Uncertainty Relation for Smooth Entropies

Marco Tomamichel[*] and Renato Renner

Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland
(Received 1 October 2010; revised manuscript received 7 January 2011; published 16 March 2011)

Uncertainty relations give upper bounds on the accuracy by which the outcomes of two incompatible measurements can be predicted. While established uncertainty relations apply to cases where the predictions are based on purely classical data (e.g., a description of the system's state before measurement), an extended relation which remains valid in the presence of quantum information has been proposed recently [Berta *et al.*, Nature Phys. **6**, 659 (2010)]. Here, we generalize this uncertainty relation to one formulated in terms of smooth entropies. Since these entropies measure operational quantities such as extractable secret key length, our uncertainty relation is of immediate practical use. To illustrate this, we show that it directly implies security of quantum key distribution protocols. Our security claim remains valid even if the implemented measurement devices deviate arbitrarily from the theoretical model.

Introduction.—Quantum mechanics has the peculiar property that, even if the state of a system is fully known, certain measurements will result in a random outcome. In other words, the information contained in the description of a system's state is generally not sufficient to predict measurement outcomes with certainty. Heisenberg's uncertainty principle [1] can be seen as a quantitative characterization of this property.

We consider a quantum system, A, and two positive operator valued measurements (POVMs) acting on it, $\mathbb{X}$ with elements $\{M_x\}$, and $\mathbb{Z}$ with elements $\{N_z\}$. In its entropic version, as first proposed by Deutsch and later proved by Maassen and Uffink [2] and Krishna *et al.* [3], the uncertainty principle reads

$$H(X|S) + H(Z|S) \geq q. \tag{1}$$

H denotes the Shannon or von Neumann entropy and characterizes the uncertainty about the measurement outcomes X of $\mathbb{X}$ or Z of $\mathbb{Z}$ given any classical description, S, of the state of A before measurement [4]. (The most general classical description of A is a full characterization of its density matrix.) The bound, q, quantifies the "incompatibility" of the two measurements and is independent of the state of A before measurement [5]

$$q := \log_2 \frac{1}{c}, \quad \text{where } c := \max_{x,z} \|\sqrt{M_x}\sqrt{N_z}\|_\infty^2. \tag{2}$$

One may now consider an agent, who, instead of holding a classical description S of A, has access to a quantum system, B, which is fully entangled with A. It is easy to verify that this agent can predict the outcome of any possible orthogonal measurement applied to A by performing a suitable measurement on his share of the entangled state. In other words, (1) is not valid in such a generalized scenario. However, as first conjectured by Renes and Boileau [4], and later proved by Berta *et al.* [6] and Coles *et al.* [7], the relation

$$H(X|B) + H(Z|C) \geq q \tag{3}$$

holds in general, for two disjoint, not necessarily classical systems B and C. If both systems contain only a classical description S of the state on A, we recover (1) [8].

To make the above statements more precise, let ρ_{ABC} be any quantum state on three systems A, B, and C. After measuring A with respect to $\mathbb{X}$ and storing the outcome in a classical register, X, the joint state of X and the system B is given by [9]

$$\rho_{XB} := \sum_x |x\rangle\langle x| \otimes \tau_B^x, \quad \text{where } \tau_B^x = \text{tr}_{AC}(M_x \rho_{ABC}).$$

[The possible measurement outcomes of $\mathbb{X}$ are encoded in an orthonormal basis $\{|x\rangle\}$ and the probability of measuring x is given by $\text{tr}(\tau_B^x)$.] Similarly, we define ρ_{ZC}, where the measurement $\mathbb{Z}$ instead of $\mathbb{X}$ is applied to A and where we keep system C instead of B. The conditional von Neumann entropies in (3) are then evaluated for these states, i.e., $H(X|B) = H(\rho_{XB}) - H(\rho_B)$.

The main contribution of this work is to generalize (3) to *smooth entropies* [10,11], which are generalizations of the von Neumann entropy. Crucially, in contrast to the latter, they characterize operational quantities beyond the standard identical and independently distributed scenario [12]. For example, the smooth min-entropy (defined in the next section) of a random variable X conditioned on a system B, denoted $H_{\min}^\varepsilon(X|B)$, corresponds to the number of bits contained in X that are ε close to uniformly distributed and independent of the quantum system B, where $\varepsilon \geq 0$ is the *smoothing parameter*. Similarly the smooth max-entropy of Z conditioned on C, denoted $H_{\max}^\varepsilon(Z|C)$, corresponds to the number of bits that are needed in order to reconstruct the value Z using the quantum system C up to a failure probability ε.

The generalized uncertainty relation reads

$$H_{\min}^\varepsilon(X|B) + H_{\max}^\varepsilon(Z|C) \geq q. \tag{4}$$

It implies most existing uncertainty relations for two incompatible measurements [13]. In particular, it generalizes and strengthens an uncertainty relation derived via operational interpretations of the smooth entropies [14]. We recover (3) by applying the entropic asymptotic equipartition property [15] to (4). Moreover, for $\varepsilon = 0$ and disregarding B and C, we find a generalization to POVMs of a result by Maassen and Uffink [2], bounding the uncertainty in terms of Rényi entropies [16] of order $1/2$ and ∞, namely, $H_\infty(X) + H_{1/2}(Z) \geq q$.

The uncertainty principle has provided intuition for various applications, in particular, in cryptography. However, previous uncertainty relations could not be applied directly, since the von Neumann entropy is often not the relevant measure of uncertainty. (See [6] for examples and a discussion.) Our uncertainty relation overcomes this limitation. Potential areas of application include entanglement witnessing, the bounded storage model [17], and quantum cryptography in general.

As an example, we show that the relation naturally leads to a concise and general security proof for quantum key distribution (QKD) [18,19]. When applied to practical prepare-and-measure protocols, it yields a strictly stronger security claim than previously known proofs. In particular, nontrivial security bounds can be obtained for realistic choices of the parameters (such as the number of exchanged signals). In addition, these bounds do not depend on the details of the measurement devices and are therefore maximally robust against imperfections in their implementation.

Smooth Entropies.—For our purposes, quantum states are positive semidefinite operators with trace smaller or equal to 1 on a finite-dimensional Hilbert space. Given a state ρ_A on (a Hilbert space) A, we say that ρ_{AB} extends ρ_A on B if $\text{tr}_B(\rho_{AB}) = \rho_A$. A purification is an extension of rank 1. We write $\rho \approx_\varepsilon \tau$ if the purified distance between ρ and τ (which is defined as the minimum trace distance between purifications of ρ and τ; see [20] for details) does not exceed ε.

We now define the smooth min- and max-entropy. Let $\varepsilon \geq 0$ and ρ_{AB} be a bipartite state on A and B. The min-entropy of A given B is defined as

$$H_{\min}(A|B)_\rho := \max_{\sigma_B} \sup\{\lambda \in \mathbb{R}: 2^{-\lambda}\mathbb{1}_A \otimes \sigma_B \geq \rho_{AB}\},$$

where σ_B is maximized over all states on B and $\mathbb{1}_A$ is the identity operator on A. Furthermore, the ε-smooth min-entropy is defined as $H_{\min}^\varepsilon(A|B)_\rho := \max_{\tilde\rho} H_{\min}(A|B)_{\tilde\rho}$, where the optimization is over all states $\tilde\rho_{AB} \approx_\varepsilon \rho_{AB}$.

The smooth max-entropy is its dual [20,21] with regards to any purification ρ_{ABC} of ρ_{AB} in the sense that

$$H_{\max}^\varepsilon(A|B)_\rho := -H_{\min}^\varepsilon(A|C)_\rho. \tag{5}$$

We are now ready to restate our uncertainty relation.

Theorem 1.—Let $\varepsilon \geq 0$, let ρ_{ABC} be a tripartite quantum state, and let $\mathbb{X}$ and $\mathbb{Z}$ be two POVMs on A. Then,

$$H_{\min}^\varepsilon(X|B)_\rho + H_{\max}^\varepsilon(Z|C)_\rho \geq q,$$

where the entropies are evaluated using ρ_{XB} and ρ_{ZC}, respectively, and ρ_{XB}, ρ_{ZC}, and q are defined as above.

Proof of the Main Result.—It will be helpful to describe the two measurements in the Stinespring dilation picture as isometries followed by a partial trace. Let U be the isometry from A to A, X and X' given by $U := \sum_x |x\rangle \otimes |x\rangle \otimes \sqrt{M_x}$. The isometry stores two copies of the measurement outcome in the registers X and X' and the postmeasurement state in A. Analogously, $V := \sum_z |z\rangle \otimes |z\rangle \otimes \sqrt{N_z}$. Furthermore, we introduce the states $\rho_{XX'ABC} := U\rho_{ABC}U^\dagger$ and $\rho_{ZZ'ABC} := V\rho_{ABC}V^\dagger$, of which the postmeasurement states appearing in Theorem 1, ρ_{XB} and ρ_{ZC}, are marginals.

We now proceed to prove the theorem for the special case where ρ_{ABC} is pure and $\varepsilon = 0$.

The duality relation (5) applied to $\rho_{ZZ'ABC}$ gives

$$H_{\max}(Z|C)_\rho + H_{\min}(Z|Z'AB)_\rho = 0. \tag{6}$$

Comparing (6) with the statement of the theorem, it remains to be shown that $H_{\min}(Z|Z'AB)_\rho \leq H_{\min}(X|B)_\rho - q$ holds. By the definition of the min-entropy, we have

$$H_{\min}(Z|Z'AB)_\rho$$
$$= \max_{\sigma_{Z'AB}} \sup\{\lambda \in \mathbb{R}: 2^{-\lambda}\mathbb{1}_Z \otimes \sigma_{Z'AB} \geq \rho_{ZZ'AB}\}$$
$$\leq \max_{\sigma_{Z'AB}} \sup\{\lambda \in \mathbb{R}: 2^{-\lambda}c\mathbb{1}_X \otimes \sigma_B \geq \rho_{XB}\}$$
$$= H_{\min}(X|B)_\rho - q, \tag{7}$$

where, in order to arrive at (7), we need to show that

$$2^{-\lambda}\mathbb{1}_Z \otimes \sigma_{Z'AB} \geq \rho_{ZZ'AB} \Rightarrow 2^{-\lambda}c\mathbb{1}_X \otimes \sigma_B \geq \rho_{XB}. \tag{8}$$

For this, we apply the partial isometry $W := UV^\dagger$ followed by a partial trace over X' and A on both sides of the inequality on the left-hand side. This implies

$$2^{-\lambda}\text{tr}_{X'A}[W(\mathbb{1}_Z \otimes \sigma_{Z'AB})W^\dagger] \geq \rho_{XB}. \tag{9}$$

Moreover, substituting the definition of W, we find

$$\text{tr}_{X'A}[W(\mathbb{1}_Z \otimes \sigma_{Z'AB})W^\dagger]$$
$$= \sum_{x,z} |x\rangle\langle x| \otimes \langle z|\text{tr}_A(\sqrt{N_z}M_x\sqrt{N_z}\sigma_{Z'AB})|z\rangle \tag{10}$$

$$\leq c\mathbb{1}_X \otimes \sigma_B. \tag{11}$$

To get (10), we used the orthonormality of $\{|x\rangle\}_x$ and $\{|z\rangle\}_z$ as well as the cyclicity of the partial trace over A. Moreover, in the last step, we used that

$$\sqrt{N_z}M_x\sqrt{N_z} = |\sqrt{N_z}\sqrt{M_x}|^2 \leq c\mathbb{1}_A.$$

Finally, combining (11) with (9) establishes (8), concluding the proof for $\varepsilon = 0$ and pure states.

Next, we generalize this proof to ε-smooth entropies. The purified distance used in the definition of the smooth entropies has some interesting properties [20] that we use

in the following: (i) Let $\mathcal{E}$ be any trace nonincreasing completely positive map (e.g., a partial isometry or a partial trace). Then, $\rho \approx_\varepsilon \tau$ implies $\mathcal{E}(\rho) \approx_\varepsilon \mathcal{E}(\tau)$. (ii) Let ρ_{AB} be a fixed extension of ρ_A. Then, $\rho_A \approx_\varepsilon \tau_A$ implies that there exists an extension τ_{AB} of τ_A that is ε close to ρ_{AB}. Furthermore, if ρ_{AB} is pure and $|\text{supp}\{\tau_A\}| \leq \dim B$, then τ_{AB} can be chosen pure.

Let $\tilde{\rho}_{ZC} \approx_\varepsilon \rho_{ZC}$ be a state that minimizes the smooth max-entropy, i.e., $H_{\max}^\varepsilon(Z|C)_\rho = H_{\max}(Z|C)_{\tilde{\rho}}$. Using the properties of the purified distance discussed above, we introduce a purification $\tilde{\rho}_{ZZ'ABC}$, a state $\tilde{\rho}_{XX'ABC} := W\tilde{\rho}_{ZZ'ABC}W^\dagger$ and its marginal $\tilde{\rho}_{XB}$, which are ε close to the corresponding states ρ. Applying the duality relation (6) as well as the argument in (7) to $\tilde{\rho}$ results in $H_{\max}(Z|C)_{\tilde{\rho}} + H_{\min}(X|B)_{\tilde{\rho}} \geq q$, from which the claim follows due to the maximization over close states used in the definition of the smooth min-entropy.

Finally, to generalize the result to mixed states, we write down the uncertainty relation for a purification ρ_{ABCD} of ρ_{ABC}, i.e., $H_{\min}^\varepsilon(X|B) + H_{\max}^\varepsilon(Z|CD) \geq q$. The claim is now a direct consequence of the data-processing inequality [20] establishing $H_{\max}^\varepsilon(Z|CD) \leq H_{\max}^\varepsilon(Z|C)$.

Application to Quantum Key Distribution.—In the following, we consider practically relevant *prepare-and-measure* schemes such as the Bennett-Brassard 1984 protocol (BB84) [18]. In these schemes, one party, called Alice, prepares a sequence of nonorthogonal quantum states and sends them over a public quantum channel to a second party, Bob, who measures these states. The correlated data gathered during this first phase of the protocol form the *raw keys*, from which Alice and Bob can then extract a final secret key by a classical postprocessing procedure (requiring only local operations and communication over an authenticated channel).

Amid recent hacking attacks on commercial QKD systems [22,23], it is important to point out that information-theoretic security proofs for quantum cryptography rely on several assumptions in addition to the validity of quantum mechanics. (1) The two parties, Alice and Bob, have access to genuine randomness. (2) The information that leaves each lab is restricted to what the protocol allows. (3) The measurement devices work according to the specifications of the protocol. These assumptions are often not satisfied by realistic implementations.

Our novel security proof allows us to drop Assumption 3, which concerns Bob's measurement device, completely. Moreover, Assumption 2 can be weakened to allow for certain imperfections of Alice's state preparation. The proof is based on the intuition, first formalized by Mayers [24] and captured by the uncertainty relation, that security of QKD can be derived from the fact that Alice has a choice between two incompatible bases for state preparation. The fact that Bob can accurately estimate the states Alice prepared in both bases directly implies that an eavesdropper cannot. Furthermore, this implication

holds independently of how Bob obtains his data, i.e., no assumption about Bob's measurement device is required.

The proof relies on two main ingredients: (i) the uncertainty relation (Theorem 1) and (ii) the following result that bounds the number of secret key bits that can be extracted from raw keys by classical postprocessing. Assume that Alice and Bob hold correlated data, X and X', about which an adversary may have information E. Then, Alice and Bob can employ a classical *postprocessing procedure* (usually consisting of an error correction scheme concatenated with a procedure called privacy amplification [25,26]), which generates a shared secret key of length [27]

$$\ell \approx H_{\min}^\varepsilon(X|E) - H_{\max}^\varepsilon(X|X'). \tag{12}$$

(This can be seen as a single-shot version of the Devetak-Winter bound [28].) In other words, the length of the key that can be generated is essentially determined by the difference between the uncertainty that the adversary has about Alice's raw key X, measured in terms of the smooth min-entropy, and the uncertainty that Bob has about X, measured in terms of the smooth max-entropy.

While the following arguments are rather general, we may for concreteness consider the BB84 protocol. For the purpose of the proof we use its *entanglement-based* version, which implies security of the original prepare-and-measure scheme [29]. Here, it is assumed that Alice and Bob start with an untrusted joint quantum state, ρ_{AB}, from which they extract a secret key. This state is supposed to be a sequence of maximally entangled qubits but may, in the presence of an adversary or noise, be arbitrarily corrupted. The protocol then proceeds as follows. First, Alice and Bob both measure each of these qubits with respect to a basis chosen at random from two possibilities, $\mathbb{X}$ and $\mathbb{Z}$, resulting in bit strings X (for Alice) and X' (for Bob). Next, they perform statistical tests on a few sample bits taken from X and X' in order to estimate the correlation. If this correlation is sufficiently large, they apply the above-mentioned postprocessing procedure to turn their raw keys into a fully secret key of an appropriate length, ℓ. Otherwise, if the estimated correlation is too small, they abort the protocol.

To prove that this protocol produces a secret key, it suffices to verify that the entropy difference in (12) is positive under the condition that the raw keys passed the correlation test. The second term of (12), $H_{\max}^\varepsilon(X|X')$, directly depends on the correlation strength between the raw keys. For example, if X and X' consist of n bits, of which at most a fraction δ disagree (according to the statistical test performed during the protocol), we have

$$H_{\max}^\varepsilon(X|X') \lesssim nh(\delta), \tag{13}$$

where $h(\cdot)$ denotes the binary entropy and n is the number of bits in the raw key.

The first term in (12), $H_{\min}^\varepsilon(X|E)$, depends on the correlations between X and the adversary's information E, which is not accessible to Alice and Bob. The challenge is to bound these correlations from the data that is available,

namely, the correlations between X and X'. This is exactly where our uncertainty relation steps in.

Recall that, according to the protocol description, Alice and Bob measure each of their qubits with respect to one out of two different bases. One may now think of a hypothetical run of the protocol where Alice and Bob use the opposite basis choice for the measurement of each of their qubits, resulting in outcomes Y and Y', respectively. We may then apply our uncertainty relation, which gives

$$H^{\varepsilon}_{\min}(X|E) \geq qn - H^{\varepsilon}_{\max}(Y|Y') = qn - H^{\varepsilon}_{\max}(X|X'),$$

where q is evaluated for Alice's apparatus [30]. The last equality follows because the choice of basis was random for each qubit, and hence the correlation between Y and Y' is identical to the one between X and X'. Inserting this into (12) and using (13), we conclude that the protocol generates a secure key of length

$$\ell \approx n[q - 2h(\delta)]. \tag{14}$$

We emphasize that, in contrast to security proofs based on previous versions of the uncertainty relation, e.g., [6,31], this security proof does not rely on additional arguments such as the postselection technique [32], the de Finetti theorem [33], and the quantum asymptotic equipartition property [11,15]. Employing these tools introduces additional terms in (14) that reduce the extractable key length significantly for experimentally feasible values of n. Our proof technique will, therefore, lead to tighter finite-key bounds [34,35].

Finally, we note that our approach is different from recent device-independent security proofs for entanglement-based protocols [19], which are based on a violation of Bell's theorem [36,37]. In these proofs Assumption 3 applies to both parties and cannot be dropped—instead, it may be replaced by the assumption that the measurement devices are memoryless.

We thank M. Berta, M. Christandl, R. Colbeck, and J. Renes for many stimulating discussions and acknowledge support from the Swiss National Science Foundation (Grant No. 200021-119868).

---

*marcoto@phys.ethz.ch

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).
[2] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[3] M. Krishna and K. R. Parthasarathy, The Indian Journal of Statistics **64**, 842 (2002).
[4] J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
[5] The norm $\| \cdot \|_{\infty}$ evaluates the largest singular value. If the measurements are projective and rank 1, namely, if $M_x = |x\rangle\langle x|$ and $N_z = |z\rangle\langle z|$, then (2) reduces to the maximum overlap, $c = \max_{x,z} |\langle x|z\rangle|^2$.
[6] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Phys. **6**, 659 (2010).
[7] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, arXiv:1006.4859.
[8] Note that classical (unlike quantum) information can be copied and, therefore, stored in two disjoint subsystems, B and C.
[9] We omit identity operators whenever their presence is implied by context, e.g., $M_x \rho_{ABC}$ should be understood as $(M_x \otimes \mathbb{1}_{BC})\rho_{ABC}$.
[10] R. Renner and S. Wolf, in *Advances in Cryptography—ASIACRYPT, LNCS* (Springer, New York, 2005), Vol. 3788, pp. 199–216.
[11] R. Renner, Ph.D. thesis, ETH Zurich, 2005 arXiv:quant-ph/0512258.
[12] Most results involving the von Neumann entropy are only valid for processes that produce a sequence of identical and independently distributed random values (see [11] for a discussion).
[13] S. Wehner and A. Winter, arXiv:0907.3704.
[14] J. M. Renes, arXiv:1003.0703.
[15] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).
[16] A. Rényi, in *Proc. Symp. on Math., Stat. and Probability* (University of California Press, Berkeley, 1961), pp. 547–561.
[17] I. B. Damgaard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Advances in Cryptography—CRYPTO, LNCS* (Springer, New York, 2007), Vol. 4622, pp. 360–378.
[18] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.* (IEEE, Bangalore, 1984), pp. 175–179.
[19] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[20] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).
[21] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[22] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).
[23] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[24] D. Mayers, in *Advances in Cryptography—CRYPTO, LNCS* (Springer, New York, 1996), Vol. 1109, pp. 343–357.
[25] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[26] R. Renner and R. König, in *Proc. TCC, LNCS* (Springer, Cambridge, USA, 2005), Vol. 3378, pp. 407–425.
[27] J. M. Renes and R. Renner, arXiv:1008.0452.
[28] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[29] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[30] The parameter $q = -\log_2 c$ is determined by the maximum overlap between the two bases used by Alice, e.g., we have $q = 1$ for the BB84 protocol. If the bases are not complementary to each other, then q is reduced accordingly.
[31] M. Koashi, J. Phys. Conf. Ser. **36**, 98 (2006).
[32] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[33] R. Renner, Nature Phys. **3**, 645 (2007).
[34] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[35] L. Sheridan, T. P. Le, and V. Scarani, New J. Phys. **12**, 123019 (2010).
[36] E. Hänggi, Ph.D. thesis, ETH Zurich, 2010.
[37] L. Masanes, S. Pironio, and A. Aćin, arXiv:1009.1567.