Achieving the limits of the noisy-storage model using entanglement sampling

Frédéric Dupuis[1,2] Omar Fawzi[2] Stephanie Wehner[3]

[1] Department of Computer Science, Aarhus University, Denmark
[2] Institute for Theoretical Physics, ETH Zürich, Switzerland
[3] Center for Quantum Technologies, National University of Singapore, Singapore

Abstract. A natural measure for the amount of quantum information that a physical system E holds about another system $A = A_1, ..., A_n$ is given by the min-entropy $\mathrm{H}_{\min}(A|E)$. Specifically, the min-entropy measures the amount of entanglement between E and A, and is the relevant measure when analyzing a wide variety of problems ranging from randomness extraction in quantum cryptography, decoupling used in channel coding, to physical processes such as thermalization or the thermodynamic work cost (or gain) of erasing a quantum system. As such, it is a central question to determine the behaviour of the min-entropy after some process M is applied to the system A. Here we introduce a new generic tool relating the resulting min-entropy to the original one, and apply it to several settings of interest, including sampling of subsystems and measuring in a randomly chosen basis. The results on random measurements yield new high-order entropic uncertainty relations with which we prove the optimality of cryptographic schemes in the bounded quantum storage model. This is an abridged version of the paper; the full version containing all proofs and further applications can be found in [13].

1 Introduction

A central task in quantum theory is to effectively quantify the amount of information that some system E holds about some classical or quantum data A. For classical data, i.e., A is a string $X^n = X_1, \ldots, X_n$, the *min-entropy* $\mathrm{H}_{\min}(X^n|E)$ forms a particularly relevant measure because it determines the length of a secure key that can be obtained from X^n. This is the setting typically considered in quantum key distribution where E is some information that an adversary Eve has gathered during the course of the protocol, and X^n is the so-called raw key. More precisely, the maximum number ℓ of (almost) random bits [4] that can be obtained from X^n that are both uniform and uncorrelated from E obeys $\ell \approx \mathrm{H}_{\min}(X^n|E)$, if E is classical [15] and quantum [25]. The process by which such randomness is obtained is known as *randomness extraction* (see [30] for a survey) or privacy amplification. Classically, a (strong) randomness extractor is simply a set of functions $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^\ell\}$ such that for almost all functions $f \in \mathcal{F}$, its output $f(X^n)$ is close to uniform and uncorrelated from the

[4] We restrict ourselves to bits in the introduction, however, all our results also apply to higher dimensional alphabets.

adversary, even if he learns which function was applied. That is, the output is of the form $\rho_{F(X)EF} \approx \mathrm{id}/2^n \otimes \rho_{EF}$. A well known example of such a set $\mathcal{F}$ is a set of two-universal hash functions which are used in quantum cryptography to turn a raw key X^n into a secure key $f(X^n)$. The min-entropy also has a very intuitive interpretation as it can be expressed as $\mathrm{H}_{\min}(X^n|E) = -\log P_{\text{guess}}(X^n|E)$ where $P_{\text{guess}}(X^n|E)$ is the probability that the adversary manages to guess X^n maximized over all measurements on E [16].

What can we say in the case of quantum data A? It turns out that the fully quantum min-entropy $\mathrm{H}_{\min}(A|E)$ provides us with a similarly useful way to quantify the amount of information that E holds about A. Its first significance is to quantum cryptography where E is again held by an adversary. More specifically, it has been shown that a quantum-to-classical extractor (QC-extractor) can produce exactly $\ell \approx \mathrm{H}_{\min}(A|E) + \log|A|$ classical bits which are uniform and uncorrelated from E [7]. Instead of applying functions to a classical string, a QC-extractor consists of a set of projective measurements on A giving a classical string as a measurement outcome. Such extractors form a useful tool in two-party quantum cryptography where one might have an estimate of $\mathrm{H}_{\min}(A|E)$, but not of the min-entropy of any classical string X^n produced from A. Thus $\mathrm{H}_{\min}(A|E)$ is directly related to the amount of cryptographic randomness that can be produced from A.

It turns out that the fully quantum min-entropy also enjoys a very appealing operational interpretation [16]. More precisely,

$$\mathrm{H}_{\min}(A|E) = -\log\left(|A| \max_{\Lambda_{E\to\bar{A}}} F(\Phi^N_{A\bar{A}}, \mathrm{id}_A \otimes \Lambda_{E\to\bar{A}}(\rho_{AE}))^2\right) , \qquad (1)$$

where F is the fidelity (see below) and $\Phi^N_{A\bar{A}}$ is the normalized maximally entangled state across A and $\bar{A}$. That is, $\mathrm{H}_{\min}(A|E)$ measures how close ρ_{AE} can be brought to the maximally entangled state by performing a quantum operation on E. Intuitively, this quantifies how close the adversary E can bring himself to being quantumly maximally correlated with A — exactly analogous to maximizing his classical correlations by trying to guess X^n.

1.1 Results

Given the significance of the min-entropy in quantum information, it is a natural question to ask how the min-entropy changes if we apply a quantum operation $\mathcal{M}$ to A. More precisely, one might ask how $\mathrm{H}_{\min}(\mathcal{M}(A)|E)$ relates to $\mathrm{H}_{\min}(A|E)$, for some completely positive trace preserving map $\mathcal{M}$. At present, we know that the min-entropy satisfies $\mathrm{H}_{\min}(\mathcal{M}(A)|E) \geqslant \mathrm{H}_{\min}(A|E)$ if $\mathcal{M}$ is unital [27]. Can we make more refined statements?

Of particular interest to us is the case where the quantum system consist of n qudits $A^n = A_1, \ldots, A_n$. Our main result is to establish the following very general theorem for maps $\mathcal{M}$ with the property that we can diagonalize $((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \mathrm{id}_{\bar{A}^n})(\Phi_{A^n\bar{A}^n}) = \sum_{s\in\{0,\ldots,d^2-1\}} \lambda_s \Phi_s$ where $A^n = A_1, \ldots, A_n$, $d = |A_j|$ is the dimension of one of the individual qudits, $\Phi_{A^n\bar{A}^n}$ is again the maximally entangled state, and $\{\Phi_s\}_s$ is a basis for the space $A^n \otimes \bar{A}^n$ consisting of maximally entangled vectors, and

$\lambda_s \geq 0$ are the corresponding eigenvalues (see Sections 2 and Section 3 for precise definitions and statement of the theorem). In terms of the smooth min-entropy $\mathrm{H}_{\min}^{\varepsilon}$, which, loosely speaking, is equal to the min-entropy except with error probability ε, our first contribution can be stated as

- **Main result (Informal)** For any partition of $\{0, \ldots, d^2 - 1\}^n = \mathfrak{S}_+ \cup \mathfrak{S}_-$ into subsets $\mathfrak{S}_+$,$\mathfrak{S}_-$ we have $2^{-\mathrm{H}_{\min}^{\varepsilon}(\mathcal{M}(A^n)|E)} \lessapprox \sum_{s \in \mathfrak{S}_+} \lambda_s 2^{-\mathrm{H}_{\min}(A^n|E)} + (\max_{s \in \mathfrak{S}_-} \lambda_s) d^n$.

At first glance, our condition on the maps $\mathcal{M}$ may seem rather unintuitive and indeed restrictive. Yet, it turns out that many interesting maps do indeed satisfy these conditions, allowing us to establish the following results.

Entanglement sampling In the study of classical extractors, a goal was to construct families of functions f that are *locally computable* [31]. That is, if our goal were to extract only a very small number of key bits from a long string X^n of length n, one might wonder whether this can be done efficiently in the sense that the functions f depend only on a small number of bits of X^n. Classically, a very beautiful method to answer this question is to show that the min-entropy can in fact be *sampled* [31,24]. That is, if we choose a subset S of the bits at random, then the min-entropy of the bits X_S in that subset S obeys

$$\mathrm{H}_{\min}(X_S|ES) \gtrapprox |S| R(\mathrm{H}_{\min}(X^n|E)/n) \; , \tag{2}$$

for some function R. The function R can be understood as a rate function that determines the relation of the original min-entropy rate $\frac{\mathrm{H}_{\min}(X^n|E)}{n}$ to the min-entropy rate on a subset S of the bits. In other words, min-entropy sampling says that if X^n is hard to guess, then even given the choice of subset S it is tricky for the adversary to guess X_S. To see why this yields the desired functions f note that one way to construct a randomness extractor would be to first pick a random subset S, and then apply an arbitrary extractor to the much shorter bit string X_S. In the classical literature, this is known as the sample-then-extract approach [31].

Inspired by the classical results of Vadhan [31], it is a natural question whether there exists QC-extractors which are efficient in the sense that the measurements $M \in \mathcal{M}$ only act on a small number of qubits of $A^n = A_1, \ldots, A_n$. Or, even more generally, whether there exist decoupling operations which depend on only very few qubits. As before, one way to answer this question in generality is to show that even the fully quantum min-entropy can be sampled.

- **Entanglement sampling (Informal)** For any quantum state ρ_{A^nE}, i.e., $\mathrm{H}_{\min}^{\varepsilon}(A_S|ES) \gtrapprox |S| R(\mathrm{H}_{\min}(A^n|E)/n)$ for the rate function R plotted in Figure 1. See Theorem 2 for a precise statement.

It should be noted that even the case of standard min-entropy sampling of a classical string X^n, but quantum side information E has proved challenging. The results of [4] imply that sampling of classical strings is possible when the distribution over the strings X^n is uniform (i.e., $\rho_{X^nE} = (1/2^n) \sum_{x \in \{0,1\}^n} |x\rangle\langle x| \otimes \rho_E^x$), and the size of E

is bounded, and [18] has shown that sampling of blocks (but not individual bits) is possible. This was later refined in [34] to show that bitwise sampling is also possible (see Figure 1 for a comparison of the rate function). Very roughly, the techniques used in [34] relate the adversary's ability to guess the string X^n to his ability to guess the XOR of bits in the string. Clearly, in the case of fully quantum A^n such techniques cannot be used as it is indeed unclear what the XOR of qubits even means.

As this is the first result on entanglement sampling, it required entirely novel techniques. More precisely, it inspired the even more general theorem sketched above, from which entanglement sampling follows by choosing an appropriate map $\mathcal{M}$. As a byproduct, using the same techniques, we also obtain a stronger statement of sampling a classical string X^n with respect to a quantum system E in the sense that the rate R is improved (see Figure 1 for a comparison). What's more, we are able to show an even more precise statement in terms of the entropy $\mathrm{H}_2(A^n|E)_\rho$ - without any ε error terms. Classically, this quantity is known as the (conditional) collision entropy. In general, it is very closely related to the min-entropy, and in fact enjoys a very similar operational interpretation. More specifically, it can be expressed in the same form as (1) where the optimization over all quantum operations $\Lambda_{E\to\bar{A}^n}$ is replaced by the so-called *pretty good recovery* map $\Lambda^{\mathrm{pg}}_{E\to\bar{A}^n}$ which is close to optimal [2].

Uncertainty relations Another consequence of our main result is a new uncertainty relation with quantum side information for measurements of n qubits $A^n = A_1, \ldots, A_n$ in randomly chosen BB84 bases. Apart from the foundational consequences, such relations have found applications in quantum cryptography (see e.g., [7]). Our result establishes the first entropic uncertainty relation with quantum side-information that uses a high-order entropy like the min-entropy and that is nontrivial as soon as the system being measured is not maximally entangled with the observer E. In other words, this shows a quantitative bound on the probability of successfully guessing the measurement outcome that is nontrivial as soon as $\mathrm{H}_{\min}(A^n|E) > -n$. [5]

- **High-order entropic uncertainty relation for BB84 bases** If X^n is obtained by measuring the system A^n in a random BB84 basis Θ^n, we have $\mathrm{H}_{\min}(X^n|E\Theta^n) \geqslant n \cdot \frac{1}{2}\gamma\left(\frac{\mathrm{H}_{\min}(A^n|E)}{n}\right)$, where the function γ is plotted in Figure 2. See Theorem 5 and Corollary 6 for precise statements.

We can also prove uncertainty relations for qudit-wise measurements in mutually unbiased bases (see full version [13]). Again, these results follow from our very general theorem sketched above, this time for a map $\mathcal{M}$ that represents randomly chosen measurements.

Applications to the noisy-storage model Our new uncertainty relations have several interesting applications to cryptography. The goal of two-party cryptography is to enable Alice and Bob to solve tasks in cooperation even if they do not trust each other. A classic example of such tasks are bit commitment and oblivious transfer. Unfortunately, it has been shown that even using quantum communication, none of these tasks can

[5] The fully quantum min-entropy can be negative up to $\mathrm{H}_{\min}(A^n|E) = -n$ if ρ_{A^nE} is the maximally entangled state.

be implemented securely without making assumptions [22,19]. What makes such tasks more difficult than quantum key distribution is that Alice and Bob cannot collaborate to check on any eavesdropper. Instead, each party has to fend for itself.

Nevertheless, because two-party computation is such a central part of modern cryptography, one is willing to make *assumptions* on how powerful an attacker can be in order to implement them securely. Classically, such assumptions generally take the form of computational assumptions, where we assume that a particular mathematical problem cannot be solved in polynomial time. Here, we consider *physical* assumptions that can enable us to solve such tasks. In particular, can the sole assumption of a limited storage device lead to security [21]? This is indeed the case and it was shown that security can be obtained if the attacker's *classical* storage is limited [21,9]. Yet, apart from the fact that classical storage is cheap and plentiful, assuming a limited classical storage has one rather crucial caveat: If the honest players need to store n classical bits to execute the protocol in the first place, *any* classical protocol can be broken if the attacker can store more than roughly n^2 bits [14]. Motivated by this unsatisfactory gap, it was thus suggested to assume that the attacker's *quantum* storage was bounded [5,10,11,12,8], or, more generally, noisy [32,26,17]. The central assumption of the noisy-storage model is that during waiting times Δt introduced in the protocol, the attacker can keep quantum information only in his noisy quantum storage device; otherwise he is all-powerful (see Section 4.4).

The assumption of bounded or noisy quantum storage offers significant advantages in that the proposed protocols do not require any quantum storage at all to be implemented by the honest parties. They are typically based on BB84 [17] or six-state [7] encodings, and indeed the first implementation of a bit commitment protocol has recently been performed experimentally [23]. So far it was known that there exist protocols that send n qubits encoded in either the BB84 or six-state encoding, and that are secure as long as the adversary can only store strictly less than $n/2$ or $2n/3$ noise-free qubits respectively.

Using our new techniques, we are able to show security of the primitive called *weak string erasure* [17] (see Section 4.4), which in turn can be supplemented with additional classical or quantum communication to obtain primitives such as bit commitment.

- **Application 1: Bounded storage** There exists a weak string erasure protocol transmitting n qubits that is secure as long as the adversary can store at most strictly less than $n - O(\log^2 n)$ qubits. The protocol does not require any quantum memory to be executed, and merely requires simple quantum operations and measurements. See Theorem 8 for a precise statement.

It should be noted that no such protocol can be secure as soon as the adversary can store n qubits, so our result is essentially optimal. Our result highlights the sharp contrast between the classical and the quantum bounded storage model and answers the main open question in the BQSM. The noisy-storage model offers an advantage over the case of bounded-storage not only for implementations using high-dimensional encodings such as the infinite-dimensional states sent in continuous variable experiments, but allows security even for arbitrarily large storage devices as long as the noise is large enough. Essentially, the noisy-storage model captures our intuition that security should be linked to how much information the adversary can store in his quantum memory. The first proofs linked security to the classical capacity [17], the entanglement cost [6] and finally the quantum capacity [7]. The latter result used a protocol based on six-state encodings and required the fidelity of the device to be exponentially small in the number of qubits communicated during the protocol.

– **Application 2: Noisy storage** We prove that security in the noisy-storage model is possible basically as soon as the fidelity of the storage device is smaller than desired error parameter, which is best possible (see Section 4.4). Furthermore, we link security of a BB84-based protocol to the quantum capacity of the adversary's storage device for the first time. See Theorem 7 for a precise statement.

2 Preliminaries

2.1 Basic concepts and notation

In quantum mechanics, a system such as Alice's or Bob's labs are described mathematically by *Hilbert spaces*, denoted by $A, B, C, \ldots$. Here, we follow the usual convention in quantum cryptography and assume that all Hilbert spaces are finite-dimensional. We write $|A|$ for the dimension of A. A system of n qudits is also denoted as $A^n = A_1, \ldots, A_n$, where we also use $|A|$ to denote the dimension of one single qudit in A^n. The set of linear operators on A is denoted by $\mathcal{L}(\mathcal{A})$, and we write $\mathrm{Herm}(A)$ and $\mathrm{Pos}(A)$ for the set of hermitian and positive semidefinite operators on A respectively. We denote the adjoint of an operator M by $M^\dagger$. A *quantum state* ρ_A is an operator $\rho_A \in \mathcal{S}(A)$, where $\mathcal{S}(A) = \{\sigma_A \in \mathrm{Pos}(A) \mid \mathrm{Tr}(\sigma_A) = 1\}$. We will often make use of *operator inequalities*: whenever $X, Y \in \mathrm{Herm}(A)$, we write $X \leqslant Y$ to mean that $Y - X \in \mathrm{Pos}(A)$. A quantum operation is given by a completely positive map $\mathcal{M} : \mathcal{L}(A) \to \mathcal{L}(C)$. A map $\mathcal{M}$ is said to be completely positive if for any system B and $X \in \mathrm{Pos}(A \otimes B)$ we have $(\mathcal{M} \otimes \mathrm{id})(X) \geqslant 0$.

Throughout, we use the shorthand $[d] = \{0, 1, \ldots, d-1\}$. We will follow the convention to use H to denote the unitary that takes the computational $\{|0\rangle, |1\rangle\}$ to the Hadamard basis: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. When considering n qubits, we also use $H^{\theta^n} = H^{\theta_1} \otimes \cdots \otimes H^{\theta_n}$ for the unitary defining the basis $\theta^n \in \{0,1\}^n$.

2.2 Entropies

Next to its operational interpretation given in (1), the *conditional min-entropy* of a state $\rho_{AB} \in \mathcal{S}(AB)$ can also be expressed as $\mathrm{H}_{\min}(A|B)_\rho = \max_{\sigma_B \in \mathcal{S}(B)} \mathrm{H}_{\min}(A|B)_{\rho|\sigma}$, with

$$\mathrm{H}_{\min}(A|B)_{\rho|\sigma} = \max\left\{\lambda \in \mathbb{R} : 2^{-\lambda} \cdot \mathrm{id}_A \otimes \sigma_B \geqslant \rho_{AB}\right\} \ , \tag{3}$$

where the symbol id_A refers to the identity on A. We use the subscript ρ to emphasize the state ρ_{AB} of which we evaluate the min-entropy. The smoothed version is defined by $\mathrm{H}^{\varepsilon}_{\min}(A|B)_\rho = \max_{\tilde{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})} \mathrm{H}_{\min}(A|B)_{\tilde{\rho}}$, where $\mathcal{B}^\varepsilon(\rho)$ is the set of states at a distance at most ε from ρ. We use the purified distance as the distance measure [28]. We refer to [27] for a review of the properties of the min-entropy.

It is simpler to state our results in terms of the related collision entropy defined for any $\rho_{AB} \in \mathrm{Pos}(A \otimes B)$ by

$$\mathrm{H}_2(A|B)_\rho = -\log \mathrm{Tr}\left[\left(\rho_B^{-1/4} \rho_{AB} \rho_B^{-1/4}\right)^2\right]. \tag{4}$$

We use relations between $\mathrm{H}_{\min}$ and H_2 proved in the full version [13], in particular

$$\mathrm{H}_{\min}^{\varepsilon}(A|B)_\rho \geq \mathrm{H}_2(A|B)_\rho - \log(2/\varepsilon^2), \tag{5}$$

and

$$\mathrm{H}_{\min}(X|B)_\sigma \leq \mathrm{H}_2(X|B)_\sigma \leq 2\mathrm{H}_{\min}(X|B)_\sigma, \tag{6}$$

for a classical-quantum state σ_{XB}. Finally, we use the binary entropy function $h(x) = -x \log x - (1-x)\log(1-x)$.

2.3 A convenient basis

Throughout, we make use of a very convenient basis of maximally entangled states for the space $A \otimes \bar{A}$ where $\bar{A} \simeq A$. The (unnormalized) maximally entangled state

$$|\Phi\rangle_{A\bar{A}} = \sum_a |a\rangle_A \otimes |a\rangle_{\bar{A}} \tag{7}$$

will play an important role in our analysis. Here, the vectors $|a\rangle$ label the standard basis of A. We use $|\Phi^N\rangle_{A\bar{A}}$ to denote the normalized version $|\Phi^N\rangle_{A\bar{A}} = \frac{1}{\sqrt{|A|}}|\Phi\rangle_{A\bar{A}}$. We repeatedly use the following properties. For any operators X and Y acting on A, we have

$$\mathrm{Tr}[XY] = \mathrm{Tr}[X \otimes \top(Y)\Phi_{A\bar{A}}] \tag{8}$$

where $\top$ denotes the transpose map in the standard basis and $\Phi_{A\bar{A}} = |\Phi\rangle\langle\Phi|_{A\bar{A}}$. Moreover, if $X : A \to C$ is a linear operator from A to C we have

$$(X \otimes \mathrm{id}_{\bar{A}})|\Phi\rangle_{A\bar{A}} = (\mathrm{id}_C \otimes \top(X))|\Phi\rangle_{C\bar{C}}. \tag{9}$$

Using (8) and (9) one can naturally construct an orthogonal basis of $A\bar{A}$ by applying unitary transformations to $|\Phi\rangle$ that are orthogonal with respect to the Hilbert-Schmidt inner product. Define for $s \in [|A|^2]$, $|\Phi_s\rangle = (W_s \otimes \mathrm{id})|\Phi\rangle_{A\bar{A}}$ where W_s denote the generalized Pauli operators (see e.g., [1]), sometimes also called Weyl operators. In fact, all our results would hold for any unitary operators W_s that are orthogonal with respect to the Hilbert-Schmidt inner product. We again use $\Phi_s = |\Phi_s\rangle\langle\Phi_s|$.

In particular for $|A| = 2$, W_0, W_1, W_2, W_3 are the Pauli operators id, X, Y, Z respectively, and we obtain the well-known Bell basis.

For $n > 0$, we will denote by A^n the system $\bigotimes_{i=1}^n A_i$, where each A_i is a copy of A. Furthermore, if $S \subseteq \{1, \ldots, n\}$, we write A_S to denote $\bigotimes_{i \in S} A_i$. In other words, A^n consists of n copies of the system A, and A_S contains the copies that correspond to indices in S. In such a setting the dimension of the system A is denoted d. We can naturally define for $s \in [d^2]^n$, $|\Phi_s\rangle = \otimes_{i=1}^n |\Phi_{s_i}\rangle_{A_i\bar{A}_i}$. We then have that $\{\frac{1}{\sqrt{d^n}}|\Phi_s\rangle\}_s$ is an orthonormal basis of $A^n\bar{A}^n$. For such strings s, we denote $\mathrm{supp}(s) = \{i \in \{1, \ldots, n\} : s_i \neq 0\}$ and $|s| = |\mathrm{supp}(s)|$.

3 Evolution of H_2 under general maps

In this section, we derive constraints on the evolution of the conditional collision entropy H_2 when the system A^n undergoes some transformation described by a completely positive map $\mathcal{M}$. Our results on entanglement sampling and uncertainty relations are obtained by evaluating this bound for particular channels $\mathcal{M}$. A statement for the smooth min-entropy follows directly by applying inequality (5).

Theorem 1 *Let $\mathcal{M}_{A^n \to C}$ be a completely positive map such that $((\mathcal{M}^\dagger \circ \mathcal{M})_{A^n} \otimes \mathrm{id}_{\bar{A}^n})(\varPhi_{A^n \bar{A}^n}) = \sum_{s \in [d^2]^n} \lambda_s \varPhi_s$ and let $\rho_{A^n E} \in \mathcal{S}(A^n E)$ be a state, where $A^n = A_1, \ldots, A_n$ is comprised of n qudits of dimension d. Then for any partition $[d^2]^n = \mathfrak{S}_+ \cup \mathfrak{S}_-$ into subsets $\mathfrak{S}_+$ and $\mathfrak{S}_-$, we have*

$$2^{-\mathrm{H}_2(C|E)_{\mathcal{M}(\rho)}} \leqslant \sum_{s \in \mathfrak{S}_+} \lambda_s 2^{-\mathrm{H}_2(A^n|E)_\rho} + (\max_{s \in \mathfrak{S}_-} \lambda_s) d^n. \tag{10}$$

The maps $\mathcal{M}$ of interest typically have some symmetry. For example, if the map $\mathcal{M}$ is invariant under permutations of the n systems $A_1, \ldots, A_n$, then the coefficients λ_s only depend on the type of s, i.e., the number of times each symbol in $[d^2]$ occurs in s. For example, for the entropy sampling result (Theorem 2), the map $\mathcal{M}$ is such that λ_s only depends on the weight $|s| = |\{i \in [n] : s_i \neq 0\}|$.

Proof. Let $\tilde{\rho}_{A^n E} = \rho_E^{-1/4} \rho_{A^n E} \rho_E^{-1/4}$, and let $\widehat{\rho}_{A^n \bar{A}^n} = \mathrm{Tr}_{E\bar{E}}[(\tilde{\rho}_{A^n E} \otimes \top(\tilde{\rho}_{\bar{A}^n \bar{E}}))\varPhi_{E\bar{E}}]$. Note that $\widehat{\rho}_{A^n \bar{A}^n} \geq 0$ and $\mathrm{Tr}[\widehat{\rho}_{A^n \bar{A}^n}] = \mathrm{Tr}[\tilde{\rho}_E^2] = 1$. Furthermore, define $\bar{\mathcal{M}}$ as $\bar{\mathcal{M}}(X) = \top(\mathcal{M}(\top(X)))$ for all X. Our first goal is to rewrite $\mathrm{H}_2(C|E)_\sigma$ in terms of the basis $\{\varPhi_s\}_s$. We obtain from (8)

$$\begin{aligned}
2^{-\mathrm{H}_2(C|E)_\sigma} &= \mathrm{Tr}[\mathcal{M}(\tilde{\rho}_{A^n E})^2] \\
&= \mathrm{Tr}[(\mathcal{M}(\tilde{\rho}_{A^n E}) \otimes \top(\mathcal{M}(\tilde{\rho}_{\bar{A}^n \bar{E}})))\varPhi_{C\bar{C}} \otimes \varPhi_{E\bar{E}}] \\
&= \mathrm{Tr}[(\mathcal{M}(\tilde{\rho}_{A^n E}) \otimes \bar{\mathcal{M}}(\top(\tilde{\rho}_{\bar{A}^n \bar{E}})))\varPhi_{C\bar{C}} \otimes \varPhi_{E\bar{E}}] \\
&= \mathrm{Tr}[(\tilde{\rho}_{A^n E} \otimes \top(\tilde{\rho}_{\bar{A}^n \bar{E}}))((\mathcal{M}^\dagger) \otimes (\bar{\mathcal{M}}^\dagger))(\varPhi_{C\bar{C}}) \otimes \varPhi_{E\bar{E}}].
\end{aligned}$$

Now by writing a Kraus representation $\mathcal{M}(X) = \sum_i K_i X K_i^\dagger$ with operators $K_i : A \to C$ and using (9), we see that $(\mathrm{id}_C \otimes \bar{\mathcal{M}}^\dagger)(\varPhi_{C\bar{C}}) = (\mathcal{M}_{A^n \to C} \otimes \mathrm{id}_{\bar{A}^n})(\varPhi_{A^n \bar{A}^n})$. Thus, we obtain using the definition of $\widehat{\rho}_{A^n \bar{A}^n}$ and the condition on $\mathcal{M}$

$$\begin{aligned}
2^{-\mathrm{H}_2(C|E)_\sigma} &= \mathrm{Tr}[(\tilde{\rho}_{A^n E} \otimes \top(\tilde{\rho}_{\bar{A}^n \bar{E}}))((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \mathrm{id}_{\bar{A}^n})(\varPhi_{A^n \bar{A}^n}) \otimes \varPhi_{E\bar{E}}] \\
&= \mathrm{Tr}[\widehat{\rho}_{A^n \bar{A}^n}((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \mathrm{id}_{\bar{A}^n})(\varPhi_{A^n \bar{A}^n})] \\
&= \sum_{s \in [d^2]^n} \lambda_s \, \mathrm{Tr}[\widehat{\rho}_{A^n \bar{A}^n} \varPhi_s]. \qquad (11)
\end{aligned}$$

We prove the two key constraints on the terms $\mathrm{Tr}[\widehat{\rho}_{A^n \bar{A}^n} \varPhi_s]$ we will be using. First, we have a global constraint. Note that the set of vectors $\{\frac{1}{\sqrt{d^n}} |\varPhi_s\rangle\}_{s \in [d^2]^n}$ forms an *orthonormal* basis and thus $\mathrm{id}_{A^n \bar{A}^n} = \frac{1}{d^n} \sum_{s \in [d^2]^n} \varPhi_s$. This yields

$$\sum_{s \in [d^2]^n} \mathrm{Tr}[\widehat{\rho}_{A^n \bar{A}^n} \varPhi_s] = d^n \, \mathrm{Tr}[\widehat{\rho}_{A^n \bar{A}^n}] = d^n. \tag{12}$$

The second observation concerns the individual terms $\mathrm{Tr}[\widehat{\rho}_{A^n\bar{A}^n}\mathit{\Phi}_s]$. For any s,

$$\begin{aligned}\mathrm{Tr}[\widehat{\rho}_{A^n\bar{A}^n}\mathit{\Phi}_s] &= \mathrm{Tr}[\widehat{\rho}_{A^n\bar{A}^n}(W_s \otimes \mathrm{id}_{\bar{A}^n})\mathit{\Phi}_{A^n\bar{A}^n}(W_s^\dagger \otimes \mathrm{id}_{\bar{A}^n})] \\ &= \mathrm{Tr}[\big(W_s^\dagger \tilde{\rho}_{A^nE} W_s \otimes \top(\tilde{\rho}_{\bar{A}^n\bar{E}})\big)\,\mathit{\Phi}_{A^n\bar{A}^n} \otimes \mathit{\Phi}_{E\bar{E}}] \\ &= \mathrm{Tr}[W_s^\dagger \tilde{\rho}_{A^nE} W_s \tilde{\rho}_{A^nE})] \\ &\leqslant \mathrm{Tr}[\tilde{\rho}_{A^nE}^2] = 2^{-\mathrm{H}_2(A^n|E)_\rho},\end{aligned}$$

using the Cauchy-Schwarz inequality in the form $\mathrm{Tr}[XY] \leq \sqrt{\mathrm{Tr}[X^2]\,\mathrm{Tr}[Y^2]}$ with $X = W_s^\dagger \tilde{\rho}_{A^nE} W_s$ and $Y = \tilde{\rho}_{A^nE}$. Also, observe that the positivity of $\widehat{\rho}_{A^n\bar{A}^n}$ implies that $\mathrm{Tr}[\widehat{\rho}_{A^n\bar{A}^n}\mathit{\Phi}_s] = \langle \mathit{\Phi}_s|\widehat{\rho}_{A^n\bar{A}^n}|\mathit{\Phi}_s\rangle \geqslant 0$. Thus, we have

$$0 \leqslant \mathrm{Tr}[\widehat{\rho}_{A^n\bar{A}^n}\mathit{\Phi}_s] \leqslant 2^{-\mathrm{H}_2(A^n|E)_\rho}. \tag{13}$$

Applying inequalities (12) and (13) to (11), we obtain the desired result.

4 Applications

We now derive several interesting consequences of Theorem 1. All of these follow by making an appropriate choice for the map $\mathcal{M}$.

4.1 Quantum-quantum min-entropy sampling

We now state our results on entanglement sampling. The theorem below deals with the following scenario: we have n qudits and we choose a subset of them of size k uniformly at random. We have a lower bound on the collision entropy of the whole state conditioned on some quantum side-information E; the theorem then gives a lower bound on the conditional collision entropy of the sample. The rate function obtained is plotted in Figure 1. The same figure also shows plots of classical-quantum sampling results that are discussed in Section 4.2.

Theorem 2 *Let $\rho_{A^nE} \in \mathcal{S}(A^nE)$ and $1 \leqslant k \leqslant n$, let $d = |A|$ be the dimension of a single system, and let $h_2 := \frac{\mathrm{H}_2(A^n|E)_\rho}{n}$. Then, we have for $n > d^2$*

$$2^{-\mathrm{H}_2(A_S|ES)_\rho} = \mathbb{E}_{S\subseteq[n],|S|=k} 2^{-\mathrm{H}_2(A_S|E)_\rho} \leqslant 2^{-kR_d(h_2)+\log(n^2+1)}, \tag{14}$$

where $R_d(\cdot)$ is the rate function defined as $R_d(x) := -\log(d - df_d^{-1}(x))$, and $f_d(x) := h(x) + x\log(d^2-1) - \log d$. Using (5)*, we have for any $\varepsilon \in [0,1)$*

$$\mathrm{H}_{\min}^\varepsilon(A_S|ES)_\rho \geqslant kR_d(h_{\min}) - \log(n^2+1) - \log\frac{2}{\varepsilon^2}, \tag{15}$$

where $h_{\min} := \frac{\mathrm{H}_{\min}(A^n|E)_\rho}{n}$.

Proof. We now prove (14) by applying Theorem 1 for an appropriately chosen map $\mathcal{M}$. Naturally, $\mathcal{M}$ will (up to normalization) select a random subset S and discard all the qubits of the input except the ones in S. More formally, define $\mathcal{M}_{A^n\to A^kS}(X) =$

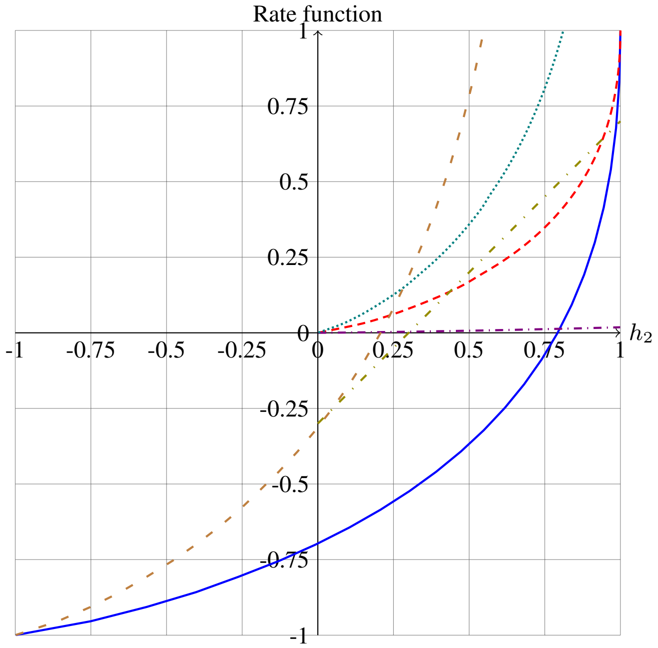

Fig. 1. Plot of our quantum-quantum rate function $R_2(h_2)$ from Theorem 2 (——), our classical-quantum rate function $C_2(h_2)$ from Theorem 4 (- - -), Wullschleger's min-entropy sampling result [34, Corollary 1] (-·-·), Vadhan's purely classical min-entropy sampling results [31, Lemma 6.2] (- · -), and the classical and quantum upper bounds we get from a state that is uniform on strings of a fixed type analyzed in the full version [13] (·······, - -). As Vadhan's result requires a choice of parameters we chose $\tau = 0.1$, which yields a lower bound on the *smooth* min-entropy, with smoothing parameter of the order of 10^{-6} for a block size of $n = 10000$.

$\frac{1}{\sqrt{\binom{n}{k}}}\sum_{S\subseteq[n],|S|=k}\mathrm{Tr}_{S^c}[X]\otimes|S\rangle\langle S|$, for $X \in \mathcal{L}(A^n)$, where the second register contains a classical description of the set S, and S^c denotes the complement of S in $[n]$. The reason for this normalization will be clear in the following calculation. Our first task is to relate this map to $\mathrm{H}_2(A_S|ES)_\rho$. A simple calculation reveals that

$$2^{-\mathrm{H}_2(A^kS|E)_{\mathcal{M}(\rho)}} = \mathbb{E}_{S\subseteq[n],|S|=k}\,\mathrm{Tr}\left[\left(\rho_E^{-1/4}\rho_{A_SE}\rho_E^{-1/4}\right)^2\right] = 2^{-\mathrm{H}_2(A_S|ES)_\rho}.$$

Our second task is to show that our choice of $\mathcal{M}$ satisfies the conditions of Theorem 1. We have

$$((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \mathrm{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) = \mathcal{M}^\dagger \left(\frac{1}{\sqrt{\binom{n}{k}}} \sum_{|S|=k} |S\rangle\langle S| \otimes \Phi_{A_S \bar{A}_S} \otimes \mathrm{id}_{\bar{A}_{S^c}} \right)$$

$$= \frac{1}{\binom{n}{k}} \sum_{|S|=k} \Phi_{A_S \bar{A}_S} \otimes \mathrm{id}_{A_{S^c} \bar{A}_{S^c}}.$$

We now write this operator in terms of $\{\Phi_s\}_{s \in [d^2]^n}$. Recall that $\{\frac{1}{\sqrt{d^n}} |\Phi_s\rangle\}_s$ forms an orthonormal basis and thus $\mathrm{id}_{A^n \bar{A}^n} = \frac{1}{d^n} \sum_{s \in [d^2]^n} \Phi_s$:

$$((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \mathrm{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) = \frac{1}{d^{n-k}\binom{n}{k}} \sum_{|S|=k} \sum_{s:\mathrm{supp}(s) \subseteq S^c} \Phi_s$$

$$= \frac{1}{d^{n-k}\binom{n}{k}} \sum_{s:|s| \leqslant n-k} \binom{n-|s|}{k} \Phi_s.$$

As a result, the coefficients λ_s from Theorem 1 are $\lambda_s = \frac{\binom{n-|s|}{k}}{d^{n-k}\binom{n}{k}}$. Observe that λ_s only depends on $|s|$ and is a decreasing function of $|s|$. In order to apply Theorem 1, it is natural to choose the partition $\mathfrak{S}_+ \cup \mathfrak{S}_-$ of the form $\mathfrak{S}_+ = \{s \in [d^2]^n : |s| \leqslant \ell_0\}$ and $\mathfrak{S}_- = \{s \in [d^2]^n : |s| > \ell_0\}$ for a value of $\ell_0 \in \{0, \ldots, n\}$ to be chosen as a function of h_2.

Writing equation (10) in our case we obtain,

$$2^{-\mathrm{H}_2(A_S|ES)_\rho} \leqslant \sum_{\ell=0}^{\ell_0} \frac{\binom{n-\ell}{k}}{d^{n-k}\binom{n}{k}} \binom{n}{\ell} (d^2-1)^\ell 2^{-h_2 n} + \frac{\binom{n-\ell_0-1}{k}}{\binom{n}{k}} d^k$$

$$= \frac{2^{-h_2 n}}{d^{n-k}} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell + \frac{\binom{n-\ell_0-1}{k}}{\binom{n}{k}} d^k. \qquad (16)$$

Now all that remains is to optimize over ℓ_0 and to find a simple expression for this quantity. Before choosing ℓ_0, we simplify the expression above. For the second term, we bound

$$\frac{\binom{n-\ell_0-1}{k}}{\binom{n}{k}} d^k \leqslant \left(\frac{n-\ell_0-1}{n} \right)^k d^k.$$

To obtain a simple bound on the first term, we use the following lemma whose proof can be found in the appendix of the full version [13].

Lemma 3 *For any $\ell_0 \in \{0, \ldots, n\}$ such that $\ell_0 \leqslant \frac{d^2-1}{d^2} n$ where $d^2 < n$, we have*

$$\sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell \leqslant n^2 \binom{n}{\ell_0} (d^2-1)^{\ell_0} \max \left(\frac{n-\ell_0-1}{n}, \frac{1}{d^2} \right)^k.$$

It then follows from equation (16) that

$$2^{-\mathrm{H}_2(A_S|ES)_\rho} \leqslant \max\left(\frac{n-\ell_0-1}{n}, \frac{1}{d^2}\right)^k d^k \left(\frac{2^{-h_2 n}}{d^n} n^2 \binom{n}{\ell_0}(d^2-1)^{\ell_0} + 1\right).$$

We now determine the value of ℓ_0 as a function of h_2. Observe that using properties of binomial coefficients, we have $\binom{n}{\ell}(d^2-1)^\ell \leqslant 2^{nh(\ell_0/n)}(d^2-1)^{\ell_0} = 2^{nf_d(\ell_0/n)}d^n$ provided $\ell_0 \leqslant \frac{d^2-1}{d^2}n$. We define ℓ_0 to be the largest integer that is at most $\frac{d^2-1}{d^2}n$ such that $f_d(\ell_0/n) \leqslant h_2$. As a result, we have

$$2^{-\mathrm{H}_2(A_S|ES)_\rho} \leqslant \max\left(\frac{n-\ell_0-1}{n}, \frac{1}{d^2}\right)^k d^k \left(n^2+1\right). \qquad (17)$$

Observe also that in the case where the maximum is $1/d^2$, the result follows directly as $R_d(h_2) \leq \log d$. In the case where $(n-\ell_0-1)/n > 1/d^2$, we observe that $(\ell_0+1)/n > f_d^{-1}(h_2)$ by our choice of ℓ_0. Note that if $\ell_0 + 1 \leqslant (d^2-1)/d^2 \cdot n$, this follows from the fact that f_d is nondecreasing, and otherwise it follows from the fact that by definition f_d^{-1} is always upper bounded by $(d^2-1)/d^2$. We now write $\left(\frac{n-\ell_0-1}{n}\right)^k$ in terms of the entropy rate h_2:

$$\begin{aligned} k\log\left(\frac{n-\ell_0-1}{n}\right) &= k\log\left(1-\frac{\ell_0+1}{n}\right) \\ &\leqslant k\log(1-f_d^{-1}(h_2)) \\ &= k\log(d-df_d^{-1}(h_2)) - k\log d \\ &= -kR_d(h_2) - k\log d. \end{aligned}$$

By plugging these inequalities into (17), we obtain the desired result.

4.2 Classical-quantum min-entropy sampling

Statement Observe that in the case where the system A^n is classical, i.e., $\rho_{A^nE} = \sum_{x^n\in[d]^n} p(x^n)|x^n\rangle\langle x^n| \otimes \rho_E(x^n)$ for some distribution p and states $\rho_E(x^n)$, Theorem 2 can still be applied but in many cases it gives trivial bounds. In fact, when A^n is classical, we have $\mathrm{H}_2(A^n|E) \geqslant 0$ as well as $\mathrm{H}_2(A_S|ES) \geqslant 0$. In order to improve on the lower bound of Theorem 2 in the case of a classical system, we can apply Theorem 1 to a more specific map $\mathcal{M}$ that *measures* the systems A_S that are sampled. This allows us to obtain a lower bound on the collision entropy $\mathrm{H}_2(A_S|ES)$ that is nontrivial for the entire range $\mathrm{H}_2(A^n|E) \in [0, n\log d]$.

Theorem 4 *Let ρ_{A^nE} be a classical-quantum state, and $1 \leqslant k \leqslant n$, let $d = |A|$, and let $h_2 := \frac{\mathrm{H}_2(A^n|E)_\rho}{n}$. Then, for any $n > d$,*

$$2^{-\mathrm{H}_2(A_S|ES)_\rho} = \mathbb{E}_{S\subseteq[n],|S|=k} 2^{-\mathrm{H}_2(A_S|E)_\rho} \leqslant 2^{-kC_d(h_2)+\log(n^2+1)},$$

where $C_d(\cdot)$ is the rate function defined as $C_d(\alpha) := -\log(1-c_d^{-1}(\alpha))$, and $c_d(\alpha) := h(\alpha) + \alpha\log(d-1)$.

4.3 High-order uncertainty relations against quantum side-information

Uncertainty relations play a fundamental role in quantum information and in particular in quantum cryptography. Many of the modern security proofs for quantum key distribution are based on an uncertainty relation (see, e.g. [29]). They are also at the heart of security proofs in the bounded quantum storage model [11,10,7]. An uncertainty relation is a statement about a guaranteed uncertainty in the outcome of a measurement in a randomly chosen basis. We refer the reader to [33] for a survey on uncertainty relations.

Uncertainty relation for BB84 measurements Here we consider a system A^n of n qubits. Then we measure each one of these qubits in either the standard basis (labeled 0 with vector $|0\rangle, |1\rangle$) or the Hadamard basis (labeled 1 with vectors $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$). More precisely, choose a random vector $\Theta^n \in \{0,1\}^n$ and measure qubit i in the basis specified by the i-th component of $\Theta^n = \Theta_1, \dots, \Theta_n$. Call the outcome X_i. An uncertainty relation is a statement about the amount of uncertainty in the random variable $X^n = X_1, \dots, X_n$ given the knowledge of the basis choice Θ^n. The uncertainty is often measured in terms of the Shannon entropy. However, for the applications we consider here, the measure of uncertainty needs to be stronger, i.e., we should use a higher order entropy like $\mathrm{H}_{\min}$ or H_2. Such an uncertainty relation has been established in [10]:

$$\mathrm{H}^{\varepsilon}_{\min}(X^n|\Theta^n) \gtrapprox n/2. \tag{18}$$

The way this uncertainty relation was used in the context of the bounded storage model was to apply a chain rule to (18) to obtain $\mathrm{H}^{\varepsilon}_{\min}(X^n|E\Theta^n) \gtrapprox n/2 - \log|E|$. There are two reasons for this inequality to be unsatisfactory: it depends on the dimension of E rather than on the correlations between A^n and E, and it becomes trivial when $\mathrm{H}_2(A^n|E) < -n/2$ as this implies $\log|E| > n/2$. An uncertainty relation for measurements in the six-state bases that depends on $\mathrm{H}_2(A^n|E)$ was established in [7], but it also becomes trivial when $\mathrm{H}_2(A^n|E) < -0.586n$.

It is simple to see that if the system A^n is maximally entangled with some system E, then the outcome X^n of this measurement can be perfectly predicted by having access to E. In other words, if the conditional entropy $\mathrm{H}_2(A^n|E) = -n$, then X^n can be correctly guessed with probability 1. The following theorem provides a converse: if $\mathrm{H}_2(A^n|E) \geqslant -(1-\varepsilon)n$ for $\varepsilon > 0$, then X^n cannot be guessed with probability better than $2^{-n\delta(\varepsilon)}$ with $\delta(\varepsilon) > 0$ whenever $\varepsilon > 0$.

Theorem 5 *Let $\rho_{A^nE} \in \mathcal{S}(A^nE)$ where A^n is an n-qubit space and define $h_2 = \frac{\mathrm{H}_2(A^n|E)_\rho}{n}$. Then we have*

$$\mathrm{H}_2(X^n|E\Theta^n)_\rho \geqslant n\gamma(h_2) - 1$$

where $\rho_{X^nE\Theta^n} = \frac{1}{2^n}\sum_{x^n\in\{0,1\}^n,\theta^n\in\{0,1\}^n} |x^n\rangle\langle x^n| \langle x^n|H^{\theta^n}\rho_{A^nE}H^{\theta^n}|x^n\rangle \otimes |\theta^n\rangle\langle\theta^n|$ is the state obtained when system A^n is measured in the basis defined in the register Θ^n and the function γ (plot in Figure 2) is defined by $\gamma(h_2) = h_2$ if $h_2 \geq 1/2$ and $\gamma(h_2) = g^{-1}(h_2)$ if $h_2 < 1/2$ with $g(\alpha) = h(\alpha) + \alpha - 1$.

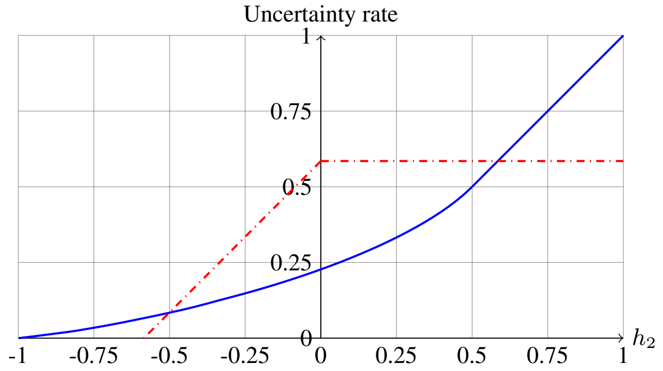

Fig. 2. Plot of the function $\gamma(h_2)$ (—) from Theorem 5 giving a lower bound on the uncertainty of the outcome of BB84 measurement as a function of the entropy rate h_2 of the state being measured. For comparison, we also plot the uncertainty rate function proved in [7] for measurements in the six-state bases (-·-·).

Proof. We apply Theorem 1 with $\mathcal{M}_{A^n \to X^n \Theta^n} = \mathcal{N}^{\otimes n}$ where $\mathcal{N}(\rho) = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}, \theta \in \{0,1\}} |\theta\rangle\langle\theta| \otimes |x\rangle\langle x| \langle x|H^\theta \rho H^\theta|x\rangle$. We have

$$
\begin{aligned}
&2^{-\mathrm{H}_2(X^n\Theta^n|E)_{\mathcal{M}(\rho)}} = \mathrm{Tr}\left[\left(\rho_E^{-1/4}(\mathcal{N}^{\otimes n} \otimes \mathrm{id})(\rho_{A^nE})\rho_E^{-1/4}\right)^2\right] \\
&= \frac{1}{2^n} \sum_{\theta^n \in \{0,1\}^n} \mathrm{Tr}\left[\left(\rho_E^{-1/4} \sum_{x^n \in \{0,1\}^n} |\theta^n\rangle\langle\theta^n| \otimes |x^n\rangle\langle x^n| \langle x^n|H^{\theta^n} \rho H^{\theta^n}|x^n\rangle \rho_E^{-1/4}\right)^2\right] \\
&= 2^{-\mathrm{H}_2(X^n|E\Theta^n)_\rho}.
\end{aligned}
$$

We then evaluate the state $(\mathcal{N}^\dagger \circ \mathcal{N} \otimes \mathrm{id})(\Phi) = \frac{1}{2}\left(\Phi_0 + \frac{1}{2}\Phi_1 + \frac{1}{2}\Phi_3\right)$, where Φ_i are defined Section 2.3. In the notation of Theorem 1, we have for the map $\mathcal{M}$ and for $s \in \{0,1,3\}^n$, $\lambda_s = \frac{1}{2^n} \cdot \frac{1}{2^{|s|}}$. For $s \notin \{0,1,3\}^n$, $\lambda_s = 0$. As a result, when applying Theorem 1, it is natural to choose the partition $\mathfrak{S}_+ \cup \mathfrak{S}_-$ of the form $\mathfrak{S}_+ = \{s \in [d^2]^n : |s| \leqslant \ell_0\}$ and $\mathfrak{S}_- = \{s \in [d^2]^n : |s| > \ell_0\}$ for a value of $\ell_0 \in \{0, \ldots, n\}$ to be chosen as a function of h_2. We obtain for any ℓ_0

$$
2^{-\mathrm{H}_2(X^n|E\Theta^n)_\rho} \leqslant \sum_{\ell=0}^{\ell_0} \binom{n}{\ell} 2^{-h_2 n - n} + 2^{-\ell_0 - 1}\delta_{\ell_0 \leq n-1}\,, \tag{19}
$$

where $\delta_{\ell_0 \leq n-1} = 1$ if $\ell_0 \leq n-1$ and 0 if $\ell_0 = n$. If $h_2 \geqslant 1/2$, let $\ell_0 = n$, in which case we obtain a bound of $2^{-\mathrm{H}_2(X^n|E\Theta^n)_\rho} \leqslant 2^{-h_2 n}$.

If $h_2 < 1/2$, then we are going to choose $\ell_0 \leqslant n/2$. Define the function $g(\alpha) = h(\alpha) + \alpha - 1$ and let $\alpha_0 \leqslant 1/2$ be such that $g(\alpha_0) = h_2$. We then choose

$\ell_0 = \lfloor \alpha_0 n \rfloor$. As a result,

$$\sum_{\ell=0}^{\ell_0} \binom{n}{\ell} 2^{-h_2 n - n} \leqslant 2^{n(h(\ell_0/n) - h_2 - 1)}$$
$$\leqslant 2^{n(h(\alpha_0) - h_2 - 1)} = 2^{n(-\alpha_0 + 1 + h_2 - h_2 - 1)} = 2^{-\alpha_0 n}.$$

In addition, we have $2^{-\ell_0 - 1} \leqslant 2^{-\alpha_0 n}$. Using these bounds in (19), we obtain in this case $2^{-\mathrm{H}_2(X^n|E\Theta^n)_\rho} \leqslant 2^{-\alpha_0 n + 1}$. Taking the logarithm leads to the desired result.

The following corollary expresses the uncertainty relation described in Theorem 5 in terms of min-entropies, which will be more convenient for the cryptographic applications.

Corollary 6 *Using the same notation as in Theorem 5, we have*

$$\mathrm{H}_{\min}(X^n|E\Theta^n)_\rho \geqslant \frac{1}{2}(n\gamma(h_{\min}) - 1), \tag{20}$$

where $h_{\min} = \frac{\mathrm{H}_{\min}(A^n|E)_\rho}{n}$*. Moreover, for any* $\varepsilon \in (0,1]$*, we have* $\mathrm{H}^{\varepsilon}_{\min}(X^n|E\Theta^n)_\rho \geqslant n\gamma(h_{\min}) - 1 - \log\frac{2}{\varepsilon^2}$.

4.4 Security in the noisy-storage model

General noisy storage model We now use our new uncertainty relations to prove that the primitive weak string erasure can be secure as soon as one of the parties has a memory that cannot reliably store n qubits. In weak string erasure, the objective is to generate a string X^n such that Alice holds X^n and Bob holds a random subset $I \subseteq [n]$ and the bits X_I of X^n corresponding to the indices in I. Randomly chosen here means that each index $i \in [n]$ has probability $1/2$ of being in I. The security criterion is that at the end of the protocol, a cheating Bob should have a state satisfying $\mathrm{H}_{\min}(X^n|B) \geqslant \lambda n$ where B represents Bob's system, and a cheating Alice should not learn anything about I. To summarize all relevant parameters, we speak of an (n, λ)-WSE scheme and refer to [17] for a definition. [6] It is proved in [17] that bit commitment can be implemented using weak string erasure and classical communication.

Protocol. The protocol we use here is the same as the one of [17]. Alice prepares a random string $X^n \in \{0,1\}^n$ and encodes each bit X_i in either the standard basis $\Theta_i = 0$ or the Hadamard basis $\Theta_i = 1$, each with probability $1/2$. Then Bob measures these qubits in randomly chosen bases Θ'_i. After the waiting time, Alice reveals both X^n and Θ^n. The set I is defined by $I = \{i : \Theta_i = \Theta'_i\}$. For a more detailed description of the protocol, we refer the reader to [17].

To state the result, we first define the notion of *channel fidelity* introduced by [3] which is perhaps the most widely used quantity to measure how good a channel is at sending quantum information. For a channel $\mathcal{N} : \mathcal{S}(Q) \to \mathcal{S}(Q')$, the channel fidelity F_c quantifies how well $\mathcal{N}$ preserves entanglement with a reference:

$$F_c(\mathcal{N}) = F(\Phi^N_{Q'A}, [\mathcal{N} \otimes \mathrm{id}_A]\,(\Phi^N_{QA})), \tag{21}$$

[6] Note that the original definition includes a security error ε, which in our case is $\varepsilon = 0$.

where Φ^N_{QA} is a normalized maximally entangled state. For example, one way of defining the (one-shot) quantum capacity with free classical forward communication of a channel $\mathcal{F}_{B\to C}$ is by the maximum of $\log|Q|$ over all encodings $\mathcal{E}: \mathcal{S}(Q) \to \mathcal{S}(B \otimes M)$ and decodings $\mathcal{D}: \mathcal{S}(C \otimes M) \to \mathcal{S}(Q')$ such that $F_c(\mathcal{D} \circ (\mathcal{F} \otimes \overline{\mathrm{id}}_M) \circ \mathcal{E}) \geqslant 1 - \varepsilon$ for small enough ε. Here $\overline{\mathrm{id}}_M$ refers to a noiseless classical channel.

The following theorem states that as soon as the storage device of Bob cannot send quantum information with reliability better than η, then we can perform two-party computation securely provided $\eta \leqslant 2^{-c(\log^2 n + \log n \log(1/\varepsilon))}$ for some large enough constant c. Previously, this was only known when $\eta < 2^{-(2-\log 3)n}$ [7]. Before that, security was analyzed in terms of other more specific quantities like the ability of the storage device to transmit *classical* information [17], or to simulate noiseless quantum channels [6]. As the ability to transmit quantum information is a stronger requirement, the results we prove here apply to more general settings and give better bounds.

Theorem 7 *Let Bob's storage device be given by $\mathcal{F} : \mathcal{S}(\mathcal{H}_{\mathrm{in}}) \to \mathcal{S}(B)$, and let $\eta \in (0,1)$. Assume that we have*

$$\max_{\mathcal{D},\mathcal{E}} F_c(\mathcal{D} \circ (\mathcal{F} \otimes \overline{\mathrm{id}}_M) \circ \mathcal{E})^2 \leqslant \eta \tag{22}$$

where the maximum is over all quantum channels $\mathcal{E} : \mathcal{S}\left((\mathbb{C}^2)^{\otimes n}\right) \to \mathcal{S}(\mathcal{H}_{\mathrm{in}} \otimes M)$ and $\mathcal{D} : \mathcal{S}(B \otimes M) \to \mathcal{S}((\mathbb{C}^2)^{\otimes n})$.

Then, the protocol described above implements a (n, λ)-WSE for

$$\lambda = \frac{1}{2}\left(\gamma\left(-1 + \log(1/\eta)/n\right) - \frac{1}{n}\right).$$

Proof. The proof of correctness of the protocol, and security against dishonest Alice is identical to [17] and does not lead to any error terms. For the security against dishonest Bob, it is convenient to imagine a purification of the protocol, in which Alice prepares n EPR pairs $\Phi^N_{A^n Q}$, where she sends Q to Bob and later measures her n qubits A^n in randomly chosen BB84 bases. Bob's general attack can be modeled as performing some encoding on Q and obtaining some classical output M together with a quantum output that has to be stored in the device described by $\mathcal{F}$. The output of this device is denoted B. We use the uncertainty relation in Equation (20), with $E = BM\Theta^n$ on $\rho_{A^n BM\Theta^n}$. In order to do that, we first derive a lower bound on $h_{\min} = \frac{\mathrm{H}_{\min}(A^n|BM\Theta^n)_\rho}{n}$. Note that because Θ^n is independent of $A^n BM$, we have $\mathrm{H}_{\min}(A^n|BM\Theta^n)_\rho = \mathrm{H}_{\min}(A^n|BM)_\rho$. We now use Condition (22) to obtain a lower bound on $\mathrm{H}_{\min}(A^n|BM)$. In fact, we use an operational interpretation of the conditional min-entropy due to [16]:

$$\mathrm{H}_{\min}(A^n|BM)_\rho = -\log|A^n| \max_{\Lambda_{BM\to\bar{A}^n}} F(\Phi^N_{A^n\bar{A}^n}, \mathrm{id}_{A^n} \otimes \Lambda(\rho_{A^n BM}))^2 , \tag{23}$$

where $\Phi^N_{A^n\bar{A}^n}$ is the normalized maximally entangled state across $A^n\bar{A}^n$. That is, the min-entropy is directly related to the "amount" of entanglement between A^n and BM. The map Λ in (23) can be understood as a decoding attack $\mathcal{D}$ aiming to restore entanglement with Alice.

Further, note that the expression in (23) is the same as

$$\max_{\mathcal{D},\mathcal{E}} F\left(\Phi^N_{A^n B}, \mathrm{id}_{A^n} \otimes \left[\mathcal{D} \circ (\mathcal{F} \otimes \overline{\mathrm{id}}_M) \circ \mathcal{E}\right] (\Phi^N_{A^n Q})\right) = \max_{\mathcal{D},\mathcal{E}} F_c(\mathcal{D} \circ (\mathcal{F} \otimes \overline{\mathrm{id}}_M) \circ \mathcal{E}) \, .$$

By the assumption on the storage device $\mathcal{F}$, we obtain that for any encoding $\mathcal{E}$ and decoding $\mathcal{D}$ attack of Bob

$$\mathrm{H}_{\min}(A^n|BM)_\rho \geqslant -\log 2^n F_c(\mathcal{D} \circ (\mathcal{F} \otimes \overline{\mathrm{id}}_M) \circ \mathcal{E})^2 \geqslant -\left(n - \log(1/\eta)\right) .$$

Then, using the uncertainty relation (20), we obtain $\mathrm{H}_{\min}(X^n|BM\Theta^n)_\rho \geq \frac{1}{2}\left(n\gamma\left(-1 + \log(1/\eta)/n\right) - 1\right)$, which proves the desired result.

Special case: bounded storage model The next theorem simply states the result in the important special case of the bounded storage model.

Theorem 8 (WSE in the bounded storage model) *If Alice has q qubits of quantum memory then the protocol described in the previous section implements (n, λ)-WSE with $\lambda = \frac{1}{2}\left(\gamma(-q/n) - \frac{1}{n}\right)$.*

Previously, in this case, security was only proven when $q < \frac{2n}{3}$ [20] with a variant of this protocol that uses a six-state encoding. Using simple estimates for the function γ, the previous theorem shows that $q < n - c\log^2 n$ for some large enough c would be sufficient to perform WSE securely. Using the construction of [17], this leads to a secure bit commitment provided $q < n - c\log^2 n - c\log n \log(1/\varepsilon)$ for some large enough constant c and where ε is the failure probability.

Acknowledgments We thank Oleg Szehr, Marco Tomamichel and Thomas Vidick for useful discussions. OF is supported by the European Research Council grant No. 258932. SW thanks ETH Zürich for their hospitality. SW is supported by the National Research Foundation and the Ministry of Education, Singapore. FD acknowledges support from the Danish National Research Foundation and The National Science Foundation of China (under the grant 61061130540) for the Sino-Danish Center for the Theory of Interactive Computation, within which part of this work was performed; and also from the CFEM research center (supported by the Danish Strategic Research Council) within which part of this work was performed.

References

1. S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002. arXiv:quant-ph/0103162.
2. H. Barnum and E. Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *J. Math. Phys.*, 43:2097, 2002.
3. H. Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. *IEEE Trans. Inform. Theory*, 46:1317–1329, 2000. arXiv:quant-ph/9809010.
4. A. Ben-Aroya, O. Regev, and R. de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In *Proc. IEEE FOCS*, 2008. arXiv:0705.3806.

5. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. International Conference on Computers, Systems and Signal Processing*, 1984.
6. M. Berta, F. Brandao, M. Christandl, and S. Wehner. Entanglement cost of quantum channels. 2011. arXiv:1108.5357.
7. M. Berta, O. Fawzi, and S. Wehner. Quantum to classical randomness extractors. In *Proc. CRYPTO*, volume 7417 of *LNCS*, pages 776–793. Springer Verlag, 2012. arXiv:1111.2026.
8. N. J. Bouman, S. Fehr, C. González-Guillén, and C. Schaffner. An all-but-one entropic uncertainty relation, and application to password-based identification. In *Proc. TQC*, volume 7582, pages 29–44. 2013. arXiv:1105.6212.
9. C. Cachin and U. M. Maurer. Unconditional security against memory-bounded adversaries. In *Proc. CRYPTO*, volume 1294 of *LNCS*, pages 292–306, 1997.
10. I. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Proc. CRYPTO*, volume 4622 of *LNCS*, pages 360–378. 2007. arXiv:quant-ph/0612014.
11. I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *Proc. IEEE FOCS*, pages 449–458, 2005. arXiv:quant-ph/0508222.
12. I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *Proc. CRYPTO*, Springer Lecture Notes in Computer Science, pages 342–359, 2007. arXiv:0708.2557.
13. F. Dupuis, O. Fawzi, and S. Wehner. Entanglement sampling and applications. 2013. arXiv:1305.1316.
14. S. Dziembowski and U. Maurer. On generating the initial key in the bounded-storage model. In *Proc. EUROCRYPT*, volume 3027 of *LNCS*, pages 126–137, 2004.
15. R. Impagliazzo, L. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proc. ACM STOC*, pages 12–24. ACM, 1989.
16. R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inform. Theory*, 55:4674–4681, 2009. arXiv:0807.1338.
17. R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Trans. Inform. Theory*, 58(3):1962 –1984, 2012. arXiv:0906.1030.
18. R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. *IEEE Trans. Inform. Theory*, 57(7):4760 –4787, 2011. arXiv:0712.4291.
19. H-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410, 1997.
20. P. Mandayam and S. Wehner. Achieving the physical limits of the bounded-storage model. *Phys. Rev. A*, 83:022329, 2011. arXiv:1009.1596.
21. U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *J. Cryptol.*, 5:53–66, 1992.
22. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, 1997.
23. N. Ng, S. Joshi, C. Chia, C. Kurtsiefer, and S. Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Comm.*, 3:1326, 2012.
24. N. Nisan and D. Zuckerman. Randomness is linear in space. *J. Comput. Syst. Sci.*, 52(1):43 – 52, 1996.
25. R. Renner. Security of quantum key distribution. *Int. J. Quantum Inf.*, 6:1, 2008. arXiv:quant-ph/0512258.
26. C. Schaffner, B. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Inf. Comput.*, 9:11, 2008. arXiv:0807.1333.
27. M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zürich, 2012. arXiv:1203.2142.

28. M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. *IEEE Trans. Inform. Theory*, 55:5840–5847, 2009. arXiv:0811.1221.
29. M. Tomamichel, C.C.W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nat. Comm.*, 3:634, 2012.
30. S. Vadhan. Pseudorandomness.
31. S. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *J. Cryptol.*, 17:43–77, 2004.
32. S. Wehner, C. Schaffner, and B. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, 2008. arXiv:0711.2895.
33. S. Wehner and A. Winter. Entropic uncertainty relations—a survey. *New J. Phys.*, 12:025009, 2010. arXiv:0907.3704.
34. J. Wullschleger. Bitwise quantum min-entropy sampling and new lower bounds for random access codes. 2010. arXiv:1012.2291.