A min-entropy uncertainty relation for finite size cryptography

Nelly Ng Huei Ying,[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*

(Dated: May 16, 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 thereby relations in terms of the smooth min-entropy for BB84 and six-state encodings. Previously, strong uncertainty relations were obtained which are valid in the limit of large block lengths. Here, we prove a new 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.

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 labelled $x \in \mathcal{X}$. Let $p_{x|\rho,\theta}$ denote the probability of observing outcome x when making the measurement labelled θ on the state ρ. For each measurement, we can consider some form of entropy of the outcome distribution such as for example the Shannon entropy $\mathrm{H}(X|\Theta = \theta) = -\sum_x p_{x|\rho,\theta} \log_2 p_{x|\rho,\theta}$. 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

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

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 ($\mathrm{H}(X|\Theta = \theta) = 0$), then the outcome of at least one other measurement $\theta' \neq \theta$ is uncertain ($\mathrm{H}(X|\Theta = \theta') > 0$). Similarly, the larger the value of c, 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 *min-entropy* $\mathrm{H}_{\min}(X|\Theta = \theta) = -\log \max_x p_{x|\rho,\theta}$ 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 (labelled 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

$$\mathrm{H}_{\min}(X|\Theta K) \geq c' \ , \tag{2}$$

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 appendix)

$$\mathrm{H}_{\min}(X|\Theta K) = -\log \sum_{\theta} p_\theta \sum_k p_{k|\theta} \max_x \ p_{x|k\theta} \ . \tag{3}$$

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 BB84 bases [4], i.e., in the eigenbasis of Pauli σ_x or σ_z. It is known that in this case $c' = -n \cdot \log(1/2 + 1/(2\sqrt{2})) \approx n \cdot 0.22$ 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 model [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 primitives such as oblivious transfer, bit commitment, and even secure identification of e.g. a user to 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 $c' \approx n \cdot 0.22$ 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 $\mathrm{H}^{\varepsilon}_{\min}(X|\Theta K)$. 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 appendix)

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

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 $\delta \in (0, \frac{1}{2}]$,

$$\mathrm{H}^{\varepsilon}_{\min}(X|\Theta K) \geq n \cdot \left(\frac{1}{2} - \delta\right) \ , \qquad (5)$$

where

$$\varepsilon = \exp\left[-\frac{\delta^2 n}{512(2 + \log\frac{2}{\delta})^2}\right] \ . \qquad (6)$$

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 $c' = 0.4788$, we need $n \geq 2 \times 10^8$ to even have $\varepsilon = 0.1$! In an experiment using weak coherent pulses, with frequency of 1GHz and Poisson parameter $\mu = 1$ it takes approximately 2.5 seconds 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 post-processing of such large block lengths is time-consuming.

RESULTS

To implement 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

$$\mathrm{H}^{\varepsilon}_{\min}(X|\Theta K) \geq n \cdot c_{BB84} \ , \qquad (7)$$

where

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

At the 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 $\varepsilon = 0.1$, $c_{BB84} \geq 0.4837$ with $n = 1 \times 10^4$. Comparing this with calculations in the previous section, the required block length n is approximately 10^{-4} times smaller. Figure 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.

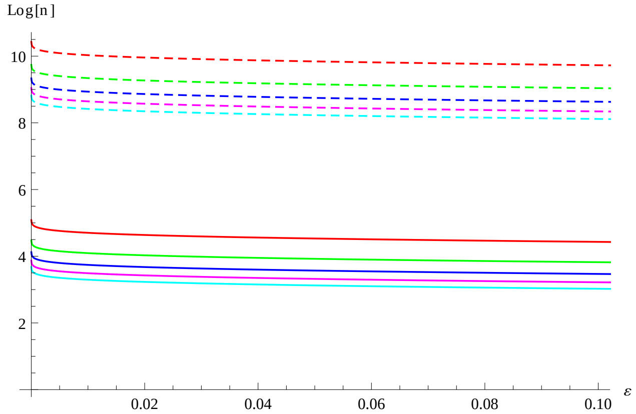

FIG. 1: This plot shows the minimal required block length n on a logarithmic scale of base 10, in order to achieve an error parameter ϵ. The dashed curves are plotted for the previous known bound (6), while the solid lines are obtained from our new analysis (8). The different colors represent the fixed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

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

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

where

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

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 $\mathrm{H}_\alpha(A|B)$. These may be of independent interest. Previously, 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

$$\min_{\rho} \mathrm{H}_\alpha(X|\Theta)_{\rho|\rho} = n \cdot \frac{\alpha - \log(1+2^{\alpha-1})}{\alpha - 1} \ , \tag{11}$$

where

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

Similarly, for measurements in the six-state bases

$$\min_{\rho} \mathrm{H}_\alpha(X|\Theta)_{\rho|\rho} = n \cdot \frac{\log 3 - \log\left(1+2^{2-\alpha}\right)}{\alpha - 1} \ . \tag{13}$$

A detailed technical proof of this result can be found in the full paper on arXiv [19].

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 small block length. Indeed, our relation has already been employed in [16] for an experimental implementation of bit commitment in the bounded/noisy-storage model.

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 again a slightly weaker uncertainty relation as might be possible for other values of $\alpha \in (1,2]$. As the amount of uncertainty is the 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.

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

[1] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010).
[2] H. Maassen and J. Uffink, Physical Review Letters **60**, 1103 (1988).
[3] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theor. **55**, 4337 (2009).
[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (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* (2005), pp. 449–458.
[6] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Proceedings of CRYPTO 2007* (2007), Springer LNCS, pp. 360–378.
[7] S. Wehner, C. Schaffner, and B. Terhal, Physical Review Letters **100**, 220502 (2008).
[8] C. Schaffner, B. Terhal, and S. Wehner, Quantum Information & Computation **9**, 11 (2008).
[9] R. König, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory - To appear (2009), arXiv:0906.1030v4.
[10] I. Damgaard, S. Fehr, L. Salvail, and C. Schaffner, Springer LNCS **4622**, 22 (2007).
[11] M. Berta, O. Fawzi, and S. Wehner (2011), arXiv:1111.2026v2.
[12] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Physical Review A **81**, 052336 (2010).
[13] C. Schaffner, Phys. Rev. A **82**, 032308 (2010).
[14] C. Schaffner, Ph.D. thesis, University of Aarhus (2007), arXiv:0709.0289v1.
[15] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Transactions on Information Theory **56** (2010).
[16] N. Ng, K. S. Joshi, C. M. Chia, C. Kurtsiefer, and S. Wehner (2012), arXiv.
[17] S. Wehner and A. Winter, Journal of Mathematical Physics **49**, 062105 (2008).
[18] G. M. Bosyk, M. Portesi, and A. Plastino, Physical Review A **85**, 012108 (2012).
[19] N. Ng, M. Berta, and S. Wehner (2012), arXiv:1205.0842v1.
[20] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010).
[21] P. J. Coles, L. Yu, and M. Zwolak (2011), arXiv:1105.4865v2.
[22] M. Berta, F. Brandao, M. Christandl, and S. Wehner (2011), arXiv:1108.5357.