $|\tilde{\psi}_{R'P^nS^n}\rangle$ be this purification and let $\tilde{\mathcal{K}}_{R'P^n\to\mathbb{C}}$ be the superoperator that first maps $|\tilde{\psi}_{R'P^nS^n}\rangle$ to $\tilde{\psi}_{ZS^n}$ and then applies $\sigma_Z\mapsto\mathrm{tr}_Z(\mathbb{P}_Z\sigma_Z)$ to register Z. Then, using the definition of $\tilde{\psi}_{R'P^nS^n}$ and $\tilde{\mathcal{K}}_{R'P^n}$, and since completely positive trace non-increasing maps cannot increase the trace distance,

[4] It is always possible to define such an isometry and projector for any trace non-increasing completely positive superoperator $\mathcal{E}_{A\to B}$. To see this, let $\mathcal{E}(\sigma_A)=\sum_k E_k\sigma_A E_k^\dagger$ where $E_k\in L(\mathcal{H}_A,\mathcal{H}_B)$ are the Kraus operators of $\mathcal{E}$ and define the isometry $U_{A\to BZ}$ as mapping an arbitrary state $|\psi\rangle_A$ to $\sum_k E_k|\psi\rangle_A|k\rangle_Z+\sqrt{\mathbb{1}-\sum_k E_k^\dagger E_k}|\psi\rangle_A|\perp\rangle_Z$ where $|\perp\rangle_Z$ is orthogonal to $|k\rangle_Z$ for every k. Then $\mathbb{P}_Z=\sum_k|k\rangle\langle k|_Z$ suffices as the required projector since $\mathrm{tr}_Z((\mathbb{1}_B\otimes\mathbb{P}_Z)U_{A\to BZ}\sigma_A U^\dagger_{A\to BZ})=\sum_k E_k\sigma_A E_k^\dagger=\mathcal{E}_{A\to B}(\sigma_A)$.

$$\begin{aligned}
&\|\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N}) - c_{N,d^2}(\tilde{\mathcal{K}}_{R'P^n}\otimes \mathrm{id}_{S^n})(\tilde{\psi}_{R'P^nS^n})\|_1 \\
&\qquad = \Bigg\| c_{N,d^2}\cdot \mathrm{tr}_Z\Bigg(\mathbb{P}_Z\otimes \mathbb{1}_{S^n})\cdot \\
&\qquad\qquad \sum_{\pi\in\mathcal{S}_n}[U^{\pi}_{R'P^n\to Z}\otimes \pi^{-1}_{S^n}]\Big(\tau_{R'P^nS^n}-\psi_{R'P^nS^n}\Big)\Bigg)\Bigg\|_1 \\
&\qquad \le c_{N,d^2}\cdot \|\tau_{R'P^nS^n}-\psi_{R'P^nS^n}\|_1 \\
&\qquad \le \exp(-\Omega(N))
\end{aligned}$$

where in the first inequality $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})$ is replaced with (16) and the last inequality follows from our choice of $|\tau_{R'P^nS^n}\rangle$. □

6 Conclusion and Open Questions

Statistical sampling is a natural task that is well understood from a classical perspective. Classical tools such as Hoeffding's inequality, Azuma's inequality and other results on concentration of measure that are used to analyze classical sampling (and quantum sampling to a certain degree [6]) are of no use when trying to sample from quantum data with a *mixed* reference state. The tools of symmetric invariance can substitute the classical tools up to a certain degree when analyzing fully quantum sampling protocols. We have introduced a framework for sampling mixed states by presenting a general sampling protocol and we have shown that if an instantiation of that general protocol respects simple criteria, then it can be used to certify that a quantum population is close to an n-fold tensor product of a reference state φ in an adversarial setting.

We have also shown that this result can be applied to yield a two-party randomness generation protocol. While perfect coin tossing is impossible without assumptions, we can achieve the "next best thing" by producing a string that has an almost-maximal min-entropy from the point of view of both participants.

Sampling of a quantum population is a new concept and many questions are left unanswered, especially when sampling with a mixed reference state where the usual (classical) tools do not apply. Precisely, future directions for this work include:

1. A formulation of our results where a conclusion can be made when an error rate significantly larger than 0 has been observed. From an observed error rate of $\delta > 0$ within the sample, we would want to conclude that the state of the remaining positions can be controlled by means of an $(\varepsilon+\delta)$-ideal state for small $\varepsilon > 0$.
2. An extension of our results to multiple reference states for the same population instead of a fixed reference state φ, e.g. with reference states φ_0, φ_1 where register i of the population is tested against φ_{x_i} for $x \in \{0,1\}^n$. While sampling according to an arbitrary (pure) reference state is given "for free" for pure state sampling (since all pure states are related by a unitary transformation on the sampler's register), it requires more work in the case of mixed state sampling.

3. On top of the previous point, it is often useful for quantum sampling applications to have a statement in terms of an *adaptive* sampling protocol where the reference states (i.e. the bits of x) are chosen adaptively by the adversary based on what positions were sampled. Such an extension would have applications in two-party cryptography where sampling is done in a sequential manner using a 1- or 2-bit cryptographic primitive, such as cut-and-choose. In fact, if our results were extended in such a way, it would allow to certify states with a 2-bit description (such as the BB84 encoding) using a 1-bit cut-and-choose, a task that is not known to be possible relying on existing sampling tools. The pure-state sampling framework of [6] was shown to apply in the adaptive setting in [12].

Acknowledgments. FD acknowledges funding from GAČR grant GA16-22211S, and LS is funded by NSERC discovery and acceleration to discovery grants.

A Permutation Invariance of Sampling Protocols

A.1 Proof of Proposition 3

We can assume w.l.o.g. that the state $\rho_{RS^N} \in \mathcal{D}(\mathcal{H}_R \otimes \mathcal{H}_S^{\otimes N})$ is pure and that adversarial strategies against the protocol depicted in Fig. 1 is described by a family of isometries of the form $U^t_{R\to R'P^k}$ for $t \subseteq [N]$ of size k, where P^k represents the register sent to Sam and supposed to contain the purifications of φ_S, and R' is a register kept by Paul.

For convenience, define the isometry $V^t_{S^N\to S^nS^k}$ that, for any $t \subseteq [N]$, maps subsystems S_i for $i \in t$ into the last k subsystems (denoted S^k) and subsystems S_i for $i \notin t$ into the first $n = N - k$ subsystems (denoted S^n). In other words, isometry V^t_S simply groups together the registers to be sampled.

For an adversarial strategy as described above, the completely positive trace non-increasing map $\mathcal{E}^{\text{acc}}_{RS^N\to S^n}$ that maps the input state ρ_{RS^N} to the sampler's conditional output is defined by

$$\mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho_{RS^N}) := \frac{1}{\binom{N}{k}} \sum_{t\subseteq[N]} \text{tr}_{R'}\left(\langle\varphi|^{\otimes k}_{P^kS^k} \cdot [U^t_R \otimes V^t_{S^N}](\rho_{PS}) \cdot |\varphi\rangle^{\otimes k}_{P^kS^k}\right) .$$

where we left the identity operator acting on $R'S^n$ implicit and where $[U](\rho)$ is short for $U\rho U^\dagger$ for any isometry U.

The following property of $V^t_{S^N\to S^nS^k}$ will be useful for proving Lemma 7 below.

Remark 4. Let $\pi \in \mathcal{S}_N$, and let $t_\pi = \{\pi^{-1}(i) \mid i \in [k]\}$. There exist $\tau^\pi \in \mathcal{S}_k$ and $\bar{\tau}^\pi \in \mathcal{S}_n$ such that $V^{[k]}_{S^N\to S^nS^k} \cdot \pi_S = (\bar{\tau}^\pi_{S^n} \otimes \tau^\pi_{S^k}) \cdot V^{t_\pi}_{S^N\to S^nS^k}$. Furthermore, there is a one-to-one correspondence between permutations $\pi \in \mathcal{S}_N$ and triplets $(t_\pi, \tau^\pi, \bar{\tau}^\pi)$.

Lemma 7. *Protocol* **Purification-Based Sampling** *from Fig. 1 satisfies the first criterion of Definition 4.*

Proof. We need to show the existence of a completely positive trace non-increasing map $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ such that for any ρ_{RS^N},

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} |\pi\rangle\langle\pi|_{\Pi} \otimes \pi_{S'} \mathcal{E}^{\text{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^{\dagger}_{S'} = \bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}(\bar{\rho}_{P^N S^N}) \tag{17}$$

for some symmetric purification $|\bar{\rho}_{P^N S^N}\rangle$ of $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N} \pi_{S^N}\rho_{S^N}\pi^{\dagger}_{S^N}$ where $\mathcal{E}^{\text{acc}}_{RS^N\to S^n}$ is defined earlier in this section.

Let $|\bar{\rho}_{P^N S^N}\rangle \in \text{Sym}^N(\mathcal{H}_P \otimes \mathcal{H}_S)$ be an arbitrary purification of $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N} \pi_{S^N}\rho_{S^N}\pi^{\dagger}_{S^N}$. Since all purifications are equivalent up to an isometry on the purifying register, there exists an isometry $W_{P^N\to R\bar{\Pi}}$ such that

$$(W_{P^N} \otimes \mathbb{1}_{S^N})|\bar{\rho}_{P^N S^N}\rangle = \frac{1}{\sqrt{N!}}\sum_{\pi\in\mathcal{S}_n} (\mathbb{1}_R \otimes \pi_{S^N})|\rho_{RS^N}\rangle \otimes |\pi\rangle_{\bar{\Pi}}.$$

Let $\bar{U}_{P^N\to\bar{R}P^k}$ be the isometry that performs the following actions unitarily on register P^N of $|\bar{\rho}_{P^N S^N}\rangle$:

1. Apply W_{P^N}, producing registers R and $\bar{\Pi}$.
2. From permutation $\pi \in \mathcal{S}_N$ held in register $\bar{\Pi}$, compute t_π, $\tau^\pi \in \mathcal{S}_k$ and $\bar{\tau}^\pi \in \mathcal{S}_n$ as in Remark 4, i.e. such that $V^{[k]}_{S^N\to S^n S^k}\cdot\pi_S = (\tau^\pi_{\hat{S}} \otimes \bar{\tau}^\pi_{S'})\cdot V^{t_\pi}_{S^N\to S^n S^k}$.
3. Apply attack $U^{t_\pi}_{R\to R'P^k}$ on register R, producing registers R' and P^k and reorder register P^k using permutation τ^π so that each P_i aligns with the right sampled S_i.
4. Let register $\bar{R}$ be composed of registers R', $\bar{\Pi}$. Output registers P^k, $\bar{R}$ and register Π containing the permutation $\bar{\tau}^\pi$ that acts on the output S^n (i.e. on the unsampled registers).

From the definition of the above isometry,

$$\begin{aligned}&(\bar{U}_{P^N\to\bar{R}P^k} \otimes V^{[k]}_{S^N\to S^n S^k})|\bar{\rho}_{P^N S^N}\rangle \\ &= \frac{1}{\sqrt{N!}}\sum_{\pi\in\mathcal{S}_N} (\tau^\pi_{P^k} \otimes \tau^\pi_{S^k} \otimes \bar{\tau}^\pi_{S^n})(U^{t_\pi}_{R\to R'P^k} \otimes V^{t_\pi}_{S^N\to S^n S^k})|\rho_{RS^N}\rangle|\pi\rangle_{\bar{\Pi}}|\bar{\tau}^\pi\rangle_{\Pi}\end{aligned}$$

Tracing out register $\bar{\Pi}$ from the above and using the one-to-one correspondence between π and $(t_\pi, \tau^\pi, \bar{\tau}^\pi)$ to break the sum over π into sums over t, τ and $\bar{\tau}$, we get

$$\begin{aligned}&\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N} [(\tau^\pi_{P^k} \otimes \tau^\pi_{S^k} \otimes \mathbb{1}_{R'} \otimes \bar{\tau}^\pi_{S^n})(U^{t_\pi}_{R\to R'P^k} \otimes V^{t_\pi}_{S^N\to S^n S^k})](\rho_{RS^N}) \otimes |\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_{\Pi} \\ &= \frac{1}{n!}\frac{1}{k!}\frac{1}{\binom{N}{k}}\sum_{\bar{\tau}\in\mathcal{S}_n} \bar{\tau}_{S^n}\left(\sum_{\substack{\tau\in\mathcal{S}_k \\ t\subseteq[N]:|t|=k}} [(\tau_{P^k} \otimes \tau_{S^k})(U^t_R \otimes V^t_{S^N})](\rho_{RS^N})\right)(\bar{\tau}_{S^n})^{\dagger} \otimes |\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_{\Pi}\end{aligned}$$

Taking the partial inner product with $|\varphi\rangle^{\otimes k}_{P^kS^k}$ and tracing out R' leaves us with

$$\frac{1}{n!\binom{N}{k}}\sum_{\bar\tau\in\mathcal{S}_n}\bar\tau_{S^n}\left(\sum_t \mathrm{tr}_{R'}\left(\langle\varphi|^{\otimes k}_{P^kS^k}\cdot[U_R^t\otimes V_{S^N}^t](\rho_{RS^N})\cdot|\varphi\rangle^{\otimes k}_{P^kS^k}\right)\right)(\bar\tau_{S^n})^\dagger\otimes|\bar\tau^\pi\rangle\langle\bar\tau^\pi|_\Pi$$
$$=\frac{1}{n!}\sum_{\bar\tau\in\mathcal{S}_n}\bar\tau_{S^n}\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})\bar\tau^\dagger_{S^n}\otimes|\bar\tau^\pi\rangle\langle\bar\tau^\pi|_\Pi$$

where the sum over τ disappeared because $|\varphi\rangle^{\otimes k}_{P^kS^k}$ is invariant under permutation. Then $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}$ defined as

$$\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}(\bar\rho_{P^NS^N}):=\mathrm{tr}_{\bar R}\left(\langle\varphi|^{\otimes k}_{P^kS^k}\cdot[\bar U_{P^N}\otimes V^{[k]}_{S^N}](\bar\rho_{P^NS^N})\cdot|\varphi\rangle^{\otimes k}_{P^kS^k}\right).$$

satisfies (17). □

Lemma 8. *Protocol* **Purification-Based Sampling** *from Fig. 1 satisfies the second criterion of Definition 4.*

Proof. We need to show that for any $\epsilon>0$, $\|\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}(|\theta\rangle\langle\theta|^{\otimes N}_{P^NS^N})\|_1\le\exp(-\Omega(N))$ whenever $F(\theta_S,\varphi_S)^2<1-\epsilon$ where

$$\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}(\bar\rho_{P^NS^N}):=\mathrm{tr}_{\bar R}\left(\langle\varphi|^{\otimes k}_{P^kS^k}\cdot[\bar U_{P^N}\otimes V^{[k]}_{S^N}](\bar\rho_{P^NS^N})\cdot|\varphi\rangle^{\otimes k}_{P^kS^k}\right).$$

The proof is based on the simple observation that the isometry $\bar U$ that maximizes the probability of observing $|\varphi\rangle^{\otimes k}$ on registers P^kS^k is the one that matches the fidelity with $\varphi^{\otimes k}$ by the fact that the fidelity is monotonous. Therefore it holds that, since the fidelity is multiplicative for product states,

$$\|\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}\left(|\theta\rangle\langle\theta|^{\otimes N}_{P^NS^N}\right)\|_1\le F(\theta^{\otimes k}_{S^k},\varphi^{\otimes k}_{S^k})^2\le(1-\epsilon)^{2k}\le\exp(-2\epsilon k)$$

whenever $F(\theta_S,\varphi_S)^2<1-\epsilon$. □

The third criterion of Definition 4 follows trivially from the observation that neither $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}$ nor $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}$ acts on the unsampled qubits other than by rearranging them.

A.2 Proof of Proposition 4

As in Appendix A.1, let us establish that the protocol satisfies the each criterion of Definition 4.

Lemma 9 (First criterion). *Let $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}$ be the output of the sampling protocol* **EPR-LOCC Sampling** *from Fig. 2. For any $\rho_{RS^N}\in\mathcal{D}(\mathcal{H}_R\otimes\mathcal{H}_S^{\otimes N})$ there exists $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}$ such that*

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n}|\pi\rangle\langle\pi|_\Pi\otimes\pi_{S^n}\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}(\rho_{RS^N})\pi^\dagger_{S^n}=\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}(\bar\rho_{P^NS^N})\tag{18}$$

for some symmetric purification $|\bar\rho_{P^NS^N}\rangle$ of $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N}\pi_{S^N}\rho_{S^N}\pi^\dagger_{S^N}$.

Proof. Recall the linear operator $V^t_{S^N \to S^n S^k}$ from Appendix A.1 that maps S_t to S^k and $S_{\bar{t}}$ to S^n (where S^k is understood to represent the last k registers). The completely positive trace non-increasing map $\mathcal{E}^{\text{acc}}_{RS^N \to S^n}$ that models the action of the protocol on the state ρ_{RS^N} when Sam accepts can be represented as

$$2^{-k}\binom{N}{k}^{-1} \sum_{t,c,x} \operatorname{tr}_{RS^k}\left((E^{t,c}_x \otimes \mathbb{P}^{x,c}_{S^k}) V^t_{S^N \to S^n S^k} \rho_{RS^N} V^t_{S^N \to S^n S^k}\right)$$

where the sum is over $t \subset [N]$ such that $|t| = k$, $c \in \{+, \times\}^k$ and $x \in \{0,1\}^k$ and where, for t and c sent by Sam, $E^{t,c} = \{E^{t,c}_x\}_{x \in \{0,1\}^k}$ is the POVM measurement on R that produces x and $\mathbb{P}^{x,c}_{S^k} := H^{\otimes c}|x\rangle\langle x|H^{\otimes c}$ is the projector onto x in basis c.

Let $\bar{\rho}_{P^N S^N}$ be an arbitrary purification of $\frac{1}{N!}\sum_{\pi \in \mathcal{S}_N} \pi_{S^N} \rho_{S^N} \pi^\dagger_{S^N}$. Define the map $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ as follows:

1. Map state $\bar{\rho}_{P^N S^N}$ to $\frac{1}{N!}\sum_{\pi \in \mathcal{S}_N} |\pi\rangle\langle\pi|_{\bar{\Pi}} \otimes (\mathbb{1}_R \otimes \pi_{S^N})\rho_{RS^N}(\mathbb{1}_R \otimes \pi^\dagger_{S^N})$.
2. From permutation $\pi \in \mathcal{S}_N$ held in register R, compute t_π, $\tau^\pi \in \mathcal{S}_k$ and $\bar{\tau}^\pi \in \mathcal{S}_n$ as in Remark 4.
3. Apply $V^{[k]}_{S^N \to S^n S^k}$ on S^N, choose $c \in \{+, \times\}^k$ at random and apply POVM $E^{t_\pi, c}$ on R producing output x.
4. Measure the sampled registers S^k by projecting on $H^{\otimes \tau^\pi(c)}|\tau^\pi(x)\rangle_{S^k} = \tau^\pi H^{\otimes c}|x\rangle_{S^k}$.
5. Output $\bar{\tau}^\pi$ in register Π and register S^n.

The output of $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ applied on $\bar{\rho}_{P^N S^N}$ is

$$\begin{aligned}
&\frac{2^{-k}}{N!}\sum_{\pi,c,x} \operatorname{tr}_{RS^k}\left((E^{t_\pi,c}_x \otimes \tau^\pi_{S^k}\mathbb{P}^{x,c}_{S^k}(\tau^\pi_{S^k})^\dagger) \cdot [V^{[k]}_{S^N \to S^n S^k}\pi_{S^N}](\rho_{RS^N})\right) \otimes |\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi \\
&= \frac{2^{-k}}{N!}\sum_{\pi,c,x} \bar{\tau}^\pi_{S^n} \operatorname{tr}_{RS^k}\left(E^{t_\pi,c}_x \otimes \mathbb{P}^{x,c}_{S^k})[V^{t_\pi}_{S^N \to S^n S^k}](\rho_{RS^N})\right)\bar{\tau}^\pi_{S^n} \otimes |\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi \\
&= \frac{2^{-k}}{n!}\binom{N}{k}^{-1} \sum_{\bar{\tau}^\pi \in \mathcal{S}_n} [\bar{\tau}^\pi_{S^n}]\left(\sum_{t,c,x} \operatorname{tr}_{RS^k}\left((E^{t,c}_x \otimes \mathbb{P}^{x,c}_{S^k})[V^t_{S^N}](\rho_{RS^N})\right)\right) \otimes |\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi \\
&= \frac{1}{n!}\sum_{\bar{\tau}^\pi \in \mathcal{S}_n} \bar{\tau}^\pi_{S^n} \mathcal{E}^{\text{acc}}_{RS^N \to S^n}(\rho_{RS^N})\bar{\tau}^\pi_{S^n} \otimes |\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi
\end{aligned}$$

where the second equality uses Remark 4. □

Lemma 10 (Second criterion). *Let $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ be as in the proof of Lemma 9. For any $\epsilon > 0$, $\|\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}(|\theta\rangle\langle\theta|^{\otimes N}_{P^N S^N})\|_1 \leq \exp(-\Omega(N))$ whenever $F(\theta_S, \varphi_S)^2 < 1 - \epsilon$.*

Proof. For any $c \in \{+, \times\}^k$, let $\bar{E}^c_x$ be the POVM element on P^N that gives the probability of x being outputted in Step 3 of $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ when c is chosen in the same step. In essence, $\bar{E}^c_x$ is to $\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}$ what $E^{t_\pi,c}$ is to $\mathcal{E}^{\text{acc}}_{RS^N \to S^n}$; it gives the probability of observing x when the following measurement is done on

P^N: produce registers $\bar{\Pi}R$ from P^N, measure π from register $\bar{\Pi}$, compute the corresponding sample t_π, and apply the measurement corresponding to POVM $E^{t_\pi,c}$.

Using these POVM operators $\bar{E}_x^c$, we can express the norm we wish to upper-bound as

$$\|\bar{\mathcal{E}}^{\text{acc}}_{P^N S^N \to \Pi S^n}(|\theta\rangle\langle\theta|^{\otimes N}_{P^N S^N})\|_1 = 2^{-k}\sum_{c,x} \text{tr}\left((\bar{E}_x^c \otimes \mathbb{P}^{x,c}_{S^k} \otimes \mathbb{1}_{S^n})|\theta\rangle\langle\theta|^{\otimes N}_{P^N S^N}\right) \quad (19)$$

where $\mathbb{P}^{x,c}_{S^k}$ is the projector onto x in basis c. Note that the right-hand side of (19) can be interpreted as the probability of guessing the outcome of measuring register S^k in a known but random basis c by observing the reduced operator of register P^N. We now analyze this guessing probability to provide an upper-bound on (19).

Since each measurement on S^k is independent of each other and since the joint state is in an i.i.d. form, the probability of Paul guessing outcome x is of the form γ^k where γ corresponds to the probability of guessing a single bit of x. This probability is given by the expression

$$\gamma = \frac{1}{2}\Pr(\text{guess } X \mid C = +) + \frac{1}{2}\Pr(\text{guess } X \mid C = \times)$$

We show that at least one of the above conditional term is bounded above by a constant strictly smaller than 1 when $F(\theta_S, \varphi_S) < 1 - \epsilon$, which means that γ^k is negligible in k.

The maximum probability of guessing X when $C = +$ is given by the probability of distinguishing states

$$\left|\theta_P^0\right\rangle = (\mathbb{1}_p \otimes \langle 0|_S)|\theta_{PS}\rangle \text{ and } \left|\theta_P^1\right\rangle = (\mathbb{1}_p \otimes \langle 1|_S)|\theta_{PS}\rangle$$

and the same holds when $C = \times$ for similarly defined $|\theta_P^+\rangle$ and $|\theta_P^-\rangle$. Let

$$\sqrt{\lambda_0}|f_0\rangle_P|e_0\rangle_S + \sqrt{\lambda_1}|f_1\rangle_P|e_1\rangle_S$$

be the Schmidt decomposition of $|\theta_{PS}\rangle$ and consider the quantity

$$\begin{aligned}
&\left|\langle\theta_P^0|\theta_P^1\rangle\right| + \left|\langle\theta_P^+|\theta_P^-\rangle\right| \geq \left|\langle\theta_P^0|\theta_P^1\rangle + \langle\theta_P^+|\theta_P^-\rangle\right| \\
&= |\langle\theta_{PS}|(\mathbb{1}_P \otimes |0\rangle\langle 1|_S)|\theta_{PS}\rangle + \langle\theta_{PS}|(\mathbb{1}_P \otimes |+\rangle\langle -|_S)|\theta_{PS}\rangle| \\
&= \frac{1}{2}\left|\langle\theta_{PS}|(\mathbb{1}_P \otimes H_S)|\theta_{PS}\rangle\right| = \frac{1}{2}\left|\lambda_0\langle e_0|_S H_S|e_0\rangle_S + \lambda_1\langle e_1|_S H_S|e_1\rangle_S\right| \\
&= \frac{1}{2}\left|\lambda_0 - \lambda_1\right|
\end{aligned}$$

where $H_S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, the only inequality above is the triangle inequality and the last equality follows from the fact that $\langle e_0|_S H_S|e_0\rangle_S = -\langle e_1|_S H_S|e_1\rangle_S$ for any two orthogonal vectors $|e_0\rangle_S$ and $|e_1\rangle_S$. The last term from the above equation can be bounded above by ϵ since

$$|\lambda_0 - \lambda_1| = \left|\lambda_0 - \frac{1}{2}\right| + \left|\lambda_1 - \frac{1}{2}\right| = \left\|\theta_S - \frac{\mathbb{1}_S}{2}\right\|_1 \geq 2(1 - F(\theta_S, \frac{\mathbb{1}_S}{2})) \geq 2\epsilon$$

Suppose that $\left|\langle\theta_P^0|\theta_P^1\rangle\right| \geq \epsilon/2$ (otherwise, $\left|\langle\theta_P^+|\theta_P^-\rangle\right| \geq \epsilon/2$ and the same argument holds for those two states), this means that Paul cannot distinguish between the two reduced states $|\theta_P^0\rangle$ and $|\theta_P^1\rangle$ with probability better than one minus some constant (that depends on ϵ). We conclude that γ is bounded above by a constant strictly less than 1 and that the probability γ^k of guessing all measurement outcomes correctly declines exponentially fast in k. □

The third criterion of Definition 4 follows trivially from the observation that neither $\mathcal{E}^{\mathrm{acc}}_{RS^N\to S^n}$ nor $\bar{\mathcal{E}}^{\mathrm{acc}}_{P^NS^N\to\Pi S^n}$ acts on the unsampled qubits other than by relabeling them.

References

1. Ahlswede, R., Winter, A.: Strong converse for identification via quantum channels. IEEE Trans. Inf. Theory **48**(3), 569–579 (2002)
2. Ambainis, A.: A new protocol and lower bounds for quantum coin flipping. In: Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing, STOC 2001, pp. 134–142. ACM, New York (2001)
3. Ambainis, A.: A new protocol and lower bounds for quantum coin flipping. J. Comput. Syst. Sci. **68**(2), 398–416 (2004)
4. Koenraad, M.R., et al.: Discriminating states: the quantum Chernoff bound. Phys. Rev. Lett. **98**(16), 160501 (2007)
5. Blum, M.: Coin-flipping by telephone. In: Proceedings of CRYPTO 1991, pp. 11–15 (1981)
6. Bouman, N.J., Fehr, S.: Sampling in a quantum population, and applications. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 724–741. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_39
7. Chailloux, A., Kerenidis, I.: Optimal quantum strong coin flipping. In: Proceedings of FOCS 2009, pp. 527–533 (2009)
8. Christandl, M., König, R., Mitchison, G., Renner, R.: One-and-a-half quantum de Finetti theorems. Commun. Math. Phys. **273**(2), 473–498 (2007)
9. Christandl, M., König, R., Renner, R.: Postselection technique for quantum channels with applications to quantum cryptography. Phys. Rev. Lett. **102**, 020504 (2009)
10. Damgård, I., Dupuis, F., Nielsen, J.B.: On the orthogonal vector problem and the feasibility of unconditionally secure leakage-resilient computation. In: Lehmann, A., Wolf, S. (eds.) ICITS 2015. LNCS, vol. 9063, pp. 87–104. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-17470-9_6
11. Dupuis, F., Fehr, S., Lamontagne, P., Salvail, L.: Adaptive versus non-adaptive strategies in the quantum setting with applications. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9816, pp. 33–59. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53015-3_2
12. Fehr, S., Katz, J., Song, F., Zhou, H.-S., Zikas, V.: Feasibility and completeness of cryptographic tasks in the quantum world. In: Sahai, A. (ed.) TCC 2013. LNCS, vol. 7785, pp. 281–296. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36594-2_16
13. Gutoski, G., Watrous, J.: Toward a general theory of quantum games. In: Proceedings of STOC 2007, pp. 565–574. ACM, New York (2007)

14. Hayashi, M.: Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing. J. Phys. A Math. Gen. **35**(50), 10759–10773 (2002)
15. Hofheinz, D., Müller-Quade, J., Unruh, D.: On the (Im-)possibility of extending coin toss. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 504–521. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_30
16. Kerenidis, I., Nayak, A.: Weak coin flipping with small bias. Inf. Process. Lett. **89**(333), 131–135 (2004)
17. Kitaev, A.: Quantum coin-flipping. Presentation at the 6th Workshop on Quantum Information Processing (QIP 2003) (2003)
18. Mochon, C.: Quantum weak coin-flipping with bias of 0.192. In: Proceedings of FOCS 2004, pp. 2–11 (2004)
19. Mochon, C.: Large family of quantum weak coin-flipping protocols. Phys. Rev. A **72**(2), 022341 (2005)
20. Mochon C.: Quantum weak coin flipping with arbitrarily small bias (2007)
21. Ogawa, T., Nagaoka, H.: A new proof of the channel coding theorem via hypothesis testing in quantum information theory. In: IEEE International Symposium on Information Theory, p. 73 (2002)
22. Pappa, A., et al.: Experimental plug and play quantum coin flipping. Nature Commun. **5**, 3717 (2014)
23. Renner, R.: Security of quantum key distribution. Ph.D. thesis, ETH Zürich (2005)
24. Renner, R.: Symmetry of large physical systems implies independence of subsystems. Nature Phys. **3**, 645–649 (2007)
25. Renner, R.: Simplifying information-theoretic arguments by post-selection. Quantum Cryptogr. Comput. **26**, 66–75 (2010)
26. Salvail, L., Schaffner, C., Sotáková, M.: Quantifying the leakage of quantum protocols for classical two-party cryptography. Int. J. Quantum Inf. **13**(04), 1450041 (2015)
27. Spekkens, R.W., Rudolph, T.: Degrees of concealment and bindingness in quantum bit commitment protocols. Phys. Rev. A **65**(1), 012310 (2001)
28. Spekkens, R.W., Rudolph, T.: Quantum protocol for cheat-sensitive weak coin flipping. Phys. Rev. Lett. **89**(22), 227901 (2002)
29. Winkler, S., Wullschleger, J.: On the efficiency of classical and quantum secure function evaluation. IEEE Trans. Inf. Theory **60**(6), 3123–3143 (2014)
30. Winter, A.: Coding theorem and strong converse for quantum channels. IEEE Trans. Inf. Theory **45**(7), 2481–2485 (1999)
31. Zyczkowski, K., Sommers, H.-J.: Induced measures in the space of mixed quantum states. J. Phys. A Math. Gen. **34**(35), 7111 (2001)