Min-entropy uncertainty relation for finite-size cryptography

Nelly Huei Ying Ng,[1,2,*] Mario Berta,[3,†] and Stephanie Wehner[1,‡]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2] *School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371*
[3] *Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*

(Received 7 June 2012; published 15 October 2012)

Apart from their foundational significance, entropic uncertainty relations play a central role in proving the security of quantum cryptographic protocols. Of particular interest are therefore relations in terms of the smooth min-entropy for Bennett-Brassard 1984 (BB84) and six-state encodings. The smooth min-entropy $H_{\min}^{\epsilon}(X/B)$ quantifies the negative logarithm of the probability for an attacker B to guess X, except with a small failure probability ϵ. Previously, strong uncertainty relations were obtained which are valid in the limit of large block lengths. Here, we prove an alternative uncertainty relation in terms of the smooth min-entropy that is only marginally less strong but has the crucial property that it can be applied to rather small block lengths. This paves the way for a practical implementation of many cryptographic protocols. As part of our proof we show tight uncertainty relations for a family of Rényi entropies that may be of independent interest.

DOI: 10.1103/PhysRevA.86.042315 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Entropic uncertainty relations form a modern way to characterize the uncertainty inherent in several quantum measurements. As opposed to more traditional methods of capturing the notion of uncertainty, they have the advantage that they are able to quantify uncertainty solely in terms of the measurements we consider and are independent of the state to be measured. To see this clearly, let us explain the notion of entropic uncertainty in more detail (also, see [1] for a survey). Suppose we are given a state ρ on which we can make one of L possible measurements with outcomes labeled $x \in \mathcal{X}$. Let $p_{x|\rho,\theta}$ denote the probability of observing outcome x when making the measurement labeled θ on the state ρ. For each measurement, we can consider some form of entropy of the outcome distribution such as the Shannon entropy $H(X|\Theta = \theta) = -\sum_x p_{x|\rho,\theta} \log_2 p_{x|\rho,\theta}$. An entropic uncertainty relation in terms of the Shannon entropy is then determined by the average ($p_\theta = 1/L$) over the individual entropies. More precisely, such a relation states that, for *all* states ρ,

$$\frac{1}{L}\sum_{\theta} H(X|\Theta = \theta) = H(X|\Theta) \geqslant c, \tag{1}$$

where c is a constant that depends solely on the measurements. For example, if ρ is a single qubit state and we consider $L = 2$ measurements in the Pauli σ_X and σ_Z eigenbases, we have $c = \frac{1}{2}$ [2]. To see why (1) for $c > 0$ is indeed connected with uncertainty, note that if the outcome is certain with respect to some measurement θ on the state ρ [$H(X|\Theta = \theta) = 0$], then the outcome of at least one other measurement $\theta' \neq \theta$ is uncertain [$H(X|\Theta = \theta') > 0$]. Similarly, the larger the value of c is, the more uncertain these outcomes are. The value of c thus give a natural measure of the incompatibility of different sets of measurements. *Strong* uncertainty relations have the property that c is large.

From a cryptographic perspective, uncertainty relations in terms of the minimum entropy (min-entropy) $H_{\min}(X|\Theta = \theta) = -\log_2 \max_x p_{x|\rho,\theta}$ are of particular interest since the min-entropy determines how many random bits (key) can be extracted from X [3]. In a cryptographic setting, it is thereby often interesting to consider a slight extension of the notion of uncertainty relations above. Namely, instead of measuring one state ρ, we imagine that an adversary prepares with some probability p_k a state ρ_k (labeled by some classical label $K = k$) which we subsequently measure. Since entropic uncertainty relations hold for any state, they do, in particular, hold for any state ρ_k that the adversary may have prepared. Yet the distribution $\{p_{x|k\theta}\}$ over measurement outcomes may, of course, depend on k. Uncertainty relations with respect to such classical side information K thus take the form

$$H_{\min}(X|\Theta K) \geqslant c' \tag{2}$$

for some constant c' depending on the measurements we make. Averaging over bases Θ and classical information K, the conditional min-entropy is given by (see the Appendix)

$$H_{\min}(X|\Theta K) = -\log \sum_{\theta} p_\theta \sum_{k} p_{k|\theta} \max_{x} p_{x|k\theta}. \tag{3}$$

For example, imagine that ρ is an n-qubit state and we perform one of the 2^n possible measurements given by measuring each qubit independently in one of the two Bennett-Brassard 1984 (BB84) bases [4], i.e., in the eigenbasis of Pauli σ_x or σ_z. It is known that in this case $c' = -n \log_2[1/2 + 1/(2\sqrt{2})] \approx 0.22n$ for any K. This is also optimal as there exists a state that attains this lower bound.

Measurements in BB84 bases are indeed common in many quantum cryptographic protocols. In particular, they are used in two-party cryptographic protocols in the bounded [5,6] and noisy-storage models [7–9]. These models allow for the secure implementation of any two-party cryptographic primitive under the assumption that the adversary's quantum memory device is bounded and imperfect. This includes interesting

[*] nell0002@e.ntu.edu.sg
[†] berta@phys.ethz.ch
[‡] wehner@nus.edu.sg

primitives such as oblivious transfer, bit commitment, and even secure identification of, e.g., a user of an ATM machine. The security of all protocols in this model crucially rests on the existence of uncertainty relations in terms of min-entropy [5–11]. Yet the value of $c' \approx 0.22n$ for BB84 bases is usually too low to be cryptographically useful. In particular, a low value for c' means that the adversary's memory must be very limited and/or noisy for security to be possible [5,6,9] at all. Furthermore, a low value of c' means that any experiment implementing such protocols can tolerate only a small amount of bit-flip errors and losses [8,12,13]. For instance, if p_{err} is the bit-flip error on the channel connecting Alice and Bob, then security for the cryptographic primitive known as oblivious transfer is possible if $c' - h(p_{\text{err}}) > 0$ [12,14], where $h(p) = -p \log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy.

Motivated by this need to obtain a strong uncertainty relation for BB84 bases, that is, a large c', the authors of [6] considered the so-called *smooth* min-entropy $H^{\varepsilon}_{\min}(X|\Theta K)$. Intuitively, a lower bound c' on this quantity tells us that we do indeed have min-entropy at least c', except for some small error parameter $\varepsilon > 0$. Formally, this quantity is defined as (see the Appendix)

$$H^{\varepsilon}_{\min}(X|\Theta K)_{\rho} = \sup_{\rho'} H_{\min}(X|\Theta K)_{\rho'}, \tag{4}$$

where ρ' is ϵ close to ρ in terms of the purified distance [15].

It turns out that at the expense of such a small error ε, a much stronger uncertainty relation can indeed be obtained. In particular, it has been shown [6] that for measurements in the BB84 bases and any $\delta \in (0,\frac{1}{2}]$,

$$H^{\varepsilon}_{\min}(X|\Theta K) \geqslant n\left(\tfrac{1}{2} - \delta\right), \tag{5}$$

where

$$\varepsilon = \exp\left[-\frac{\delta^2 n}{128\left(2 + \log_2 \frac{2}{\delta}\right)^2}\right]. \tag{6}$$

Using this relation in a cryptographic protocol only yields an additional error ε in the overall security error, and it is widely employed in the protocols of [6,9,10,12–14].

From a theoretical (asymptotic) viewpoint, this uncertainty relation is certainly sufficient. Yet, when it comes to putting any of such protocols into a practical experiment, it has a small caveat: whereas ε decreases exponentially in the number of qubits n, for a large amount of uncertainty, i.e., $c' = 1/2 - \delta \approx 1/2$, the convergence is extremely slow. For example, for $\delta = 0.0106$ [13] corresponding to $c' = 0.4894$, we need $n \geqslant 2.39 \times 10^8$ to even have $\varepsilon = 0.1$. In an experiment using weak coherent pulses, with a frequency of 1 GHz and Poisson parameter $\mu = 1$, it takes approximately 2.5 s to generate such an n [13] if there are absolutely no losses of any kind. However, compared to the generation time, a more significant inconvenience is that the classical postprocessing of such large block lengths is time-consuming.

II. RESULTS

To implement the aforementioned protocols, it would thus be desirable to have a relation that is useful for significantly smaller values of n. Here, we prove such a relation that makes a statement for any desirable *fixed* error $\varepsilon > 0$. In particular, we show that, for any n qubit quantum state ρ and measurements in BB84 bases,

$$H^{\varepsilon}_{\min}(X|\Theta K) \geqslant n c_{BB84}, \tag{7}$$

where

$$c_{BB84} := \max_{s\in(0,1]} \frac{1}{s}[1 + s - \log_2(1 + 2^s)] - \frac{1}{sn}\log_2\frac{2}{\epsilon^2}. \tag{8}$$

At first glance, it may be hard to see that c_{BB84} is indeed large. However, applying it to the example from [13] (see above) by plugging in $s = 0.1$ demonstrates that for the same $\varepsilon = 0.1$, $c_{BB84} \geqslant 0.4894$ whenever $n \geqslant 2.36 \times 10^4$. Comparing this with calculations in the previous section, the required block length n is approximately 10^{-4} times smaller. Figure 1 provides a comparison of these two bounds. We see that even for large ϵ, the required bound on the block length n given by (6) is large.

Our relation can readily be applied to any BB84-based two-party protocols in the bounded (or noisy) storage model and enables experiments for significantly smaller values of n. For example, it enables the experimental implementation of [16] with $n = 2.5 \times 10^5$ instead of $n > 10^9$ for the same error parameter ε.

Furthermore our relation can be extended to the case of six-state protocols, i.e., measurements in Pauli σ_x, σ_z, and σ_y eigenbases as suggested in [10,11,14]. For this case we obtain

$$H^{\varepsilon}_{\min}(X|\Theta K) \geqslant n c_6\ , \tag{9}$$

where

$$c_6 := \max_{s\in(0,1]} -\frac{1}{s}\log_2\left[\frac{1}{3}(1 + 2^{1-s})\right] - \frac{1}{sn}\log_2\frac{2}{\epsilon^2}. \tag{10}$$

This yields a similar improvement over the relation analogous to (5) proven in [6].

A crucial step in our proof is to show *tight* uncertainty relations for conditional Rényi entropies of order α, denoted by $H_{\alpha}(A|B)$. These may be of independent interest. Previously,

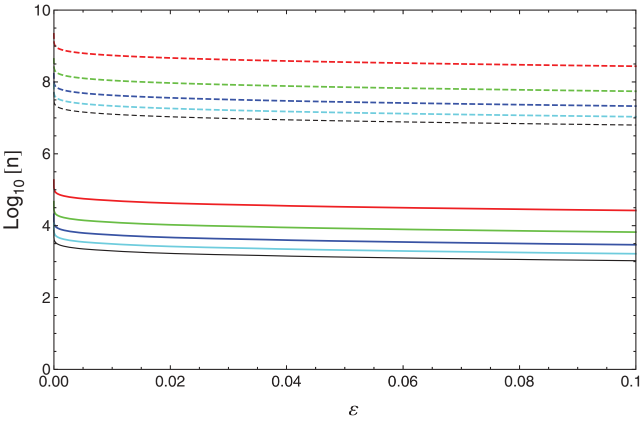

FIG. 1. (Color online) The minimal required block length n on a logarithmic scale of base 10 in order to achieve an error parameter ϵ. The dashed curves are plotted for the previous known bound (6), while the solid lines are obtained from our present analysis (8). The different colors represent the fixed values of the lower bound c', with values 0.45, 0.46, 0.47, 0.48, and 0.49, from bottom to top. As c' increases, the plotted bounds get relatively higher.

such relations were only known for single qudit measurements for $\alpha \to 1$, $\alpha = 2$, and $\alpha \to \infty$ (see, e.g., [1,17,18]). More precisely, we show that for measurements on n-qubit states ρ in BB84 bases, the minimum values of the conditional Rényi entropies for any $\alpha \in (1,2]$ are

$$\min_{\rho} H_\alpha(X|\Theta)_{\rho|\rho} = n\frac{\alpha - \log_2(1+2^{\alpha-1})}{\alpha - 1}, \qquad (11)$$

where

$$H_\alpha(A|B)_{\rho|\rho} := \frac{1}{1-\alpha}\log_2 \mathrm{tr}\left[\rho_{AB}^{\alpha}(\mathbb{I}_A \otimes \rho_B)^{1-\alpha}\right]. \qquad (12)$$

Similarly, for measurements in the six-state bases,

$$\min_{\rho} H_\alpha(X|\Theta)_{\rho|\rho} = n\frac{\log_2 3 - \log_2(1+2^{2-\alpha})}{\alpha - 1}. \qquad (13)$$

III. PROOF

Let us now explain the proof of our results. A technical derivation including all details may be found in the Appendix. For simplicity, we restrict ourselves to the case of BB84 measurements. An extension for six-state protocols is analogous and can be found in the Appendix. To obtain (8) we proceed in four steps. First, we will prove a tight uncertainty relation in terms of the α-Rényi entropy when ρ is just an $n = 1$ qubit state. Second, we show how to extend this result to an uncertainty relation for $n > 1$ qubits, giving us (11). The third step is to reintroduce K as outlined in the Introduction. Finally, we relate the Rényi entropies of order $\alpha \in (1,2]$ to the smooth min-entropy.

Step 1: A single qubit uncertainty relation. For the case when A and B are classical the conditional α-Rényi entropy reduces to the simple form

$$H_\alpha(A|B)_{\rho|\rho} = \frac{1}{1-\alpha}\log_2 \sum_b p_{B=b} \sum_a p^{\alpha}_{A=a|B=b}. \qquad (14)$$

The relevant α-Rényi entropy for a single qubit state ρ_k (where k denotes some classical information associated with the state ρ_k) is

$$\begin{aligned} H_\alpha(X|\Theta)_{\rho_k|\rho_k} &= \frac{1}{1-\alpha}\log_2 \sum_{\theta\in\{0,1\}} p_\theta \sum_{x\in\{0,1\}} p^{\alpha}_{x|k\theta} \\ &= \frac{1}{1-\alpha}\log_2\left[\frac{1}{2}\sum_{\theta\in\{0,1\},x\in\{0,1\}} p^{\alpha}_{x|k\theta}\right]. \qquad (15) \end{aligned}$$

Here $p_{x|k\theta} := \mathrm{tr}(M_{x|\theta}\rho_k)$, where $M_{x|\theta}$ denotes the measurement operator

$$M_{x|\theta} = \mathbf{H}^{\theta}|x\rangle\langle x|\mathbf{H}^{\theta}, \qquad (16)$$

with $\mathbf{H}$ being the Hadamard matrix. To minimize the α-Rényi entropy for values of $\alpha \in (1,2]$, it is sufficient to maximize the summation term. Defining

$$P(X|\Theta)_{\rho_k} = \frac{1}{2}\sum_{\theta\in\{0,1\},x\in\{0,1\}} p^{\alpha}_{x|k\theta}\ , \qquad (17)$$

we first rewrite $p_{x|k\theta}$ as functions of two variables: $g_x := \mathrm{tr}(\sigma_x\rho_k)$ and $g_z := \mathrm{tr}(\sigma_z\rho_k)$. The Bloch sphere condition for a qubit gives $g_x^2 + g_y^2 + g_z^2 \leqslant g_x^2 + g_z^2 \leqslant 1$, which serves as a constraint in maximizing (17). Switching to spherical coordinates and evaluating the partial derivatives of (17) according to multiple independent variables, we prove

$$\begin{aligned} H_\alpha(X|\Theta)_{\rho_k|\rho_k} &\geqslant \frac{1}{1-\alpha}\log_2\left[\frac{1}{2^{1+\alpha}}(2^\alpha + 2)\right] \\ &= \frac{1}{\alpha-1}[\alpha - \log_2(1+2^{\alpha-1})]. \qquad (18) \end{aligned}$$

Moreover, the minimal α-Rényi entropy is achieved on an eigenstate of either measurement basis.

Step 2: A relation for n qubits. To extend the one qubit uncertainty relation to multiple qubits, the central problem is to prove that the lower bound on the conditional entropy scales linearly with the block length n. This essentially implies that for a system of n qubits, the entanglement across qubits does not give rise to a lower minimal α-Rényi entropy. In our analysis, we show this by first considering the last qubit measured, conditioned on all the previous $n - 1$ measurement bases and values. That is, we consider an n-qubit normalized density operator ρ_{ABk}, where B denotes the last qubit and A is the remaining $n - 1$ qubits, and write

$$P(X_B|\Theta)_{\rho_{ABk}} = \frac{1}{2}\sum_{\theta_B,x_B\in\{0,1\}} p^{\alpha}_{x_B|\theta_B x_A \theta_A k}, \qquad (19)$$

where $p_{x_B|\theta_B x_A\theta_A k} = \mathrm{tr}(M_{x_B|\theta_B}\sigma_B)$, with the corresponding normalized density operator

$$\sigma_B = \mathrm{tr}_A\left[\frac{M_{x_A|\theta_A}\rho_{ABk}M^{\dagger}_{x_A|\theta_A}}{\mathrm{tr}[M_{x_A|\theta_A}\rho_{ABk}M^{\dagger}_{x_A|\theta_A}]}\right]. \qquad (20)$$

Since the uncertainty relation for one qubit (18) holds for any density operator, it holds in particular for σ_B. By induction, it is then easily shown that the minimal entropy is additive.

Step 3: Classical side information K. After steps 1 and 2, we established a tight uncertainty relation for a binary string X^n conditioned on the basis string Θ^n. Namely, we have

$$H_\alpha(X^n|\Theta^n)_{\rho_k|\rho_k} \geqslant n\frac{1}{\alpha-1}[\alpha - \log_2(1+2^{\alpha-1})] \qquad (21)$$

for any n-qubit state ρ_k. In this step, we obtain the conditioning with relation to classical side information K. In other words, we need to evaluate $H_\alpha(X|\Theta K)_{\rho|\rho}$ with

$$\rho = \sum_{\theta\in\{0,1\}^n} p_\theta|\theta\rangle\langle\theta| \sum_k p_{k|\theta}\rho_k \sum_{x\in\{0,1\}^n} p_{x|\theta k}|x\rangle\langle x|\ . \qquad (22)$$

By observing the independence of Θ and K, we show that the bounds of these values coincide, implying that

$$H_\alpha(X|\Theta K)_{\rho|\rho} \geqslant n\frac{1}{\alpha-1}[\alpha - \log_2(1+2^{\alpha-1})]. \qquad (23)$$

Step 4: Relation to the min-entropy. As motivated previously, the final desired measure of entropy is the *smooth* min-entropy $H^{\varepsilon}_{\min}(X|\Theta K)_\rho$. A recent work [19] has shown that a lower bound can be obtained for this quantity. Namely, we have for any state ρ and $\alpha \in (1,2]$

$$H^{\varepsilon}_{\min}(X|\Theta K)_\rho \geqslant H_\alpha(X|\Theta K)_{\rho|\rho} - \frac{1}{\alpha-1}\log_2\frac{2}{\epsilon^2}. \qquad (24)$$

This combined with (23) implies the claim

$$H_{\min}^{\varepsilon}(X|\Theta K)_{\rho} \geqslant n \max_{s\in(0,1]} \frac{1}{s}[1+s-\log_2(1+2^s)]-\frac{1}{s}\log_2\frac{2}{\epsilon^2}. \tag{25}$$

It is worth noting that as $n \to \infty$, the maximum is obtained for $s \to 0$, implying that as the system size approaches infinity, the optimal bound is still given by (5), that is, in terms of a bound which comes from the Shannon entropy. However, our analysis provides a better alternative to bound the smooth min-entropy for finite system sizes and hence is more useful for practical implementations.

IV. CONCLUSIONS

We have proven entropic uncertainty relations that pave the way for a practical implementation of BB84 and six-state protocols [5–10,12–14] at a small block length. Indeed, our relation has already been employed in [16] for an experimental implementation of bit commitment in the bounded and noisy-storage models.

It is an interesting open question whether similarly strong relations can also be obtained with respect to quantum side information [11,20,21]. This would allow security statements for such protocols in terms of the quantum capacity [11] of the storage device, rather than the classical capacity [9] or the entanglement cost [22]. For the six-state case this has been done (implicitly) in [11] for the special case of a Rényi-type entropy of order $\alpha = 2$, yielding, however, a slightly weaker uncertainty relation than what might be possible for other values of $\alpha \in (1,2]$. As the amount of uncertainty is the key element in being able to tolerate experimental errors and losses in said protocols, it would be nice to extend our result to this setting.

APPENDIX

In this appendix, we provide the technical details that lead to our claims. In Appendix 1, the complete proof for the uncertainty relation for BB84 bases (measurements in eigenstates of Pauli σ_x and σ_z) is presented. In Appendix 2, similar methods are used to derive bounds for six-state bases (measurements in eigenstates of Pauli σ_x, σ_y, and σ_z).

We first restate the definitions of the relevant entropic quantities. Given any finite-dimensional Hilbert space $\mathcal{H}$, let $\mathcal{S}_{\leqslant}(\mathcal{H})$ denote the set of subnormalized density operators on $\mathcal{H}$ and $\mathcal{S}(\mathcal{H})$ denote the set of normalized density operators on $\mathcal{H}$. For $\mathcal{H}_A$ and $\mathcal{H}_B$, the conditional min-entropy of $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ given $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$ is defined as

$$H_{\min}(A|B)_{\rho|\sigma} := \sup\{\lambda \in \mathbb{R} : 2^{-\lambda} \times \mathbb{I}_A \otimes \sigma_B \geqslant \rho_{AB}\}, \tag{A1}$$

and the conditional min-entropy of A given B is defined as

$$H_{\min}(A|B)_{\rho} := \sup_{\sigma_B \in \mathcal{S}(\mathcal{H}_B)} H_{\min}(A|B)_{\rho|\sigma}. \tag{A2}$$

The smooth conditional min-entropy of A given B and $\varepsilon \geqslant 0$ is defined as

$$H_{\min}^{\varepsilon}(A|B)_{\rho} := \sup_{\rho' \in \mathcal{B}^{\varepsilon}(\rho)} H_{\min}(A|B)_{\rho'}, \tag{A3}$$

where $\mathcal{B}^{\varepsilon}(\rho_{AB}) := \{\rho'_{AB} \in \mathcal{S}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B)|P = \sqrt{1-F^2(\rho,\rho')} \leqslant \varepsilon\}$ is an ε ball in terms of the purified distance with

$$F(\rho,\rho') := \|\sqrt{\rho}\sqrt{\rho'}\|_1 + \sqrt{(1-\mathrm{tr}[\rho])(1-\mathrm{tr}[\rho'])} \tag{A4}$$

being the (generalized) fidelity [15].

The conditional α-Rényi entropies are defined as

$$H_{\alpha}(A|B)_{\rho|\rho} := \frac{1}{1-\alpha}\log \mathrm{tr}\left[\rho_{AB}^{\alpha}(\mathbb{I}_A \otimes \rho_B)^{1-\alpha}\right], \tag{A5}$$

where (possible) inverses are understood as generalized inverses. Note that there exist also slightly different definitions of conditional α-Rényi entropies in the literature.

1. Uncertainty relation for BB84 measurements

a. Step 1: Single qubit relation

For any qubit state $\rho \in \mathcal{S}(\mathbb{C}^2)$ we have to examine the quantities

$$\begin{aligned} H_{\alpha}(X|\Theta)_{\rho|\rho} &= \frac{1}{1-\alpha}\log P_{\alpha}(X|\Theta),\\ P_{\alpha}(X|\Theta) &= \mathrm{tr}\left[\rho_{X\Theta}^{\alpha}(\mathbb{I}_X \otimes \rho_{\Theta})^{1-\alpha}\right],\\ \rho_{X\Theta} &= \sum_{\theta,x} p_{\theta}\, p_{x|\theta}|x\rangle\langle x| \otimes |\theta\rangle\langle\theta|,\\ p_{x|\theta} &= \mathrm{tr}(M_{x|\theta}\rho), \end{aligned} \tag{A6}$$

with $M_{x|\theta} = \mathbf{H}^{\theta}|x\rangle\langle x|\mathbf{H}^{\theta}$ and $\mathbf{H} = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$ being the Hadamard matrix. Since the choice of measurements is uniform, we get

$$P_{\alpha}(X|\Theta) = \frac{1}{2}\sum_{\theta,x} p_{x|\theta}^{\alpha}. \tag{A7}$$

Theorem 1. Let $\rho \in \mathcal{S}(\mathbb{C}^2)$ and $\alpha = 1+s$ with $s \in (0,1]$. Then we have for BB84 measurements as in (A6) that

$$H_{\alpha}(X|\Theta)_{\rho|\rho} \geqslant \frac{1}{s}[1+s-\log(1+2^s)]. \tag{A8}$$

Proof. We evaluate the term

$$\begin{aligned} P_{1+s}(X|\Theta) &= \frac{1}{2}\sum_{\theta\in\{0,1\}}\sum_{x\in\{0,1\}} p_{x|\theta}^{1+s}\\ &= \frac{1}{2}[\mathrm{tr}(\rho|0\rangle\langle 0|)^{1+s} + \mathrm{tr}(\rho|1\rangle\langle 1|)^{1+s}\\ &\quad + \mathrm{tr}(\rho|+\rangle\langle +|)^{1+s} + \mathrm{tr}(\rho|-\rangle\langle -|)^{1+s}]\\ &= \frac{1}{2^{2+s}}\{[1+\mathrm{tr}(\sigma_z\rho)]^{1+s} + [1-\mathrm{tr}(\sigma_z\rho)]^{1+s}\\ &\quad + [1+\mathrm{tr}(\sigma_x\rho)]^{1+s} + [1-\mathrm{tr}(\sigma_x\rho)]^{1+s}\}\\ &= \frac{1}{2^{2+s}}[(1+z)^{1+s} + (1-z)^{1+s} + (1+x)^{1+s}\\ &\quad + (1-x)^{1+s}], \end{aligned} \tag{A9}$$

where $x := \mathrm{tr}(\sigma_x\rho)$ and $z := \mathrm{tr}(\sigma_z\rho)$. For any one qubit state ρ, we have the Bloch sphere condition

$$\mathrm{tr}(\sigma_x\rho)^2 + \mathrm{tr}(\sigma_y\rho)^2 + \mathrm{tr}(\sigma_z\rho)^2 \leqslant 1 \tag{A10}$$

and can therefore parametrize x and z by polar coordinates,

$$x = r\sin\phi, \quad z = r\cos\phi, \tag{A11}$$

where $r \in [0,1]$ and $\phi \in [0,\frac{\pi}{2}]$. $P_\alpha(X|\Theta)$ can then be rewritten as a function depending on the variables s, r, and ϕ:

$$Q(s,r,\phi) = \frac{1}{2^{2+s}}[(1 + r\cos\phi)^{1+s} + (1 - r\cos\phi)^{1+s} + (1 + r\sin\phi)^{1+s} + (1 - r\sin\phi)^{1+s}]. \quad \text{(A12)}$$

The partial differential of $Q(s,r,\phi)$ with respect to r becomes

$$\frac{\partial Q(s,r,\phi)}{\partial r} = \frac{1+s}{2^{2+s}}[\cos\phi(1 + r\cos\phi)^s - \cos\phi(1 - r\cos\phi)^s + \sin\phi(1 + r\sin\phi)^s - \sin\phi(1 - r\sin\phi)^s]. \quad \text{(A13)}$$

Since in the range of ϕ, $\sin\phi$ and $\cos\phi$ are positive, we obtain $\frac{\partial Q(s,r,\phi)}{\partial r} \geqslant 0$, which implies that the maximum is attained at $r = 1$. The partial differential of $Q(s,r,\phi)$ with respect to ϕ at $r = 1$ becomes

$$\begin{aligned}\frac{\partial Q(s,1,\phi)}{\partial \phi} &= \frac{1+s}{2^{2+s}}[-\sin\phi(1+\cos\phi)^s + \sin\phi(1-\cos\phi)^s + \cos\phi(1+\sin\phi)^s - \cos\phi(1-\sin\phi)^s] \\ &= \frac{1+s}{2^{2+s}}\{\sin\phi[(1-\cos\phi)^s - (1+\cos\phi)^s] + \cos\phi[(1+\sin\phi)^s - (1-\sin\phi)^s]\}. \quad \text{(A14)}\end{aligned}$$

For a stationary point of $Q(s,1,\phi)$, (A14) is zero, and the solution is obtained at three points: $\phi = 0,\frac{\pi}{4},\frac{\pi}{2}$. The characteristics of the endpoints $\phi = 0,\frac{\pi}{2}$ are the same; hence it suffices to analyze either. It remains to analyze the characteristic of these stationary points. To do so, we evaluate the second partial derivative at these points as a function of s:

$$f_1(s) = \left.\frac{\partial^2 Q(s,1,\phi)}{\partial\phi^2}\right|_{\phi=0} = \frac{1+s}{2^{1+s}}(s - 2^{s-1}), \quad s \geqslant 0, \quad \text{(A15)}$$

$$\begin{aligned}f_2(s) &= \left.\frac{\partial^2 Q(s,1,\phi)}{\partial\phi^2}\right|_{\phi=\frac{\pi}{4}} \\ &= \frac{1+s}{2^{2+s}}\left\{s\left[\left(1-\frac{1}{\sqrt{2}}\right)^{s-1} + \left(1+\frac{1}{\sqrt{2}}\right)^{s-1}\right] - \sqrt{2}\left[\left(1+\frac{1}{\sqrt{2}}\right)^{s} - \left(1-\frac{1}{\sqrt{2}}\right)^{s}\right]\right\}. \quad \text{(A16)}\end{aligned}$$

To determine if the stationary point is a local minima or maxima, we show the positivity or negativity of these functions over the interval $s \in (0,1]$. Note that $f_1(0) = -\frac{1}{4}$ and $f_1(1) = 0$, while $f_1(s)$ is always increasing since $\frac{\partial f_1(s)}{\partial s} = \frac{s}{2^{1+s}}[2 - (1+s)\ln 2] \geqslant 0$. Hence $f_1(s)$ is negative, implying the endpoints correspond to a local maxima. On the other hand, note that the second term in (A16) is exactly of the form $g(a,s)$ as stated in Lemma 2 with $a = \frac{1}{\sqrt{2}}$. With this, we conclude that the point $\phi = \frac{\pi}{4}$ is a local minimum. This leaves the endpoints as the only candidates for optimal parameters that achieve the maxima of $Q(s,1,\phi)$. Evaluating $Q(s,1,0)$ then provides us the bound

$$P_{1+s}(X|\Theta) \leqslant Q(s,1,0) = \frac{1}{2^{1+s}}(2^s + 1), \quad \text{(A17)}$$

and plugging this back into (A6) gives (A8). ■

b. Step 2: Relation for n qubits

The goal is to prove that, for any n-qubit state measured independently on each qubit in BB84 bases, the minimal output α-Rényi entropy is additive. First, let $n = 2$ with the first system denoted by A and the second by B. We have

$$\begin{aligned}P_\alpha(X_A X_B|\Theta_A\Theta_B) &= \sum_{\theta_A,\theta_B} p_{\theta_A,\theta_B} \sum_{x_A,x_B} p^\alpha_{x_A,x_B|\theta_A,\theta_B} \\ &= \frac{1}{2}\sum_{x_A,\theta_A} p^\alpha_{x_A|\theta_A} \frac{1}{2}\sum_{x_B,\theta_B} p^\alpha_{x_B|x_A,\theta_A,\theta_B}, \quad \text{(A18)}\end{aligned}$$

where $p_{\Theta_B|\Theta_A} = p_{\Theta_B}$ and $p_{\Theta_B=0} = p_{\Theta_b=1} = 1/2$. Now, assume that we have a one-qubit upper bound

$$\frac{1}{2}\sum_{x_A,\theta_A} p^\alpha_{x_A|\theta_A} \leqslant c \quad \text{(A19)}$$

for $P_\alpha(X|\Theta)$. Note that the second summation term in (A18) corresponds to $P_\alpha(X|\Theta)$ of the single-qubit density operator

$$\sigma_B = \mathrm{tr}_A\left[\frac{M_{x_A|\theta_A}\rho_{AB}M^\dagger_{x_A|\theta_A}}{\mathrm{tr}\left[M_{x_A|\theta_A}\rho_{AB}M^\dagger_{x_A|\theta_A}\right]}\right], \quad \text{(A20)}$$

where $M_{x_A|\theta_A} = \mathbf{H}^{\theta_A}|x_A\rangle\langle x_A|\mathbf{H}^{\theta_A} \otimes \mathbb{I}_B$. Hence we have

$$P_\alpha(X_A X_B|\Theta_A\Theta_B) \leqslant \frac{c}{2}\sum_{x_A,\theta_A} p^\alpha_{x_A|\theta_A} \leqslant c^2. \quad \text{(A21)}$$

The following lemma generalizes this argument to arbitrary n.

Lemma 1. For $\rho \in \mathcal{S}((\mathbb{C}^2)^{\otimes n})$ measured independently on each qubit in BB84 bases, the minimal conditional α-Rényi entropy of X^n with respect to Θ^n is additive.

Proof. Consider

$$\begin{aligned}P_\alpha(X^n|\Theta^n)_{\rho|\rho} &= \sum_{\theta^n\in\{0,1\}^n} p_{\theta^n} \sum_{x^n\in\{0,1\}^n} p^\alpha_{x^n|\theta^n} \\ &= \frac{1}{2^n}\sum_{\theta^n\in\{0,1\}^n}\sum_{x^n\in\{0,1\}^n}\left(\prod_{i=1}^n p_{i|x^{i-1},\theta^{i-1}}\right)^\alpha, \quad \text{(A22)}\end{aligned}$$

where $p_{i|x^{i-1},\theta^{i-1}} = p_{x_i|X^{i-1}=x^{i-1},\Theta^{i-1}=\theta^{i-1},K=k}$ for $i \geqslant 2$ and $p_1 = p_{x_1|\theta_1,K=k}$. Assuming the same upper bound as in (A19), we get

$$\begin{aligned}&P_\alpha(X^n|\Theta^n)_{\rho|\rho} \\ &= \frac{1}{2^{n-1}}\sum_{\theta^n\in\{0,1\}^n}\sum_{x^n\in\{0,1\}^n}\left(\prod_{i=1}^{n-1} p_{i|x^{i-1},\theta^{i-1}}\right)^\alpha \frac{1}{2}p^\alpha_{n|x^{n-1},\theta^{n-1}} \\ &\leqslant c\frac{1}{2^{n-1}}\sum_{\Theta^{n-1},X^{n-1}\in\{0,1\}^{n-1}}\left(\prod_{i=1}^{n-1} p_i\right)^\alpha \leqslant c^n. \quad \text{(A23)}\end{aligned}$$

■

Combining this with the one-qubit uncertainty relation derived before, we obtain the following.

Corollary 1. For $\alpha = 1+s$ with $s \in (0,1]$ and $\rho \in \mathcal{S}((\mathbb{C}^2)^{\otimes n})$ measured independently on each qubit in BB84 bases, we have

$$H_\alpha(X^n|\Theta^n)_{\rho|\rho} \geqslant n\frac{1}{s}\left[1+s-\log(1+2^s)\right]. \tag{A24}$$

c. Step 3: Classical side information K

In Corollary 1 we have obtained an uncertainty relation $H_\alpha(X^n|\Theta^n)_{\rho|\rho}$ for any n-qubit states ρ. But, generally, we want to consider n-qubit states ρ_k labeled with classical information K, and we need to make a relation to the quantity $H_\alpha(X^n|\Theta^n K)_{\rho|\rho}$ for the state $\rho = \sum_k p_k \rho_k$. That is, the α-Rényi entropy is also conditioned on classical information K. This quantity is evaluated as

$$\begin{aligned} &H_\alpha(X^n|\Theta^n K)_{\rho|\rho} \\ &= \frac{1}{1-\alpha}\log\sum_k \sum_{\theta^n\in\{0,1\}^n} p_{k,\theta^n} \sum_{x^n\in\{0,1\}^n} p^\alpha_{x^n|\theta^n,k} \\ &= \frac{1}{1-\alpha}\log\sum_k p_k \sum_{\theta^n\in\{0,1\}^n} p_{\theta^n|k} \sum_{x^n\in\{0,1\}^n} p^\alpha_{x^n|\theta^n,k}, \end{aligned} \tag{A25}$$

where the difference is that now $p(\Theta|K=k)$ is conditioned on the classical information $K=k$. However, in our case Θ^n is chosen randomly regardless of what state is prepared. Thus $p(\Theta^n|K=k) = p(\Theta^n) = 2^{-n}$, and we get

$$\begin{aligned} &H_\alpha(X^n|\Theta^n K)_{\rho|\rho} \\ &= \frac{1}{1-\alpha}\log\sum_k p_k \sum_{\theta^n\in\{0,1\}^n} p_{\theta^n} \sum_{x^n\in\{0,1\}^n} p^\alpha_{x^n|\theta^n,k} \\ &\geqslant n\frac{1}{s}[1+s-\log(1+2^s)]. \end{aligned} \tag{A26}$$

d. Step 4: Relation to the min-entropy

After obtaining a bound on $H_\alpha(X^n|\Theta^n K)_{\rho|\rho}$, we now link this to a bound on $H^\varepsilon_{\min}(X^n|\Theta^n K)_\rho$. It is shown in [18], Theorem 7] that for $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$, $\epsilon \geqslant 0$, and $\alpha \in (1,2]$,

$$H^\varepsilon_{\min}(A|B)_\rho \geqslant H_\alpha(A|B)_{\rho|\rho} - \frac{1}{\alpha-1}\log\frac{2}{\epsilon^2}. \tag{A27}$$

Thus the smooth conditional min-entropy is lower bounded by general conditional α-Rényi entropies, with a correction term growing logarithmically in $1/\epsilon^2$. For the Shannon entropy ($\alpha \to 1$) this term diverges, but considering $\alpha \in (1,2]$, the bound is very useful. Namely, the smooth conditional min-entropy of X^n given $\Theta^n K$ is bounded to

$$\begin{aligned} &\frac{1}{n}H^\varepsilon_{\min}(X^n|\Theta^n K)_\rho \\ &\geqslant \frac{1}{n}H_\alpha(X^n|\Theta^n K)_{\rho|\rho} \\ &\geqslant \max_{s\in(0,1]}\frac{1}{s}[1+s-\log(1+2^s)] - \frac{1}{sn}\log\frac{2}{\epsilon^2}. \end{aligned} \tag{A28}$$

Note that the maximum value of (A28) is obtained for different values of s, as n and ϵ vary.

2. Uncertainty relation for six-state measurements

In this section, we make use of the same methods as in Appendix 1. We derive an uncertainty relation for any n-qubit state measured independently on each qubit in six-state bases. For the single-qubit version, we have to consider

$$\begin{aligned} H_\alpha(X|\Theta)_{\rho|\rho} &= \frac{1}{1-\alpha}\log P_\alpha(X|\Theta), \\ P_\alpha(X|\Theta) &= \mathrm{tr}\left[\rho^\alpha_{X\Theta}(\mathbb{I}_X\otimes\rho_\Theta)^{1-\alpha}\right], \\ \rho_{X\Theta} &= \frac{1}{3}\sum_{\theta,x} p_{x|\theta}|x\rangle\langle x|\otimes|\theta\rangle\langle\theta|, \\ p_{x|\theta} &= \mathrm{tr}(N_{x|\theta}\rho), \end{aligned} \tag{A29}$$

with $N_{x|\theta} = \mathbf{T}^\theta|x\rangle\langle x|\mathbf{T}^\theta$ and $\mathbf{T} = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & -i\\ 1 & i\end{smallmatrix}\right)$ being the matrix that cyclically permutes the eigenbases of Pauli σ_x, σ_y, and σ_z.

Theorem 2. Let $\rho \in \mathcal{S}(\mathbb{C}^2)$ and $\alpha = 1+s$, with $s \in (0,1]$. Then we have for six-state measurements as in (A29) that

$$H_\alpha(X|\Theta)_{\rho|\rho} \geqslant \frac{-1}{s}\log\left[\frac{1}{3}(1+2^{1-s})\right]. \tag{A30}$$

Proof. We evaluate the term

$$\begin{aligned} P_{1+s}(X|\Theta) &= \frac{1}{3}\sum_{x\in\{0,1\}}\sum_{\theta\in\{0,1,2\}} p^{1+s}_{x|\theta} \\ &= \frac{1}{3}\frac{1}{2^{1+s}}\sum_{i=0}^{2}[(1+x_i)^{1+s}+(1-x_i)^{1+s}], \end{aligned} \tag{A31}$$

where $\{x_0,x_1,x_2\} := \{x,y,z\}$ and $x_i := \mathrm{tr}(\sigma_{x_i}\rho)$. Parametrizing this in terms of spherical coordinates, we write

$$x_0 = r\sin\phi\sin\theta,\quad x_1 = r\cos\phi\sin\theta,\quad x_2 = r\cos\theta, \tag{A32}$$

where $0 \leqslant r \leqslant 1$, $0 \leqslant \phi$, $\theta \leqslant \frac{\pi}{2}$. Expression (A31) can be rewritten in terms of these new coordinates as

$$\begin{aligned} M(s,r,\phi,\theta) := \frac{1}{3}\frac{1}{2^{1+s}}\Bigg\{&\sum_{p=0,1}[1+(-1)^p r\sin\phi\sin\theta]^{1+s} \\ &+\sum_{p=0,1}[1+(-1)^p r\cos\phi\sin\theta]^{1+s} \\ &+\sum_{p=0,1}[1+(-1)^p\cos\theta]^{1+s}\Bigg\}. \end{aligned} \tag{A33}$$

Evaluating the partial differential of $Q(s,r,\phi)$ with respect to r,

$$\begin{aligned} &\frac{\partial M(s,r,\phi,\theta)}{\partial r} \\ &= \frac{1+s}{3}\frac{1}{2^{1+s}}\sin\theta\{\sin\phi[(1+r\sin\phi\sin\theta)^s \\ &\quad-(1-r\sin\phi\sin\theta)^s]+\cos\phi[(1+r\cos\phi\sin\theta)^s \\ &\quad-(1-r\cos\phi\sin\theta)^s]\}. \end{aligned} \tag{A34}$$

Again we see that since, in the range of ϕ, θ, all values of sines and cosines are positive, we obtain $\frac{\partial M(s,r,\phi,\theta)}{\partial r} \geqslant 0$, which implies the maximum is attained at $r = 1$. Subsequently, evaluating the partial derivative,

$$\begin{aligned}\frac{\partial M(s,1,\phi,\theta)}{\partial\phi} &= \frac{1+s}{3}\frac{1}{2^{1+s}}\sin\theta\{\cos\phi[(1+\sin\phi\sin\theta)^s \\ &\quad - (1-\sin\phi\sin\theta)^s] - \sin\phi[(1+r\cos\phi\sin\theta)^s \\ &\quad - (1-r\cos\phi\sin\theta)^s]\}, \qquad \text{(A35)}\end{aligned}$$

gives the points $\phi = 0, \frac{\pi}{4}, \frac{\pi}{2}$ as solutions. We continue by evaluating the second partial derivative at these points:

$$\begin{aligned}\left.\frac{\partial^2 M(s,1,\phi,\theta)}{\partial\phi^2}\right|_{\phi=0} &= \frac{1+s}{3}\frac{1}{2^{1+s}}\sin\theta\{2s\sin\theta \\ &\quad - [(1+\sin\theta)^s - (1-\sin\theta)^s]\}, \\ \left.\frac{\partial^2 M(s,1,\phi,\theta)}{\partial\phi^2}\right|_{\phi=\frac{\pi}{4}} &= \frac{1+s}{3}\frac{1}{2^s}c^2\bigg\{s[(1+c)^{s-1}+(1-c)^{s-1}] \\ &\quad - \frac{1}{c}[(1+c)^s - (1-c)^s]\bigg\}, \qquad \text{(A36)}\end{aligned}$$

where $c = \frac{\sin\theta}{\sqrt{2}}$. By expanding in Taylor's series, the first equation is negative for $s \in (0,1]$, whereas the second equation is positive. Hence the maximum is obtained at $\phi = 0$. The last step is to evaluate

$$\begin{aligned}\frac{\partial M(s,1,0,\theta)}{\partial\theta} &= \frac{1+s}{3}\frac{1}{2^{1+s}}\sin\theta\{\cos\phi[(1+\sin\phi\sin\theta)^s \\ &\quad - (1-\sin\phi\sin\theta)^s] - \sin\phi[(1+r\cos\phi\sin\theta)^s \\ &\quad - (1-r\cos\phi\sin\theta)^s]\}. \qquad \text{(A37)}\end{aligned}$$

But then this has a form similar to (A14), and thus the maxima is obtained at $\theta = 0$. Evaluating $M(s,1,0,0)$ then results in the claim

$$P_{1+s}(X|\theta) \leqslant M(s,1,0,0) = \tfrac{1}{3}(1+2^{1-s}). \qquad \text{(A38)}$$

■

The additivity of minimal entropy holds by using the same argument as in step 2 of Appendix 1. Namely, given a string divided into parts A and B, where B denotes a single-qubit system, the uncertainty relation for B holds for the state

$$\sigma_B = \mathrm{tr}_A\left[\frac{N_{x_A|\theta_A}\rho_{AB}N^{\dagger}_{x_A|\theta_A}}{\mathrm{tr}\left[N_{x_A|\theta_A}\rho_{AB}N^{\dagger}_{x_A|\theta_A}\right]}\right], \qquad \text{(A39)}$$

where $N_{x_A|\theta_A} = \mathbf{T}^{\theta_A}|x_A\rangle\langle x_A|\mathbf{T}^{\theta_A}\otimes\mathbb{I}_B$. By exactly the same arguments as in steps 3 and 4 in Appendix 1, the smooth conditional min-entropy of the string $X^n \in \{0,1\}^n$ conditioned on the basis $\theta^n \in \{0,2\}^n$ and the classical side information K can then be bounded by

$$\begin{aligned}\frac{1}{n}H^{\varepsilon}_{\min}(X^n|\Theta^n K)_\rho &\geqslant \frac{1}{n}H_\alpha(X^n|\Theta^n K)_{\rho|\rho} \\ &\geqslant \max_{s\in(0,1]}\frac{-1}{s}\log\left[\frac{1}{3}(1+2^{1-s})\right] \\ &\quad - \frac{1}{sn}\log\frac{2}{\epsilon^2}. \qquad \text{(A40)}\end{aligned}$$

3. Technical Lemmas

Lemma 2. Given the function $g : \mathbb{R}\times\mathbb{R}\to\mathbb{R}$,

$$\begin{aligned}g(a,s) &:= s[(1+a)^{s-1} + (1-a)^{s-1}] \\ &\quad - \frac{1}{a}[(1+a)^s - (1-a)^s]. \qquad \text{(A41)}\end{aligned}$$

Then $g(a,s) \geqslant 0$ for $a \in [0,1)$ and $s \in (0,1]$.

Proof. Since a lies within the convergence radius of the function $(1\pm a)^s$, we expand the function in Taylor's series:

$$\begin{aligned}&s[(1+a)^{s-1} + (1-a)^{s-1}] - \frac{1}{a}[(1+a)^s - (1-a)^s] \\ &= 2s\left[1 + \sum_{n=2,4,\ldots}\frac{(s-1)(s-2)\cdots(s-n)}{n!}a^n\right] \\ &\quad - \frac{1}{a}\left[2as + 2\sum_{n=3,5,\ldots}\frac{s(s-1)\cdots(s-n+1)}{n!}a^n\right] \\ &= 2s\left[\sum_{n=2,4,\ldots}\frac{(s-1)(s-2)\cdots(s-n)}{n!}a^n\right. \\ &\quad \left. - \sum_{n=3,5,\ldots}\frac{(s-1)(s-2)\cdots(s-n+1)}{n!}a^{n-1}\right] \\ &= 2s\left[\sum_{n=2,4,\ldots}\frac{(s-1)(s-2)\cdots(s-n)}{n!}a^n\right. \\ &\quad \left. - \sum_{j=2,4,\ldots}\frac{(s-1)(s-2)\cdots(s-j)}{(j+1)!}a^j\right] \\ &= 2s\sum_{n=2,4,\ldots}(s-1)(s-2)\cdots(s-n)\frac{n}{(n+1)!}a^n \\ &\geqslant 0. \qquad \text{(A42)}\end{aligned}$$

The first equality holds by a straightforward expansion of Taylor's series, the second equality holds by extracting $2s$ and absorbing $\frac{1}{a}$ into the second summation term, the third equality follows from redefining the summation variable $j = n-1$, and the last inequality follows because $(s-1)\cdots(s-n) \geqslant 0$ for $s \in (0,1]$ and n being an even integer. ■

[1] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).

[2] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[3] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[5] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Proceedings of 46th IEEE Symposium on Foundations of Computer Science* (IEEE Press, Piscataway, NJ, 2005), pp. 449–458.

[6] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Proceedings of CRYPTO 2007*, Lecture Notes in Computer Science Vol. 4622 (Springer, Berlin, 2007), pp. 360–378.

[7] S. Wehner, C. Schaffner, and B. M. Terhal, Phys. Rev. Lett. **100**, 220502 (2008).

[8] C. Schaffner, B. Terhal, and S. Wehner, Quantum Inf. Comput. **9**, 11 (2008).

[9] R. König, S. Wehner, and J. Wullschleger, IEEE Trans. Inf. Theory **58**, 1962 (2012).

[10] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, *Lecture Notes in Computer Science*, Vol. 4622 (Springer, Berlin, 2007), p. 22.

[11] M. Berta, O. Fawzi, and S. Wehner, in *Advances in Cryptology: Crypto 2012*, Lecture Notes in Computer Science Vol. 7417 (Springer, Berlin, 2012), pp. 776–793.

[12] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Phys. Rev. A **81**, 052336 (2010).

[13] C. Schaffner, Phys. Rev. A **82**, 032308 (2010).

[14] C. Schaffner, Ph.D. thesis, University of Aarhus, 2007.

[15] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).

[16] H. Y. N. Ng, K. S. Joshi, C. M. Chia, C. Kurtsiefer, and S. Wehner, arXiv:1205.3331.

[17] S. Wehner and A. Winter, J. Math. Phys. **49**, 062105 (2008).

[18] G. M. Bosyk, M. Portesi, and A. Plastino, Phys. Rev. A **85**, 012108 (2012).

[19] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).

[20] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).

[21] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, Phys. Rev. Lett. **108**, 210405 (2012).

[22] M. Berta, M. Christandl, F. G. S. L. Brandao, and S. Wehner, IEEE Intl. Symp. Inform. Theory Proc. 900 (2012).