Quantum to classical randomness extractors *

Mario Berta[1], Omar Fawzi[2], and Stephanie Wehner[3]

[1] Institute for Theoretical Physics, ETH Zurich berta@phys.ethz.ch
[2] School of Computer Science, McGill University ofawzi@cs.mcgill.ca
[3] Centre for Quantum Technologies, National University of Singapore
wehner@nus.edu.sg

Abstract. The goal of randomness extraction is to distill (almost) perfect randomness from a weak source of randomness. When the source outputs a classical string X, many extractor constructions are known. Yet, when considering a physical randomness source, X is itself ultimately the result of a measurement on an underlying quantum system. When characterizing the power of a source to supply randomness it is hence a natural question to ask, how much *classical* randomness we can extract from a *quantum* system. To tackle this question we here take on the study of *quantum-to-classical randomness extractors* (QC-extractors).

We provide constructions of QC-extractors based on measurements in a full set of mutually unbiased bases (MUBs), and certain single qubit measurements. The latter are particularly appealing since they are not only easy to implement, but appear throughout quantum cryptography. We proceed to prove an upper bound on the maximum amount of randomness that we could hope to extract from any quantum state. Some of our QC-extractors almost match this bound. We show two applications of our results.

First, we show that any QC-extractor gives rise to entropic uncertainty relations with respect to quantum side information. Such relations were previously only known for two measurements. In particular, we obtain strong relations in terms of the von Neumann (Shannon) entropy as well as the min-entropy for measurements in (almost) unitary 2-designs, a full set of MUBs, and single qubit measurements in three MUBs each.

Second, we finally resolve the central open question in the noisy-storage model [Wehner et al., PRL 100, 220502 (2008)] by linking security to the quantum capacity of the adversary's storage device. More precisely, we show that any two-party cryptographic primitive can be implemented securely as long as the adversary's storage device has sufficiently low quantum capacity. Our protocol does not need any quantum storage to implement, and is technologically feasible using present-day technology.

Keywords: randomness extractors, randomness expansion, entropic uncertainty relations, mutually unbiased bases, quantum side information, two-party quantum cryptography, noisy-storage model.

* A full version with complete proofs can be found online arXiv:1111.2026.

1 Introduction

Randomness is an essential resource for information theory, cryptography, and computation. However, most sources of randomness exhibit only weak forms of unpredictability. The goal of randomness extraction is to convert such weak randomness into (almost) uniform random bits. Classically, a weakly random source simply outputs a string X where the 'amount' of randomness is measured in terms of the probability of guessing the value of X ahead of time. That is, it is measured in terms of the min-entropy $H_{\min}(X) = -\log P_{\text{guess}}(X)$. To convert X to perfect randomness, one applies a function Ext that takes X, together with a shorter string R of perfect randomness (the *seed*) to an output string $K = \text{Ext}(X, R)$. The use of a seed is thereby necessary to ensure that the extractor works for all sources X about which we know only the min-entropy, but no additional details of the source. Much work has been invested into showing that particular classes of functions have the property that K is indeed very close to uniform as long as the min-entropy of the source $H_{\min}(X)$ is large enough (see [37] for a survey).

Yet, for most applications this is not quite enough, and we want an even stronger statement. In particular, imagine that we hold some quantum system E containing *side information* about X that increases our guessing probability to $P_{\text{guess}}(X|E)$. For example, such side information could come from an earlier application of an extractor to the same source. Intuitively, one would not talk about randomness if e.g., the output is uniformly distributed, but identical to an earlier output. In a cryptographic setting, side information can also be gathered by an adversary during the course of the protocol. We thus ask that the output is perfectly random even with respect to such side information, i.e., uniform *and* independent of E. Classically, it is known that extractors are indeed robust against classical side information [23], yielding a uniform output K, whenever the min-entropy about X *given access to side information* E ($H_{\min}(X|E) = -\log P_{\text{guess}}(X|E)$) is sufficiently high. Especially with respect to cryptographic applications, we thereby again want extractors that work for any source X of sufficiently high entropy $H_{\min}(X|E)$ without any additional assumptions about the source.

Recently, it has been recognized that since the underlying world is not classical, E may in fact hold *quantum* side information about X [21,35]. That this adds substantial difficulty to the problem was emphasized in [17] where it was shown that there are in fact situations where using the same extractor gives a uniform output K if E is classical, but is entirely predictable when E is quantum. Positive results were obtained in [35,23,34,42], eventually culminating in [39,12], proving that a wide class of classical extractors (with relatively short seed) yield a uniform output, as long as $H_{\min}(X|E)$ is sufficiently large.

Yet, in a fully quantum world we might ask ourselves: where does X itself come from? How can we hope to harness weak sources to obtain a *surplus* of classical randomness? Indeed, for any physical source hoping to create fresh randomness, X is the result of a measurement on a quantum system A. That is, we can view the source as consisting of in fact two processes: First, a *quantum*

source emits a state ρ_A. Second, a measurement takes place yielding the classical string X. Note that quantum mechanics does allow many different measurements on ρ_A, and hence the question arises whether all such measurements are equally powerful at yielding a (weakly) random classical string X, or whether some are more useful to us than others. As such, it becomes clear that when trying to study our ability to extract randomness from any physical source, it is natural to ask how much randomness we can obtain from ρ_A itself, rather than a classical distribution X that might be the outcome of a particular measurement.

The problem of extracting randomness from X alone is further complicated by the fact that it is typically very hard to bound $H_{\min}(X|E)$, when X is the result of quantum measurements on A, *even* if we know stringent bounds on the *quantum* correlations between A and E to begin with. When E is trivial, entropic uncertainty relations [45] give such bounds when we are willing to average over a few randomly chosen measurements. A crude bound on $H_{\min}(X|E)$ can then be obtained by assuming that the size of E is limited. But even classically, it is easy to see that there exist scenarios where bounding the adversaries' knowledge simply by his memory size yields very weak bounds [24]. Another approach to bounding $H_{\min}(X|E)$, common in e.g., Quantum Key Distribution (QKD), is possible in the case when randomness is extracted from a state ρ_{ABE} where measurements are made on both A and B to obtain an estimate of $H_{\min}(X|E)$ where X is obtained from A alone [41,8,31,9]. Part of the state is thereby consumed during the estimation process, which itself requires randomness. It is nevertheless possible to have an overall gain in randomness. For example, it is known that if measurements[4] between systems A and B lead to a so-called Bell inequality violation, then E knows little about X [8,31,9]. Clearly, making such an estimate is only possible in a special setting where the states have a particular form ρ_{ABE}, and we are given access to B *and* A.

1.1 Quantum to classical extractors

This leads us to study *quantum-to-classical randomness extractors* (QC-extractors). Our goal is to answer the following question: how can we extract *classical* randomness from a physical source ρ_{AE} by performing measurements on the *quantum* state ρ_A? In analogy to classical extractors, we thereby want to obtain randomness from the source given only a minimal guarantee about its randomness - i.e., like min-entropy $H_{\min}(X|E)$ for classical sources. It is important to note that unlike the classical world, quantum mechanics does allow for the creation of true randomness *if* we are given full control of the source and can prepare any state ρ_A at will.[5] However, we want our extractors to work for *any* unknown source as long as it has sufficiently high entropy.

As opposed to classical-to-classical extractors (CC-extractors) given by functions $\mathrm{Ext}(\cdot, R)$ mapping the outcome of the randomness source to a string K,

[4] That satisfy the no-signalling condition.

[5] For example, we could prepare the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and measure it in the computational basis, yielding a truly random outcome. Yet, this would correspond to controlling and knowing details of the source.

a QC-extractor is described by projective measurements whose outcomes correspond to a classical string K. That is, a QC-extractor is a set of measurements $\{\mathcal{M}^1_{A\to K}, \ldots, \mathcal{M}^L_{A\to K}\}$, where the random seed R determines the measurement $\mathcal{M}^R_{A\to K}$ that we will perform (see Section 3 for a detailed explanation and a formal definition).[6]

When talking about quantum states ρ_{AE}, what is the relevant measure of how weak or strong a source is? To gain some intuition on what the relevant measure should be, consider the case where ρ_{AE} is the maximally entangled state between A and E. Intuitively, this is the strongest quantum correlation that can exist between two systems. It is not hard to see that if we measure A in *any* basis to obtain some outcome X, and later communicate the choice of basis to an adversary holding E, then the adversary can guess X perfectly. Intuitively, we would thus expect that the relevant measure of how weak a quantum source is with respect to E involves a measure of the amount of entanglement between A and E. It turns out that the conditional min-entropy $H_{\min}(A|E)$ is exactly such a measure [22], and we find that it is indeed the quantity that determines how many classical random bits we can hope to extract from A. That this is rather analogous to the classical case is very appealing. However, unlike for classical A, $H_{\min}(A|E)$ can be *negative* if A is quantum (see below).

Note that in a quantum setting, we could also consider a quantum-to-quantum extractor (QQ-extractor). That is, an extractor in which we do not measure but merely ask that the resulting state is quantumly fully random (i.e., maximally mixed) and uncorrelated from E. Clearly, any QQ-extractor also forms a QC-extractor since any subsequent measurement on the maximally mixed state has a uniform distribution over outcomes. As such a QQ-extractor is stronger than a QC-extractor since for the latter we only require the output state to be close to uniform *after* performing a measurement.[7] Constructions for such extractors are indeed well known in quantum information theory as a consequence of a notion known as 'decoupling', which plays a central role in quantum information theory (see [18,13,14] and references therein). In general, a map that transforms a state ρ_{AE} into a state that is close to a product state $\sigma_A \otimes \rho_E$ is a decoupling map. Decoupling processes thereby typically take the form of choosing a random unitary from a set $\{U_1, \ldots, U_L\}$, applying this unitary to the system $A = A_1A_2$ and tracing out (i.e., ignoring) the system A_2. For certain classes of unitaries such as (almost) unitary 2-designs [14,38] (see below) the resulting state ρ_{A_1E} is close to maximally mixed on A_1 and uncorrelated from E,

[6] For quantum information theorists, note that one can of course performing successive measurements - however, recall that we are interested in how much randomness we can obtain from an unknown source using a single measurement. The latter is furthermore motivated by experimental situations where successive measurements are typically very hard to implement.

[7] In quantum mechanics, it is possible to obtain a uniform distribution over outcomes even if the state was not maximally mixed. E.g., consider measuring the pure state $|0\rangle\langle 0|$ in the Fourier basis.

whenever $H_{\min}(A|E)$ is sufficiently large. Measurements consisting of applying such a unitary, followed by a measurement on A_1 thus also yield QC-extractors.[8]

The authors of [2] also proposed a definition of quantum extractors that is indeed somewhat similar to a QQ-extractor, however without any side information E. Our definitions (see Section 3) impose two important requirements not present in [2, Definition 5.1]. Firstly, we require the output of the extractor to be unpredictable for any, possibly quantum, adversary with access to side information E provided $H_{\min}(A|E)$ is large enough. Secondly, we consider *strong* extractors so that even given the seed R, the output of the extractor cannot be predicted. This allows us to employ our extractor for cryptographic purposes. It also means that the output K *together with* R are jointly close to uniform, meaning that we have effectively created *more* almost perfect randomness than we invested in the seed.

QC-extractors. We give two novel constructions of QC-extractors.[9] The first one involves a full set of mutually unbiased bases (MUBs) and pair-wise independent permutations (Theorem 3). This construction is more appealing than unitary 2-designs because it is combinatorially simpler to describe and computationally more efficient, while having the same output size.
Our second construction (Theorem 4) is composed of unitaries acting on single qudits followed by some measurements in the computational basis. We also refer to these as *bitwise* QC-extractors. An appealing feature of the measurements defined by these unitaries is that they can be implemented *with current technology*. In addition to computational efficiency, the fact that the unitaries act on a single qubit is often a desirable property for the design of cryptographic protocols in which the creation of randomness is not the only requirement for security. Our example application below (see also Section 5) illustrates this.
Finally, we also prove in Proposition 1 that the maximum amount of randomness one can hope to extract is roughly $n + H_{\min}(A|E)$, where n denotes the input size. This upper bound can indeed be almost achieved by means of, e.g., our full set of MUBs QC-extractor. We also establish basic upper and lower bounds on the seed size for QC-extractors (see Table 1).

The technique we use to prove that our constructions are QC-extractors is to bound the distance between the output of the extractor and the desired output in Hilbert-Schmidt norm (cf. [38]). For the full set of MUBs, this distance can even be computed *exactly*. We use the fact that the set of all the MUB vectors forms a complex projective 2-design and that the set of permutations is pair-wise independent. For our second construction, the analysis uses similar ideas

[8] For decoupling experts, note that the measurement map in a QC-extractor can be understood as a decoupling map. We would like to emphasize though that our QC-extractor results do not follow from previous work on decoupling, and our measurements have many nice properties not shared by unitaries used previously for decoupling.

[9] That is, not following from results on QQ-extractors (i.e., from general decoupling theorems in quantum information theory).

in a more involved calculation. Our upper bound on the amount of extractable randomness follows from simple monotonicity properties of the min-entropy. The upper bound on the seed size follows from a non-explicit construction involving concentration-of-measure techniques.

1.2 Application to entropic uncertainty relations

One of the fundamental ideas in quantum mechanics is the uncertainty principle. The security of essentially all quantum cryptographic protocols is founded on its existence. Intuitively, it states that even with complete knowledge about the quantum state ρ_A of a system A, it is impossible to predict the outcomes of all possible measurements on A with certainty. In an information theoretic context it is very natural to quantify this lack of knowledge in terms of entropic uncertainty relations (see [45] for a survey). Apart from their deep significance in the foundations of quantum mechanics, entropic uncertainty relations are crucial tools in quantum information theory and quantum cryptography. The most well-known relation is for two measurements $\mathcal{M}^1_{A\to K}, \mathcal{M}^2_{A\to K}$ and reads [27]

$$\frac{1}{2}\sum_{j=1}^{2} H(K)_{\rho^j} \geq \log\frac{1}{c}\ , \tag{1}$$

where $H(K)_{\rho^j}$ denotes the Shannon entropy of the post-measurement probability distributions $\rho^j_K = \mathcal{M}^j_{A\to K}(\rho_A)$, and c measures the overlap between the measurements. Note that for any quantum state ρ_A and measurements for which $c \neq 1$, at least one of the entropies has to be greater than zero. In other words, it is impossible to predict the outcomes of both measurements with certainty. Uncertainty relations are thereby called *strong*, if $\log(1/c)$ is large.

Just as extractors can depend on side information E, it is important to realize that also uncertainty should in fact not be treated as an absolute, but with respect to the prior knowledge of an observer who has access to a quantum system E [46]. As an illustration, recall the example from above where ρ_{AE} is the maximally entangled state. In this case, for any measurement on A, there is a corresponding measurement on E that reproduces the measurement outcomes. I.e., there is no uncertainty in the outcome at all! In order to take into account possibly quantum information about A, one needs to prove new entropic uncertainty relations that would have an additional term quantifying the quantum side information. Unfortunately, up to this day, we only know such relations for *two* measurements [4,33,41]. Intuitively, uncertainty relations for two measurements are much easier to prove than relations for more measurements as in this case uncertainty coincides with another foundational notion in quantum information, complementarity. This notion is relevant when we perform two measurements in succession and was an essential ingredient in the proofs. However, it does not carry over to three or more measurements. Here, we prove the following results.

Uncertainty relations with quantum side information for more than two measurements. We show that any set of measurements forming a QC-extractor yields an entropic uncertainty relation *with respect to*

quantum side information. We thereby obtain relations both for the usual von Neumann (Shannon) entropy, as well as the min-entropy. The latter is relevant for cryptographic applications. This yields the first uncertainty relations with quantum side information for more than two measurements. From our QC-extractors, we obtain strong uncertainty relations for (almost) unitary 2-designs, measurements in a full set of mutually unbiased bases (MUBs) on the whole space, as well as on many single qudits. The latter are the measurements used e.g., in the six-state protocol of QKD, and are particularly relevant for applications in quantum cryptography.

Note that uncertainty relations in terms of the min-entropy effectively help us to bound $H_{\min}(X|ER)$, where R is the seed for the QC-extractor (see Section 4 for details). For example, for the full set of MUBs we prove that

$$H_{\min}(X|ER) \gtrsim \log |A| + H_{\min}(A|E) \ , \tag{2}$$

where the output of the measurements is called X. Since $H_{\min}(A|E)$ is negative when A and E are entangled, one obtains less uncertainty in this case (as expected when considering the example of a maximally entangled state given above). Of course, given such a bound, we could in turn apply a CC-extractor to the weakly random string X to obtain a uniform K. This underscores the beautiful relation between the concept of randomness extraction from a quantum state, and the notion of uncertainty relations with side information in quantum physics. From a QC-extractor, we obtain uncertainty relations. In turn, from any measurements inducing strong uncertainty relations *plus* a CC-extractor, we obtain a QC-extractor.[10]

1.3 Application to cryptography

Our second application is to proving security in the noisy-storage model. Unfortunately, it turns out that even quantum communication does not enable us to solve two-party cryptographic problems between two parties that do not trust each other [25]. Such problems include e.g., the well-known primitives bit commitment and oblivious transfer [26,7,30,5], of which merely very weak variants are possible. How can this be when quantum communication offers such great advantages when it comes to distributing encryption keys? Intuitively, the security proof of QKD is considerably simplified by the fact that Alice and Bob do trust each other, and can collaborate to check for any eavesdropping activity. For example, as mentioned above, when Alice and Bob share a state ρ_{ABE}, where the eavesdropper holds E, they can use up part of the state to obtain an estimate of $H_{\min}(X|E)$, where X is a measurement outcome of the remaining part of Alice's system.

Yet, since two-party cryptographic protocols are a central part of modern cryptography, one is willing to make assumptions on how powerful the adversary can be in order to obtain security. Classically, these assumptions typically

[10] Note that measurements plus a classical post-processing effectively forms a new, larger, set of measurements.

consist of two parts. First, one assumes that a particular problem requires a lot of computational resources to solve in some precise complexity-theoretic sense. Second, one assumes that the adversary does indeed have insufficient computational resources. However, we might instead ask whether there are other, more *physical* assumptions that enable us to solve such tasks?

Classically, it is possible to obtain security, when we are willing to assume that the adversary's *classical* memory is limited in size [29,6]. Yet, apart from the fact that classical storage is by now cheap and plentiful, the beautiful idea of assuming a limited classical storage has one rather crucial caveat: *any* classical protocol in which the honest players need to store n classical bits to execute the protocol can be broken by an adversary who is able to store more than $O(n^2)$ bits [15]. Motivated by this unsatisfactory gap, it was thus suggested to assume that the attacker's *quantum* storage was bounded [11,10], or, more generally, noisy [44,36,24]. The central assumption of the so-called *noisy-storage model* is that during waiting times Δt introduced in the protocol, the adversary can only keep quantum information in his quantum storage device $\mathcal{F}$. Otherwise, the attacker may be all powerful. In particular, he can store an unlimited amount of classical information, and perform computations 'instantaneously'. The latter implies that the attacker could encode his quantum information into an arbitrarily complicated error correcting code to protect it from any noise in $\mathcal{F}$ (see Section 5 for details). Of particular interest are thereby quantum memories consisting of N 'memory cells', each of which undergoes some noise described by a channel $\mathcal{N}$. That is, the memory device is of the form $\mathcal{F} = \mathcal{N}^{\otimes N}$. Note that the bounded storage model is a special case, where each memory cell is just one qubit, and $\mathcal{N}$ is the identity channel. To relate the number of transmitted qubits n to the size of the storage device one typically chooses the *storage rate* ν such that $N = \nu \cdot n$. We follow this convention here to ease comparison with earlier work.

Since its inception [44], it was clear that security in the noisy-storage model should be related to the question of how much information the adversary can send through his noisy storage device. That is, the capacity of $\mathcal{F}$ to transmit quantum information. Initial progress was made in [24] where security was linked to the storage device's ability to transmit *classical* information and shown against fully general attacks.[11] Further progress was made only very recently, linking the security to the so-called entanglement cost of the storage device [3], which lies between its classical and quantum capacities.

Security and the quantum capacity. Here, we finally resolve the question of linking security in the noisy-storage model to the quantum capacity of the storage device. More precisely, we show that any two-party cryptographic primitive can be implemented securely under the assumption that

[11] Before [24], security was only shown under the additional assumption that the adversary attacks each qubit individually [44]. Whereas this may sound similar to problems in QKD, note that the setting is entirely different when proving security between two mutually distrustful parties, and security in QKD does not imply security in this model.

the adversary is restricted to using a quantum storage device of the form $\mathcal{F} = \mathcal{N}^{\otimes \nu \cdot n}$ by means of a protocol transmitting n qubits whenever

$$\nu \cdot \mathcal{Q}(\mathcal{N}) < 1 \ , \text{ and } 2 - \log(3) \lesssim \nu \cdot \gamma^{Q}(\mathcal{N}, 1/\nu) \ , \tag{3}$$

where $\mathcal{Q}(\mathcal{N})$ is the quantum capacity of the channel $\mathcal{N}$ and $\gamma^{Q}(\mathcal{N}, 1/\nu)$ is the so-called strong converse parameter of $\mathcal{N}$ for sending information through $\mathcal{F}$ at rate $R = 1/\nu$. Note that the second condition actually *does* favor small ν, since $\gamma^{Q}(\mathcal{N}, 1/\nu)$ is large whenever the rate $R = 1/\nu$ is large. A similar statement can be obtained for general channels $\mathcal{F}$ (see Section 5 for details).

We prove our result by showing the security of a simple quantum protocol for the cryptographic primitive *weak string erasure* [24], which is known to be universal for two-party secure computation [24]. To this end, we employ the bitwise QC-extractor for measurements of single qubits, each in one of three MUBs, known from the six-state protocol in QKD.

2 Preliminaries

In this section, we briefly recall the definitions and notations we need. More details can be found in the full version.

In quantum mechanics, a system such as Alice's or Bob's labs are described mathematically by *Hilbert spaces*, denoted by $A, B, C, \ldots$. Here, we follow the usual convention in quantum cryptography and assume that all *Hilbert spaces* are finite-dimensional. We write $|A|$ for the dimension of A. The set of linear operators on A is denoted by $\mathcal{L}(\mathcal{A})$. A *quantum state* ρ_A is an operator $\rho_A \in \mathcal{S}(A)$, where $\mathcal{S}(A) = \{\sigma_A \in \mathcal{L}(A) \mid \sigma_A \geq 0, \mathrm{tr}(\sigma_A) = 1\}$. For a bipartite system $A = A_1 A_2$, we define the *measurement map* $\mathcal{T}_{A \to A_1} : \mathcal{L}(A) \to \mathcal{L}(A_1)$,

$$\mathcal{T}(.)_{A \to A_1} = \sum_{a_1 a_2} \langle a_1 a_2 | (.) | a_1 a_2 \rangle | a_1 \rangle \langle a_1 | \ , \tag{4}$$

where $\{|a_1\rangle\}, \{|a_2\rangle\}$ are (standard) orthonormal bases of A_1, A_2 respectively. When applying a unitary transformation U_j followed by the measurement map $\mathcal{T}_{A \to A_1}$, we obtain new measurements which we denote by $\mathcal{M}^{j}_{A \to K_1}$. Here the relabeling $A_1 \to K_1$ accounts for the fact that the output system is classical.

The *conditional min-entropy* of a state $\rho_{AB} \in \mathcal{S}(AB)$ is defined as

$$H_{\min}(A|B)_{\rho} = \max_{\sigma_B \in \mathcal{S}(B)} H_{\min}(A|B)_{\rho|\sigma} \tag{5}$$

$$\text{with } \ H_{\min}(A|B)_{\rho|\sigma} = \max \left\{ \lambda \in \mathbb{R} : 2^{-\lambda} \cdot \mathbb{I}_A \otimes \sigma_B \geq \rho_{AB} \right\} \ .$$

The smoothed version is defined by $H^{\varepsilon}_{\min}(A|B)_{\rho} = \max_{\tilde{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}$, where $\mathcal{B}^{\varepsilon}(\rho)$ is the set of states at a distance at most ε from ρ. We use the purified distance as the distance measure [40].

3 Quantum to Classical Randomness Extractors

To understand the definition of quantum extractors, it is convenient to see a classical extractor as a family of (deterministic) permutations acting on the possible values of the source. This family of permutations should satisfy the following property: for any probability distribution on input bit strings with high min-entropy, applying a typical permutation from the family to the input induces an almost uniform probability distribution on a prefix of the output. We define a quantum to classical extractor in a similar way by allowing the operations performed to be general unitary transformations followed by a measurement in the computational basis.

Definition 1. *Let $A = A_1A_2$ with $n = \log|A|$. Let $\mathcal{T}_{A\to A_1}$ be the measurement map defined in Equation (4).*

For $k \in [-n, n]$ and $\varepsilon \in [0, 1]$, a (k, ε)-QC-extractor is a set $\{U_1, \ldots, U_L\}$ of unitary transformations on A such that for all states $\rho_{AE} \in \mathcal{S}(AE)$ with $H_{\min}(A|E)_\rho \geq k$, we have

$$\frac{1}{L}\sum_{i=1}^{L}\left\|\mathcal{T}_{A\to A_1}\left((U_i\otimes\mathbb{I}_E)\rho_{AE}(U_i^\dagger\otimes\mathbb{I}_E)\right)-\frac{\mathbb{I}_{A_1}}{|A_1|}\otimes\rho_E\right\|_1\leq\varepsilon\ . \tag{6}$$

Observe that Definition 1 only allows a specific form of measurements obtained by applying a unitary transformation followed by a measurement in the computational basis of A_1. The reason we use this definition is that we want the output of the extractor to be determined by the source and the choice of the seed. In the quantum setting, a natural way of translating this requirement is by imposing that an adversary holding a system that is maximally entangled with the source can perfectly predict the output. This condition is satisfied by the form of measurements dictated by Definition 1. Allowing generalized measurements (POVMs) already (implicitly) allows the use of randomness for free. Note also, that in the case where the system E is trivial, a $(0, \varepsilon)$-QC-extractor is the same as an ε-metric uncertainty relation [16].

3.1 Examples and limitations of QC-extractors

The following is immediate using a general decoupling result from [13,14].

Theorem 1 (Unitary 2-designs are QC-extractors). *Let $A = A_1A_2$ with $n = \log|A|$. For all $k \in [-n, n]$ and all $\varepsilon > 0$, a unitary 2-design $\{U_1, \ldots, U_L\}$ on A is a (k, ε)-CQ-extractor with output size*

$$\log|A_1| = \min(n, n + k - 2\log(1/\varepsilon)). \tag{7}$$

The following theorem shows that choosing unitaries at random defines a QC-extractor with high probability. The seed size in this case is of the same order as the output size of the extractor. We expect that a much smaller seed size would be sufficient.

Theorem 2 (Random unitaries are QC-extractors). *Let $A = A_1A_2$ with $n = \log|A|$ and $\mathcal{T}_{A\to A_1}$ be the measurement map defined in Equation (4). Let $\varepsilon > 0$, c be a sufficiently large constant, and*

$$\log|A_1| \leq n + k - 4\log(1/\varepsilon) - c \quad \text{and} \quad \log L \geq \log|A_1| + \log n + 4\log(1/\varepsilon) + c. \tag{8}$$

Then, choosing L unitaries $\{U_1, \ldots, U_L\}$ independently according to the Haar measure defines a (k, ε)-QC-extractor with high probability.

The proof uses one-shot decoupling techniques [14,38,13] combined with an operator Chernoff bound [1]. We now give some limitations on the output size and seed size of QC-extractors. The following proposition shows that even if we are looking for a QC-extractor that works for a particular state ρ_{AE}, the ouput size is at most roughly $n + H_{\min}(A|E)_\rho$, where n denotes the size of the input.

Proposition 1 (Upper bound on the output size). *Let $A = A_1A_2$, $\rho_{AE} \in \mathcal{S}(AE)$, $\{U_1, \ldots, U_L\}$ a set of unitaries on A, and $\mathcal{T}_{A\to A_1}$ defined as in Equation (4), such that, $\frac{1}{L}\sum_{i=1}^{L} \left\| \mathcal{T}_{A\to A_1}\left(U_i\rho_{AE}U_i^\dagger\right) - \frac{\mathbb{I}_{A_1}}{|A_1|} \otimes \rho_E \right\|_1 \leq \varepsilon$. Then, $\log|A_1| \leq \log|A| + H_{\min}^{\sqrt{\varepsilon}}(A|E)_\rho$.*

The proof uses monotonicity properties of the min-entropy. Concerning the seed size, a simple argument shows that the number of unitaries of a QC-extractor has to be at least about $1/\varepsilon$. It is interesting to observe that in the case where the system E is trivial (or classical), this bound is almost tight. In fact, it was shown in [16] that in this case, there exists QC-extractors with $L = O(\log(1/\varepsilon)\varepsilon^{-2})$ unitaries. This is a difference with classical extractors for which the number of possible values of the seed is at least $\Omega((n-k)\varepsilon^{-2})$ [32].

3.2 Full set of mutually unbiased bases (MUBs)

We saw that unitary 2-designs define QC-extractors. As unitary 2-designs also define QQ-extractors, it is natural to expect that we can build smaller and simpler sets of unitaries if we are only interested in extracting random classical bits. In fact, in this section, we construct simpler sets of unitaries that define a QC-extractor. Two ingredients are used: a full set of mutually unbiased bases and a family of pair-wise independent permutations.

A set of unitaries $\{U_1, \ldots, U_L\}$ acting on A is said to define *mutually unbiased bases* if for all elements $|a\rangle, |a'\rangle$ of the computational basis of A, we have $|\langle a'|U_jU_i^\dagger|a\rangle|^2 \leq |A|^{-1}$ for all $i \neq j$. In other words, a state described by a vector $U_i^\dagger|a\rangle$ of the basis i gives a uniformly distributed outcome when measured in basis j for $i \neq j$. For example the two bases, sometimes called computational and Hadamard bases (used in most quantum cryptographic protocols), are mutually unbiased. There can be at most $|A| + 1$ mutually unbiased bases for A. Constructions of full sets of $|A| + 1$ MUBs are known in prime power dimensions [47].

A family $\mathcal{P}$ of permutations of a set X is *pair-wise independent* if for all $x_1 \neq x_2$ and $y_1 \neq y_2$, and if π is uniformly distributed over $\mathcal{P}$, $\mathbf{Pr}\{\pi(x_1) = y_1, \pi(x_2) = y_2\} = \frac{1}{|X|(|X|-1)}$. If X has a field structure, i.e., if $|X|$ is a prime power, it is simple to see that the family $\mathcal{P} = \{x \mapsto a \cdot x + b : a \in X^*, b \in X\}$ is pair-wise independent. In the following, permutations of basis elements of a Hilbert space A should be seen as a unitary transformation on A. In this section and the following $\mathcal{P}$ denotes this set of pair-wise independent permutations.

Theorem 3. *Let $\{U_1, \ldots, U_{|A|+1}\}$ define a full set of mutually unbiased bases and $\mathcal{P}$ be a family of pair-wise independent permutations. Then the set $\{PU_i : P \in \mathcal{P}, i \in [|A|+1]\}$ defines a (k, ε)-QC-extractor provided $\log|A_1| \leq n + k - 2\log(1/\varepsilon)$. The number of unitaries of this extractor is $L = (|A|+1)|\mathcal{P}| = (|A|+1)|A|(|A|-1)$.*

The idea of the proof is to bound the trace norm by the Hilbert-Schmidt (or L_2-) norm of some well-chosen operator. This term is then computed exactly using the fact that the set of all the MUB vectors form a *complex projective* 2-design and the fact that the set of permutations is pair-wise independent.

3.3 Bitwise QC-extractor

The unitaries we construct in this section are even simpler. They are composed of unitaries V acting on single qudits followed by permutations P of the computational basis elements. Note that this means that the measurements defined by these unitaries can be implemented with current technology. As the measurement $\mathcal{T}$ commutes with the permutations P, we can first apply V, then measure in the computational basis and finally apply the permutation to the (classical) outcome of the measurement. In addition to the computational efficiency, the fact that the unitaries act on single qudits, is often a desirable property for the design of cryptographic protocols. In particular, the application to the noisy storage model that we present in Section 5 does make use of this fact.

Let $d \geq 2$ be a prime power so that there exists a complete set of mutually unbiased bases in dimension d. We represent such a set of bases by a set of unitary transformations $\{V_0, V_1, \ldots, V_d\}$ mapping these bases to the standard basis. For example, for the qubit space ($d = 2$), we can choose

$$V_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad V_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad V_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix} . \tag{9}$$

We define the set $\mathcal{V}_{d,n}$ of unitary transformations on n qudits by $\mathcal{V}_{d,n} := \{V = V_{u_1} \otimes \cdots \otimes V_{u_n} | u_i \in \{0, \ldots, d\}\}$. As in the previous section, $\mathcal{P}$ denotes a family of pair-wise independent functions.

Theorem 4. *The set $\{PV : P \in \mathcal{P}, V \in \mathcal{V}_{d,n}\}$ is a (k, ε)-extractor provided $\log|A_1| \leq (\log(d+1)-1)n + \min\{0, k\} - 4\log(1/\varepsilon) - 7$. The number of unitaries of this extractor is $L = (d+1)^n d^n (d^n - 1)$.*

The analysis uses the same technique as in the proof of Theorem 3. The main difference is that we were not able to express the L_2-norm exactly in terms of the conditional min-entropy $H_{\min}(A|E)_\rho$. We use some additional inequalities, which account for the slightly more complicated expression we obtain.

4 Application to Entropic Uncertainty Relations with Quantum Side Information

The first application of our result is to entropic uncertainty relations *with quantum side information*. It is not hard to prove than any set of unitaries $\{U_j\}_j$ that form a QC-extractor define measurements that satisfy entropic uncertainty relations with quantum side information. The measurement $\mathcal{M}^j_{A\to K}$ is defined by first performing the unitary U_j followed by a measurement in the standard basis. We denote the post-measurement state by

$$\rho_{KEJ} = \frac{1}{L}\sum_{j=1}^{L} \mathcal{M}^j_{A\to K}(\rho_{AE}) \otimes |j\rangle\langle j|_J \ , \tag{10}$$

where the classical register J tells us which measurement $\mathcal{M}^j_{A\to K}$ was applied. Here, we only state the most important uncertainty relations that are obtained from our constructions of QC-extractors. We refer the reader to the full version for a more detailed treatment.

Corollary 1. *Let $d \geq 2$ be a prime power and $\mathcal{M}^j_{A\to K}$ be the measurements defined by the unitaries $\{V_j\}_j = \mathcal{V}_{d,n}$ as defined in Theorem 4. For all $\varepsilon, \delta' > 0, \delta \geq 0$ such that $\varepsilon^2 > 2(\delta + \delta')$ and any state ρ_{AE}, we have*

$$H^\varepsilon_{\min}(K|EJ)_\rho \geq n\cdot(\log(d+1)-1) + \min\left\{0, H^\delta_{\min}(A|E)_\rho - \log\left(\frac{2}{\delta'^2} + \frac{1}{1-2\delta}\right)\right\} - \log\left(\frac{1}{(\varepsilon^2/2 - 2(\delta+\delta'))^2}\right) - 2,$$

where ρ_{KEJ} is defined in (10).

Concerning uncertainty relations for the von Neumann (Shannon) entropy, we would mainly like to point to the following proposition.

Proposition 2. *Let $\rho_{AE} \in \mathcal{S}(AE)$ with A an n-qudit system, i.e., $|A| = d^n$. Then, the measurements given by the single qudit unitaries as defined in Section 3.3, give rise to the entropic uncertainty relation*

$$\frac{1}{L}\sum_{j=1}^{L} H(K|E)_{\rho^j} \geq n\cdot(\log(d+1)-1) + \min\left\{0, H(A|E)_\rho\right\} \ . \tag{11}$$

Note that the conditional von Neumann entropy on the rhs can become negative and quantifies the entanglement present in the initial state.

Previously, uncertainty relations with quantum side information were only known for two measurements [4,33,41].

5 Applications to Security in the Noisy-Storage Model

As a second application, we solve the long standing question of relating the security of cryptographic protocols in the noisy-storage model [44,36,43,24] to the quantum capacity. We will state our main theorem and an example - a more gentle explanation and the protocol can be found in the full version. In [24] it was shown that bit commitment and oblivious transfer, and hence any two-party secure computation [20], can be implemented securely given access to a simpler primitive called *weak string erasure (WSE)*. It is hence enough to prove the security of WSE, and we will follow this approach here.

Informally, weak string erasure achieves the following task - a formal definition [24,28] can be found in the full version. WSE takes no inputs from either Alice and Bob. Alice receives as output a randomly chosen string $X^n = X_1, \ldots, X_n \in \{0,1\}^n$. Bob receives a randomly chosen subset $\mathcal{I} \in [n]$ and the substring $X_{\mathcal{I}}$ of X^n. Randomly chosen thereby means that each index $i \in [n]$ has some fixed probability p of being in $\mathcal{I}$. Originally, $p = 1/2$ [24], but any probability $0 < p < 1$ allows for the implementation of oblivious transfer [28]. The security requirements of weak string erasure are that Alice does not learn $\mathcal{I}$, and Bob's min-entropy given all of his information B is bounded as $H_{\min}(X|B) \geq \lambda n$ for some parameter $\lambda > 0$. To summarize all relevant parameters, we thereby speak of a $(n, \lambda, \varepsilon, p)$-WSE scheme.

For simplicity, we here include the general statement in terms of the channel fidelity F_c, and refer to the full version for an expression in terms of the strong converse parameter γ^Q. The channel fidelity is an important concept in quantum information as it is used as a measure of success of how well a channel can transmit quantum information. Very roughly, we can determine the maximum size of a quantum state that can be transmitted over $\mathcal{F}$ with an error of at most ε, by computing the maximum size of an input system A such that $\max_{\mathcal{D},\mathcal{E}} F_c(\mathcal{D} \circ (\mathcal{F} \otimes \mathcal{I}_M) \circ \mathcal{E}) \geq 1 - \varepsilon$ where $\mathcal{E}$ and $\mathcal{D}$ are encoding and decoding maps respectively, and M is a system allowing for free feed forward classical communication. This yields the ε-error quantum capacity.

Theorem 5. *Let Bob's storage device be given by $\mathcal{F}$. For any choice of constant parameters $\varepsilon, \delta' > 0$, Protocol 1 implements an $(n, \lambda, \varepsilon, 1/3)$-WSE with*

$$\lambda = \log(3) - 1 - \frac{1}{n}\left(\max_{\mathcal{D},\mathcal{E}} \log 2^n F_c(\mathcal{D} \circ (\mathcal{F} \otimes \mathcal{I}_M) \circ \mathcal{E}) + \kappa + \xi + 1\right) , \qquad (12)$$

where $\kappa = \log\left(2/\delta'^2 + 1\right)$ and $\xi = \log\left(1/\left(\varepsilon^2/2 - \delta'\right)^2\right)$.

To get some intuition about the parameters above, we consider the example of bounded, noise-free, storage. The quantum capacity of the one qubit identity channel $\mathcal{N} = \mathcal{I}_2$ is simply $Q_{\rightarrow}(\mathcal{I}_2) = 1$. When Bob can store $\nu \cdot n$ qubits, i.e., his storage device is of the form $\mathcal{F} = \mathcal{I}_2^{\otimes \nu n}$ then security for any two-party protocol is possible if $\nu \lesssim \log(3) - 1 \approx 0.585$.

It should be noted that the parameters obtained here for the case of bounded storage are slightly worse than what was obtained in [28] where security was shown to be possible for $\nu < 2/3$ instead of $\nu \lesssim 0.585$. This is due to the fact that the lower bound 0.585 in our uncertainty relation stems from an expression involving the *collision* entropy rather than the Shannon entropy. We emphasize, however, that for the practically relevant regime of $n \lesssim 10^6$ our exact bound is still better for the same error parameters. Our result resolves the long standing question of relating security to the quantum capacity, and opens the door for improved results on strong converse parameters for *any* kind of storage device to be applied immediately to obtain security parameters.

6 Discussion and Outlook

Motivated by the problem of using physical resources to extract true classical randomness, we introduced the concept of quantum-to-classical randomness extractors. We emphasize that these QC-extractors also work against quantum side information. We showed that for a QC-extractor to distill randomness from a quantum state ρ_{AE}, the relevant quantity to bound is the conditional min-entropy $H_{\min}(A|E)_\rho$. This is in formal analogy with classical-to-classical extractors, in which case the relevant quantity is $H_{\min}(X|E)_\rho$.

We proceeded by showing various properties of QC-extractors and giving several examples for QC-extractors. Table 1 gives a comparison between our results on QC-extractors and known results about CC-extractors (holding against quantum side information as well). It is eye-catching that there is a vast difference between the upper and lower bounds for the seed size of QC-extractors. We were only able to show the existence of QC-extractors with seed length roughly the output size m, but we believe that it should be possible to find QC-extractors with much smaller seeds, say $O(\text{polylog}(n))$ bits long, where n is the input size. However, different techniques are needed to address this question.

It is interesting to note that our results do indeed lend further justification to use Bell tests to certify randomness created by measuring a quantum

		CC-extractors	QC-extractors
Seed	Low. bound	$\log(n-k) + 2\log(1/\varepsilon)$ [32]	$\log(1/\varepsilon)$
	Upp. bounds	$c \cdot \log(n/\varepsilon)$ [12]	$m + \log n + 4\log(1/\varepsilon)$ [Th 2] (NE) $3n$ [Th 3]
Output	Upp. bound	$k - 2\log(1/\varepsilon)$ [32]	$n + H_{\min}^{\sqrt{\varepsilon}}(A\|E)$ [Pr 1]
	Low. bound	$k - 2\log(1/\varepsilon)$ [19,35,42]	$n + k - 2\log(1/\varepsilon)$ [Th 3]

Table 1. Known bounds on the seed size and output size in terms of (qu)bits for different kinds of (k, ε)-randomness extractors. n refers to the number of input (qu)bits, m the number of output (qu)bits and k the min-entropy of the input $H_{\min}(A|E)$. Note that for QC-extractors, k can be as small as $-n$. Additive absolute constants are omitted. The symbol (NE) denotes non-explicit constructions.

system [8,31,9]. Note that for a tripartite pure state ρ_{ABE} where we want to create classical randomness by means of QC-extractors on A, we have to find a lower bound on $H_{\min}(A|E)_\rho$. But by the duality relation for min/max-entropies we have $H_{\min}(A|B)_\rho = -H_{\max}(A|B)_\rho$ [40], where the latter denotes the max-entropy as introduced [22]. Since $H_{\max}(A|B)_\rho$ is again a measure for the entanglement between A and B, one basically only has to do entanglement witnessing (e.g., Bell tests consuming part of the state) to ensure that the QC-extractor method can work (i.e., that $H_{\min}(A|E)_\rho$ is large enough). Note that any method to certify such an estimate would do and we could also use different measurements during the estimation process and the final extraction step. It would be interesting to know, if by using a particular QC-extractor, one can gain more randomness than in [8,31,9].

As the first application, we showed that every QC-extractor gives rise to entropic uncertainty relations with quantum side information for the von Neumann (Shannon) entropy and the min-entropy. Here the seed size translates into the number of measurements in the uncertainty relation. Since it is in general difficult to obtain uncertainty relations for a small set of measurements (except for the special case of two), finding QC-extractors with a small seed size is also worth pursuing from the point of view of uncertainty relations.

As the second application, we used the bitwise QC-extractor from Section 3.3 to show that the security in the noisy storage model can be related to the strong converse rate of the quantum storage; a problem that attracted quite some attention over the last few years. Here one can also see the usefulness of *bitwise* QC-extractors for quantum cryptography. Indeed, any bitwise QC-extractor would yield a protocol for weak string erasure. Bitwise measurements have a very simple structure, and hence are implementable with current technology. In that respect, it would be interesting to see if a similar QC-extractor can also be proven for only two (complementary) measurements per qubit. This would give a protocol for weak string erasure using BB84 bases as in [24].

We expect that QC-extractors will have many more applications in quantum cryptography, e.g., quantum key distribution. One possible interesting application could be to prove the security of oblivious transfer when purifying the protocol of [24]. Yet, it would require additional concepts of 'entanglement sampling' which still elude us.

References

1. R. Ahlswede and A. Winter. Strong converse for identification via quantum channels. *IEEE Trans. Inform. Theory*, 48:569–579, 2010. Addendum ibid 49:346, 2003, arXiv:quant-ph/0012127v2.
2. A. Ben-Aroya, O. Schwartz, and A. Ta-Shma. Quantum expanders: Motivation and construction. *Theory of Computing*, 6:47–79, 2010.
3. M. Berta, F. Brandao, M. Christandl, and S. Wehner. Entanglement cost of quantum channels. arXiv:1108.5357, 2011.
4. M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nat. Phys.*, 6:659, 2010. arXiv:0909.0950v4.

5. H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner. Security of quantum bit string commitment depends on the information measure. *Phys. Rev. Lett.*, 97:250501, 2006. arXiv:quant-ph/0609237v2.
6. C. Cachin and U. M. Maurer. Unconditional security against memory-bounded adversaries. In *Proc. CRYPTO*, Lecture Notes in Computer Science, pages 292–306, 1997.
7. H.F. Chau and H-K. Lo. Making an empty promise with a quantum computer. *Fortschritte der Physik*, 46:507–520, 1998. Republished in 'Quantum Computing, where do we want to go tomorrow?' edited by S. Braunstein, arXiv:quant-ph/9709053v2.
8. R. Colbeck. *Quantum and relativistic protocols for secure multi-party computation*. PhD thesis, University of Cambridge, 2006. arXiv:0911.3814v2.
9. R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *J. Phys. A - Math. Gen.*, 44:095305, 2011. arXiv:1011.4474v3.
10. I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Proc. CRYPTO*, Springer LNCS, pages 360–378, 2007. arXiv:quant-ph/0612014v2.
11. I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the Bounded-Quantum-Storage Model. In *Proc. IEEE FOCS*, pages 449–458, 2005. arXiv:quant-ph/0508222v2.
12. A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. 2009. arXiv:0912.5514.
13. F. Dupuis. *The Decoupling Approach to Quantum Information Theory*. PhD thesis, Université de Montréal, 2009. arXiv:1004.1641v1.
14. F. Dupuis, M. Berta, J. Wullschleger, and R. Renner. The decoupling theorem. 2010. arXiv:1012.6044v1.
15. S. Dziembowski and U. Maurer. On generating the initial key in the bounded-storage model. In *Proc. EUROCRYPT*, Springer LNCS, pages 126–137, 2004.
16. O. Fawzi, P. Hayden, and P. Sen. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. In *Proc. ACM STOC*, 2011. arXiv:1010.3007v3.
17. D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proc. ACM STOC*, pages 516–525. ACM, 2007.
18. P. Hayden, M. Horodecki, J. Yard, and A. Winter. A decoupling approach to the quantum capacity. *Open. Syst. Inf. Dyn.*, 15:7–19, 2008. arXiv:quant-ph/0702005v1.
19. R. Impagliazzo, L.A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proc. ACM STOC*, pages 12–24. ACM, 1989.
20. J. Kilian. Founding cryptography on oblivious transfer. In *Proc. ACM STOC*, pages 20–31, 1988.
21. R. König, U. Maurer, and R. Renner. On the power of quantum memory. *IEEE Trans. Inform. Theory*, 51:2391–2401, 2005. arXiv:quant-ph/0305154v3.
22. R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55:4674–4681, 2009. arXiv:0807.1338v1.
23. R. König and B. M. Terhal. The bounded-storage model in the presence of a quantum adversary. *IEEE Trans. Inform. Theory*, 54:749–762, 2008.
24. R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Trans. Inform. Theory*, 58(3):1962 –1984, march 2012. arXiv:0906.1030v3.

25. H-K. Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154, 1997.
26. H-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410, 1997.
27. H. Maassen and J. Uffink. Generalised entropic uncertainty relations. *Phys. Rev. Lett.*, 60:1103–1106, 1988.
28. P. Mandayam and S. Wehner. Achieving the physical limits of the bounded-storage model. *Phys. Rev. A*, 83:022329, 2011. arXiv:1009.1596v2.
29. U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *J. Cryptol.*, 5:53–66, 1992.
30. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, 1997.
31. S. Pironio, A. Acin, S. Massar, A.B. de la Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, and L. Luo. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010. arXiv:0911.3427v3.
32. J. Radhakrishnan and A. Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J. Discrete Math.*, 13:2, 2000.
33. J. M. Renes and J.-C. Boileau. Conjectured strong complementary information tradeoff. *Phys. Rev. Lett.*, 103:020402, 2009. arXiv:0806.3984v2.
34. R. Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6:1, 2008. arXiv:quant-ph/0512258v2.
35. R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. *Proc. TCC*, pages 407–425, 2005. arXiv:quant-ph/0403133v2.
36. C. Schaffner, B. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Inf. Comput.*, 9:11, 2008. arXiv:0807.1333v3.
37. R. Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.
38. O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner. Decoupling with unitary almost two-designs. arXiv:1109.4348, 2011.
39. A. Ta-Shma. Short seed extractors against quantum storage. In *Proc. ACM STOC*, pages 401–408. ACM, 2009.
40. M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. *IEEE Trans. Inform. Theory*, 56:4674, 2010. arXiv:0907.5238v2.
41. M. Tomamichel and R. Renner. The uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106:110506, 2011. arXiv:1009.2015v2.
42. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Trans. Inform. Theory*, 57(8):5524 –5535, aug. 2011. arXiv:1002.2436v1.
43. S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A*, 81:052336, 2010. arXiv:0911.2302v2.
44. S. Wehner, C. Schaffner, and B. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, 2008. arXiv:0711.2895v3.
45. S. Wehner and A. Winter. Entropic uncertainty relations - a survey. *New J. Phys.*, 12:025009, 2010. arXiv:0907.3704v1.
46. A. Winter. Quantum information: Coping with uncertainty. *Nat. Phys.*, 6:640, 2010.
47. W.K. Wootters and B.D. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191:363–381, 1989.