The Uncertainty Relation for Smooth Entropies

Marco Tomamichel[1] and Renato Renner[1]

[1] *Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*

(Dated: September 13, 2010)

Uncertainty relations give upper bounds on the accuracy by which the outcomes of two incompatible measurements can be predicted. While the 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 the measurement), an extended relation which remains valid in the presence of quantum information has been proposed recently [Berta et al., Nature Physics **6**, 659 (2010)]. Here we generalize this uncertainty relation to one formulated in terms of smooth entropies. Since these entropy measures are related to operational quantities, our uncertainty relation has various applications. As an example, we show that it directly implies security of quantum key distribution protocols.

I. 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 can be seen as a quantitative characterization of this property.

Uncertainty relations expressed in terms of entropies have recently attracted renewed attention [1]. We consider two possible positive operator valued measurements (POVMs), $\mathbb{X}$ and $\mathbb{Z}$, that can be applied to a quantum system A. In its entropic version, as first proposed by Deutsch and later proved by Maasen and Uffink [2] and Krishna *et al.* [3], the uncertainty principle reads[1]

$$H(\mathrm{X}|\mathrm{S}) + H(\mathrm{Z}|\mathrm{S}) \geq \log \frac{1}{c}\,, \tag{1}$$

where H denotes the Shannon entropy and characterizes the uncertainty about the measurement outcomes X and Z given any classical description S of the original state of A. The bound depends on the *overlap*, denoted c, which quantifies the "incompatibility" of the two measurements.[2]

One may now consider an agent B who, instead of holding a classical description of A, has access to a quantum system which is fully entangled with A. It is easy to verify that B 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.* [5] and Coles *et al.* [6], the relation

$$H(\mathrm{X}|\mathrm{B}) + H(\mathrm{Z}|\mathrm{C}) \geq \log \frac{1}{c} \tag{2}$$

holds in general, for two disjoint, not necessarily classical, B and C. If both systems contain only a classical description S of the state, we recover (1).[3]

The main contribution of this work is to generalize (2) to *smooth entropies* [7, 8], which are generalizations of the Shannon / von Neumann entropy. In contrast to the latter, they characterize operational quantities beyond the standard i.i.d. scenario.[4] In particular, the smooth min-entropy of a random variable X conditioned on a system B, denoted $H^{\varepsilon}_{\min}(\mathrm{X}|\mathrm{B})$, corresponds to the number of bits contained in X that are uniformly distributed and independent of B. Similarly the smooth max-entropy of Z conditioned on C, $H^{\varepsilon}_{\max}(\mathrm{Z}|\mathrm{C})$, corresponds to the number of bits that are needed in order to reconstruct the value Z using C.

The generalized uncertainty relation reads[5]

$$H^{\varepsilon}_{\min}(\mathrm{X}|\mathrm{B}) + H^{\varepsilon}_{\max}(\mathrm{Z}|\mathrm{C}) \geq \log \frac{1}{c}\,. \tag{3}$$

The above result strengthens and generalizes an uncertainty relation that was derived via operational interpretations of the smooth entropies [9]. Also note that we can recover (2) by applying the entropic asymptotic equipartition property [10] to (3). 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 [11] of order $1/2$ and ∞, i.e. $H_{\infty}(\mathrm{X}) + H_{1/2}(\mathrm{Z}) \geq \log \frac{1}{c}$.

[1] Hereafter, log denotes the binary logarithm.

[2] For example, if A is a two-level system, and if $\mathbb{X}$ and $\mathbb{Z}$ are measurements with respect to a standard and the corresponding diagonal basis, respectively, one has $c = \frac{1}{2}$.

[3] Note, however, that this assignment is only possible because classical information can be "copied" and therefore be assigned to two disjoint subsystems, B and C.

[4] Most results involving the Shannon or the von Neumann entropy are only valid for processes that produce a sequence of identical and independently distributed (i.i.d.) random values.

[5] Precise definitions of all quantities involved will follow in Section II.

Uncertainty relations have various applications, e.g., in the context of entanglement witnessing or in cryptography [5]. The generalized version provided here further extends the range of applications, particularly because of its formulation in terms of smooth entropies. To illustrate this, we show that security of quantum key distribution (QKD) is an almost immediate consequence of the relation.

The remainder of the paper is organized as follows: Section II introduces the notation and definitions necessary to state our uncertainty relation as a theorem. The proof follows in Section III. Finally, an application of our result to QKD is discussed in Section IV.

II. NOTATION AND DEFINITIONS

For our purposes, quantum states are positive semi-definite operators with trace smaller or equal to 1 on a finite-dimensional Hilbert space. We use subscripts to denote different Hilbert spaces. For a state ρ_{A} on (a Hilbert space) A we say that ρ_{AB} is an extension of ρ_{A} on B if $\mathrm{tr}_{\mathrm{B}}(\rho_{\mathrm{AB}}) = \rho_{\mathrm{A}}$. In turn, given a state ρ_{AB}, its marginals ρ_{A} and ρ_{B} are uniquely and implicitly defined via the partial trace. A purification is an extension with rank 1. For a pure state ϕ, we denote its vector representation as $|\phi\rangle$ and $|\phi\rangle^\dagger = \langle\phi|$, i.e. we may write $\phi = |\phi\rangle\langle\phi|$.

We use the purified distance (see [12] for a definition and properties) as a distance measure on the quantum state space. We write $\rho \approx_\varepsilon \tau$ (ρ is ε-close to τ) if the purified distance between ρ and τ does not exceed ε.

We now define the smooth min- and max-entropy.

Definition 1. 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

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

where σ_{B} is maximized over all states on B and $\mathbb{1}_{\mathrm{A}}$ is the identity operator on A. Furthermore, the smooth min-entropy of A given B is defined as

$$H^\varepsilon_{\min}(\mathrm{A}|\mathrm{B})_\rho := \max_{\tilde\rho_{\mathrm{AB}}} H_{\min}(\mathrm{A}|\mathrm{B})_{\tilde\rho},$$

where the optimization is over all states $\tilde\rho_{\mathrm{AB}} \approx_\varepsilon \rho_{\mathrm{AB}}$.

Definition 2. Let $\varepsilon \geq 0$ and ρ_{AB} be a bipartite state on A and B. The max-entropy of A given B is defined as

$$H_{\max}(\mathrm{A}|\mathrm{B})_\rho := \max_{\sigma_{\mathrm{B}}} \log F^2\big(\rho_{\mathrm{AB}}, \mathbb{1}_{\mathrm{A}} \otimes \sigma_{\mathrm{B}}\big),$$

where σ_{B} is maximized over all states on B and $F(\rho,\tau) := \mathrm{tr}|\sqrt{\rho}\sqrt{\tau}|$ is the fidelity. Furthermore, the smooth max-entropy of A given B is defined as

$$H^\varepsilon_{\max}(\mathrm{A}|\mathrm{B})_\rho := \min_{\tilde\rho_{\mathrm{AB}}} H_{\max}(\mathrm{A}|\mathrm{B})_{\tilde\rho},$$

where the optimization is over all states $\tilde\rho_{\mathrm{AB}} \approx_\varepsilon \rho_{\mathrm{AB}}$.

The smooth min- and max-entropies are dual [12, 13] with regards to any purification ρ_{ABC} of ρ_{AB} in the sense that, for any $\varepsilon \geq 0$,

$$H^\varepsilon_{\min}(\mathrm{A}|\mathrm{B})_\rho = -H^\varepsilon_{\max}(\mathrm{A}|\mathrm{C})_\rho\,. \tag{4}$$

In the following, let ρ_{ABC} be a quantum state on three subsystems A, B and C and let $\mathbb{X}$ and $\mathbb{Z}$ be two POVMs acting on A with elements $\{M_x\}_{x\in\mathcal{X}}$ amd $\{N_z\}_{z\in\mathcal{Z}}$, respectively.[6] Measuring the system A using $\mathbb{X}$ and disregarding the post-measurement state on A and C will result in a state[7]

$$\rho_{\mathrm{XB}} := \sum_x |x\rangle\langle x| \otimes \tau_{\mathrm{B}}^{[x]}, \quad \text{where}$$
$$\tau_{\mathrm{B}}^{[x]} = \mathrm{tr}_{\mathrm{AC}}\big(M_x \rho_{\mathrm{ABC}} M_x\big)\,.$$

The probability of measuring x is given by $\mathrm{tr}(\tau_{\mathrm{B}}^{[x]})$ and $\{|x\rangle\}_x$ is an orthonormal basis on X enumerating the possible measurement outcomes of $\mathbb{X}$. Similarly, we introduce ρ_{ZC} and $\{|z\rangle\}_z$, which result from measuring $\mathbb{Z}$ and disregarding the post-measurement state on A and B.

The overlap of the two measurements is defined as[8]

$$c := \max_{x,z} \left\|\sqrt{M_x}\sqrt{N_z}\right\|^2_\infty. \tag{5}$$

We are now ready to restate our uncertainty relation.

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

$$H^\varepsilon_{\min}(\mathrm{X}|\mathrm{B})_\rho + H^\varepsilon_{\max}(\mathrm{Z}|\mathrm{C})_\rho \geq \log\frac{1}{c}\,,$$

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

III. 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 post-measurement state in A. Analogously, $V := \sum_z |z\rangle \otimes |z\rangle \otimes \sqrt{N_z}$. Furthermore, we introduce the states $\rho_{\mathrm{XX'ABC}} := U\rho_{\mathrm{ABC}}U^\dagger$

[6] We will not mention the sets $\mathcal{X}$ and $\mathcal{Z}$ explicitly in the following. However, variables x and $\bar x$ are always to be taken from $\mathcal{X}$ and variables z and $\bar z$ are to be taken from $\mathcal{Z}$.

[7] We will henceforth omit identity operators whenever their presence is implied by context, e.g. $M_x\rho_{\mathrm{ABC}}M_x$ should be understood as $(M_x \otimes \mathbb{1}_{\mathrm{BC}})\rho_{\mathrm{ABC}}(M_x \otimes \mathbb{1}_{\mathrm{BC}})$.

[8] The norm $\|\cdot\|_\infty$ evaluates the maximum singular value of an operator. If the measurements are projective and rank 1 — i.e. if $M_x = |x\rangle\langle x|$ and $N_z = |z\rangle\langle z|$ — then (5) reduces to $c = \max_{x,z} |\langle x|z\rangle|^2$.

and $\rho_{\mathrm{ZZ'ABC}} := V\rho_{\mathrm{ABC}}V^\dagger$, of which the post-measurement states of Section II, ρ_{XB} and ρ_{ZC}, are marginals.

We now proceed to prove Theorem 1 for the special case where ρ_{ABC} is pure and $\varepsilon = 0$ and then extend the result to mixed states and $\varepsilon > 0$.

Proof of Theorem 1 (for ρ_{ABC} pure and $\varepsilon = 0$). The duality relation (4) applied to $\rho_{\mathrm{ZZ'ABC}}$ gives

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

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

$$\begin{aligned} &H_{\min}(\mathrm{Z}|\mathrm{Z'AB})_\rho \\ &\quad= \max_{\sigma_{\mathrm{Z'AB}}} \sup\{\lambda \in \mathbb{R} : 2^{-\lambda}\,\mathbb{1}_{\mathrm{Z}} \otimes \sigma_{\mathrm{Z'AB}} \geq \rho_{\mathrm{ZZ'AB}}\} \\ &\quad\leq \max_{\sigma_{\mathrm{Z'AB}}} \sup\{\lambda \in \mathbb{R} : 2^{-\lambda}\,c\,\mathbb{1}_{\mathrm{X}} \otimes \sigma_{\mathrm{B}} \geq \rho_{\mathrm{XB}}\} \qquad (7) \\ &\quad= H_{\min}(\mathrm{X}|\mathrm{B})_\rho + \log c\,, \end{aligned}$$

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

$$2^{-\lambda}\,\mathbb{1}_{\mathrm{Z}} \otimes \sigma_{\mathrm{Z'AB}} \geq \rho_{\mathrm{ZZ'AB}} \implies 2^{-\lambda}\,c\,\mathbb{1}_{\mathrm{X}} \otimes \sigma_{\mathrm{B}} \geq \rho_{\mathrm{XB}}\,. \tag{8}$$

To show (8), we apply the partial isometry[9] $W := UV^\dagger$ followed by a partial trace over X' and A on both sides of the inequality on the left-hand side. This implies

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

Moreover, substituting the definition of W, we find

$$\begin{aligned} &\mathrm{tr}_{\mathrm{X'A}}\big(W(\mathbb{1}_{\mathrm{Z}} \otimes \sigma_{\mathrm{Z'AB}})W^\dagger\big) \\ &\quad= \sum_{x,z} |x\rangle\langle x| \otimes \langle z|\mathrm{tr}_{\mathrm{A}}\big(\sqrt{N_z}M_x\sqrt{N_z}\sigma_{\mathrm{Z'AB}}\big)|z\rangle \qquad (10) \\ &\quad\leq c\,\mathbb{1}_{\mathrm{X}} \otimes \sigma_{\mathrm{B}}\,. \qquad (11) \end{aligned}$$

To find (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

$$\begin{aligned} \sqrt{N_z}M_x\sqrt{N_z} &= \big|\sqrt{N_z}\sqrt{M_x}\big|^2 \\ &\leq \big\|\sqrt{N_z}\sqrt{M_x}\big\|_\infty^2\,\mathbb{1}_{\mathrm{A}} \leq c\,\mathbb{1}_{\mathrm{A}}, \end{aligned}$$

Finally, combining (11) with (9) establishes (8), concluding the proof. □

We now generalize this result to ε-smooth entropies. The purified distance has some interesting properties [12] that we use in the following.

1. Let $\mathcal{E}$ be any trace non-increasing completely positive map (e.g. a partial isometry, a measurement or a partial trace). Then $\rho \approx_\varepsilon \tau$ implies $\mathcal{E}(\rho) \approx_\varepsilon \mathcal{E}(\tau)$.

2. Let ρ_{AB} be a fixed extension of ρ_{A}. Then $\rho_{\mathrm{A}} \approx_\varepsilon \tau_{\mathrm{A}}$ 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 $|\mathrm{supp}\,\{\tau_{\mathrm{A}}\}| \leq |\mathrm{B}|$, then τ_{AB} can be chosen pure.[10]

Let $\tilde\rho_{\mathrm{ZC}} \approx_\varepsilon \rho_{\mathrm{ZC}}$ be a state that minimizes the smooth max-entropy, i.e. $H^\varepsilon_{\max}(\mathrm{Z}|\mathrm{C})_\rho = H_{\max}(\mathrm{Z}|\mathrm{C})_{\tilde\rho}$. Using the properties of the purified distance outlined above[11], we introduce a purification $\tilde\rho_{\mathrm{ZZ'ABC}}$, a state $\tilde\rho_{\mathrm{XX'ABC}} := W\tilde\rho_{\mathrm{ZZ'ABC}}W^\dagger$ and its marginal $\tilde\rho_{\mathrm{XB}}$, which are ε-close to the corresponding unsmoothed states $\rho_{\mathrm{ZZ'ABC}}$, $\rho_{\mathrm{XX'ABC}}$ and ρ_{XB}. Applying the duality relation (6) as well as the argument in (7) to the smoothed states results in

$$H_{\max}(\mathrm{Z}|\mathrm{C})_{\tilde\rho} + H_{\min}(\mathrm{X}|\mathrm{B})_{\tilde\rho} \geq \log\frac{1}{c}\,,$$

from which the smoothed uncertainty relation follows by the definition of $\tilde\rho_{\mathrm{ZC}}$ and the maximization in the definition of the smooth min-entropy.

Finally, we generalize the result to mixed states ρ_{ABC}. After we write down the uncertainty relation for a purification ρ_{ABCD} of ρ_{ABC}, i.e. $H^\varepsilon_{\min}(\mathrm{X}|\mathrm{B}) + H^\varepsilon_{\max}(\mathrm{Z}|\mathrm{CD}) \geq \log\frac{1}{c}$, the uncertainty relation for mixed states is a direct consequence of the data-processing inequality [12] which tells us that $H^\varepsilon_{\max}(\mathrm{Z}|\mathrm{CD}) \leq H^\varepsilon_{\max}(\mathrm{Z}|\mathrm{C})$.

IV. APPLICATION TO QUANTUM KEY DISTRIBUTION

As an example application of our uncertainty relation, Theorem 1, we show how it can be used to prove security of Quantum Key Distribution (QKD). For this, we consider an *entanglement-based* QKD protocol [14], where it is assumed that two distant parties, Alice and Bob, start with an untrusted joint quantum state, ρ_{AB}, from which they extract a secret key using only local operations and public classical communication.[12] We note that the security of the technologically less demanding *prepare-and-measure schemes*, such as BB84 [15], can be inferred directly from the security of a corresponding entanglement-based scheme [16].

Our security proof will rely on two main ingredients: (i) the uncertainty relation and (ii) a result that bounds

[9] A partial isometry is an operator W satisfying $W^\dagger W = P_{\mathrm{supp}}$ and $WW^\dagger = P_{\mathrm{im}}$, where P_{supp} and P_{im} are the projectors onto the support and image of W, respectively.

[10] Here, $|\cdot|$ denotes the dimensionality of a Hilbert space.

[11] We also use that $|\mathrm{supp}\,\{\tilde\rho_{\mathrm{ZC}}\}| \leq |\mathrm{supp}\,\{\rho_{\mathrm{Z}}\}| \cdot |\mathrm{supp}\,\{\rho_{\mathrm{C}}\}| \leq |\mathrm{Z'}| \cdot |\mathrm{AB}|$, where the first inequality follows from properties of the smooth max-entropy [12].

[12] Typically, the state ρ_{AB} is generated locally by one of the parties, who then sends one part of it to the other using an (insecure) quantum channel.

the amount of key that can be extracted, by classical operations, from an only partially secure and partially erroneous *raw key*. More precisely, let X and X' be correlated bit strings held by Alice and Bob, about which an adversary may have information E. Then Alice and Bob can employ a classical *post-processing procedure* (usually consisting of an error correction scheme concatenated with a procedure called privacy amplification [17, 18]), which generates a shared secret key of length at most [19]

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

(This can be seen as a single-shot version of the Devetak-Winter bound [20].) 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 considerations are rather general, we may for concreteness consider the entanglement-based version of the BB84 protocol [16]. Here, Alice and Bob start with mutually correlated qubits. These are supposed to be maximally entangled but may, in the presence of an adversary (or noise), be arbitrarily corrupted. This means that nothing can be assumed about the initial state ρ_{AB}. 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, Alice and Bob 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 post-processing procedure to turn their raw keys, X and X', into a fully secret key of an appropriate length, ℓ. Otherwise (if the estimated correlation is too small) they abort the protocol.

To prove security of this protocol, we use the post-processing result, according to which it suffices to verify that the entropy difference in (12) is positive. It thus remains to establish bounds on the entropies, under the condition that the raw keys passed the correlation test. The smooth max-entropy, $H_{\max}^{\varepsilon}(\mathrm{X}|\mathrm{X}')$, directly depends on the correlation strength between X and X'. 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 (see, e.g., [19])

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

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

The situation is however more involved for $H_{\min}^{\varepsilon}(\mathrm{X}|\mathrm{E})$. This quantity depends on the correlations between X and the adversary's information E, which is obviously not accessible to Alice and Bob so that no direct statistical tests can be applied. The challenge is, therefore, to bound these correlations from the data that is available, i.e., 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/or 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

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

where $q = \log \frac{1}{c}$ is determined by the overlap of the two measurements. (For BB84, we typically have $q = 1$.) The last equality follows because the choice of the basis was random for each qubit, and hence the correlation between Y and Y' is identical to the the one between X and X'. Inserting this into (12) and using (13), we conclude that the protocol generates a secure key of length

$$\ell \approx n\big(q - 2h(\delta)\big) \,.$$

We emphasize that this result is valid without resorting to the assumption of collective attacks. In particular, in contrast to security proofs based on a previous version of the uncertainty relation (2), this security proof does not rely on additional arguments such as the post-selection technique [21] or the de Finetti theorem [22]. It is therefore expected that it will lead to tighter finite-key bounds [23].

We also remark that the above argument does not rely in any way on the procedure that Bob used to generate his part of the raw key, X'. Our proof is therefore independent of the internal workings of the measurement device that Bob uses. We thus conclude that the achieved security is device-independent [24] with respect to Bob.

Acknowledgments

We thank Mario Berta, Matthias Christandl, Roger Colbeck and Joe Renes for many stimulating discussions and acknowledge support from the Swiss National Science Foundation (grant No. 200021-119868).

[1] S. Wehner and A. Winter (2009), `arXiv:0907.3704`.
[2] H. Maassen and J. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[3] M. Krishna and K. R. Parthasarathy (2001),

arXiv:quant-ph/0110025.
[4] J. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
[5] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010).
[6] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths (2010), arXiv:1006.4859.
[7] R. Renner and S. Wolf, in *Advances in Cryptology — ASIACRYPT* (2005), vol. 3788 of *LNCS (Springer)*, pp. 199–216.
[8] R. Renner, Phd thesis, ETH Zurich (2005), arXiv:quant-ph/0512258.
[9] J. M. Renes (2010), arXiv:1003.0703.
[10] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. on Inf. Theory **55**, 5840 (2009).
[11] A. Rényi, in *Proc. Symp. on Math., Stat. and Probability* (Berkeley, 1961), pp. 547–561.
[12] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. on Inf. Theory **56**, 4674 (2010).
[13] R. König, R. Renner, and C. Schaffner, IEEE Trans. on Inf. Theory **55**, 4337 (2009).
[14] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[15] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.* (Bangalore, 1984), pp. 175–179.
[16] C. Bennett, G. Brassard, and N. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[17] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. on Inf. Theory **41**, 1915 (1995).
[18] R. Renner and R. König, in *Proc. TCC* (Cambridge, USA, 2005), vol. 3378 of *LNCS (Springer)*, pp. 407–425.
[19] J. M. Renes and R. Renner (2010), arXiv:1008.0452.
[20] I. Devetak and A. Winter, Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **461**, 207 (2005).
[21] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102** (2009).
[22] R. Renner, Nature Physics **3**, 645 (2007).
[23] V. Scarani and R. Renner, in *Proc. TQC* (2008), LNCS (Springer), pp. 83–95.
[24] D. Mayers and A. Yao, in *Proc. IEEE Symposium on Foundations of Computer Science* (1998), pp. 503–509.