Quantum to Classical Randomness Extractors - arXiv:1111.2026v2

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

[1] *Institut für Theoretische Physik, ETH Zürich, 8093 Zürich, Switzerland*
[2] *School of Computer Science, McGill University, Montréal, Québec, Canada*
[3] *Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, 117543 Singapore*

The goal of randomness extraction is to distill (almost) perfect randomness from a weak source of randomness. When the source yields 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. As the first application, 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. As the second application, we 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.

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. Yet, for most applications this is not quite enough, and we want an even stronger statement. In particular, imagine that we hold some side information E about X that increases our guessing probability to $P_{\text{guess}}(X|E)$. In a cryptographic setting, side information can e.g. 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 uncorrelated from E. Recently, it has been recognized that since the underlying world is not classical, E may in fact hold quantum side information about X [2, 3]. That this adds substantial difficulty to the problem was emphasized in [4] 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 [1, 3, 5, 6], eventually culminating in [7, 8], proving that a wide class of classical extractors (with relatively short seed) yield a uniform output, as long as $H_{\min}(X|E) = -\log P_{\text{guess}}(X|E)$ 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 even weak sources to obtain 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 places 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 particular classical string X. 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. 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

[*] Electronic address: berta@phys.ethz.ch
[†] Electronic address: ofawzi@cs.mcgill.ca
[‡] Electronic address: wehner@nus.edu.sg

$\mathrm{Ext}(\cdot, R)$ mapping the outcome of the randomness source to a string K, 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 [18]).

When talking about quantum states ρ_{AE}, what is the relevant measure of how weak or strong a source is? Intuitively, we would 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 [19], and we find that it is indeed the quantity that determines how many classical random bits we can hope to extract from A.

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 we only require the output state to be close to uniform after performing a measurement. 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 [20–25] 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 $\{U_1, \ldots, U_L\}$ to $A = A_1 A_2$ and tracing out (i.e., ignoring) the system A_2. For certain classes of unitaries such as (almost) unitary 2-designs [23, 26–28] the resulting state $\rho_{A_1 E}$ is close to maximally mixed on A_1 and uncorrelated from E, 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. Another example of QQ-extractors are given by protocols that aim to distill entanglement between A and B from a state ρ_{ABE} by means of arbitrary communication between A and B. The resulting output state is uncorrelated from E and maximally mixed on (part of) A. The authors of [32] 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 [18]) impose two important requirements not present in [32, 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.

We give two novel constructions of QC-extractors. The first one involves a full set of mutually unbiased bases (MUBs) and pair-wise independent permutations [18, Theorem III.8]. This construction is more appealing than unitary 2-designs because it is combinatorially much simpler to describe and computationally more efficient, while having the same output size. Our second construction [18, Theorem III.9] 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. Finally, we also prove that the maximum amount of randomness one can hope to extract is roughly $n + H_{\min}(A|E)$, where n denotes the input size [18, Proposition III.6]. 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. 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 (using ideas from [20, 21, 23, 24, 27, 28, 33]). 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.

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. The most well-known relation is for two measurements $\mathcal{M}^1_{A\to K}, \mathcal{M}^2_{A\to K}$ and reads [35]

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

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. 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 [36]. As an illustration, take ρ_{AE} as 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 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 [9, 37–42].

Here 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 (see [18]). 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. For example, for the full set of MUBs we prove that

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

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. 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.

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 [43]. Such problems include e.g., the well-known primitives bit commitment and oblivious transfer [44–48], of which merely very weak variants are possible. 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 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? It was suggested to assume that the attacker's quantum storage was bounded [52, 53], or, more generally, noisy [54–56]. 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 $\mathcal{F}$. 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 $N = \nu \cdot n$. Since its inception [54], 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 [56] where security was linked to the storage device's ability to transmit classical information and shown against fully general attacks. Further progress was made only very recently, linking the security to the so-called entanglement cost of the storage device [57], which lies between its classical and quantum capacities. 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 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 $\nu \cdot \mathcal{Q}(\mathcal{N}) < 1$ and $2 - \log(3) \lesssim \nu \cdot \gamma^{Q}(\mathcal{N}, 1/\nu)$, 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 $R = 1/\nu$ (see [18]). 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 [18]). We prove our result by showing the security of a simple quantum protocol for the cryptographic primitive weak string erasure [56], which is known to be universal for two-party secure computation [56].

[1] R. König and B. M. Terhal, IEEE Transactions on Information Theory **54**, 749 (2008).

[2] R. König, U. Maurer, and R. Renner, IEEE Transactions

on Information Theory **51**, 2391 (2005), arXiv:quant-ph/0305154v3.

[3] R. Renner and R. König, Theory of Cryptography , 407 (2005), arXiv:quant-ph/0403133v2.

[4] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, in *Proceedings of 39th ACM STOC* (ACM, 2007) pp. 516–525.

[5] R. Renner, International Journal of Quantum Information **6**, 1 (2008), arXiv:quant-ph/0512258v2.

[6] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Proceedings of IEEE Symposium on Information Theory , 2703 (2010), arXiv:1002.2436v1.

[7] A. Ta-Shma, in *Proceedings of 41st ACM STOC* (ACM, 2009) pp. 401–408.

[8] A. De, C. Portmann, T. Vidick, and R. Renner, (2009), arXiv:0912.5514.

[9] M. Tomamichel and R. Renner, Physical Review Letters **106**, 110506 (2011), arXiv:1009.2015v2.

[10] E. Hänggi and M. Tomamichel, (2011), arXiv:1108.5349v1.

[11] R. Colbeck, *Quantum and relativistic protocols for secure multi-party computation*, Ph.D. thesis, University of Cambridge (2006), arXiv:0911.3814v2.

[12] S. Pironio, A. Acin, S. Massar, A. de la Giroday, D. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, and L. Luo, Nature **464**, 1021 (2010), arXiv:0911.3427v3.

[13] A. Acin, S. Massar, and S. Pironio, (2011), arXiv:1107.2754v1.

[14] R. Colbeck and A. Kent, Journal of Physics A **44**, 095305 (2011), arXiv:1011.4474v3.

[15] U. Vazirani and T. Vidick, (2011), arXiv:1111.6054v1.

[16] S. Fehr, R. Gelles, and C. Schaffner, (2011), arXiv:1111.6052v2.

[17] S. Pironio and S. Massar, (2011), arXiv:1111.6056v2.

[18] M. Berta, O. Fawzi, and S. Wehner, (2011), arXiv:1111.2026v2.

[19] R. König, R. Renner, and C. Schaffner, IEEE Transactions on Information Theory **55**, 4674 (2009), arXiv:0807.1338v1.

[20] M. Horodecki, J. Oppenheim, and A. Winter, Nature **436**, 673 (2005), arXiv:quant-ph/0505062v1.

[21] M. Horodecki, J. Oppenheim, and A. Winter, Communications in Mathematical Physics **269**, 107 (2006), arXiv:quant-ph/0512247v1.

[22] P. Hayden, M. Horodecki, J. Yard, and A. Winter, Open Systems and Information Dynamics **15**, 7 (2008), arXiv:quant-ph/0702005v1.

[23] F. Dupuis, *The Decoupling Approach to Quantum Information Theory*, Ph.D. thesis, Université de Montréal (2009), arXiv:1004.1641v1.

[24] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, (2010), arXiv:1012.6044v1.

[25] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, Proceedings of Royal Society A **465**, 2537 (2009), arXiv:quant-ph/0606225v1.

[26] P. Hayden and J. Preskill, Journal of High Energy Physics , 0709:102 (2007), arXiv:0708.4025v2.

[27] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, "Decoupling with unitary almost two-designs," (2011), arXiv:1109.4348v1.

[28] O. Szehr, *Decoupling Theorems*, Master's thesis, ETH Zurich (2011).

[29] M. Horodecki, J. Oppenheim, and A. Winter, "Quantum mutual independence," (2009), arXiv:0902.0912.

[30] I. Devetak and A. Winter, IEEE Transaction on Information Theory **50**, 3183 (2004), arXiv:quant-ph/0304196v2.

[31] A. Ambainis, A. Smith, and K. Yang, in *Proceedings of 17th IEEE CCC* (2002) p. 103.

[32] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma, Theory of Computing **6**, 47 (2010).

[33] M. Berta, *Single-shot quantum state merging*, Master's thesis, ETH Zurich (2008), arXiv:0912.4495v1.

[34] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010), arXiv:0907.3704v1.

[35] H. Maassen and J. Uffink, Physical Review Letters **60**, 1103 (1988).

[36] A. Winter, Nature Physics **6**, 640 (2010).

[37] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010), arXiv:0909.0950v4.

[38] J. M. Renes and J.-C. Boileau, Physical Review Letters **103**, 020402 (2009), arXiv:0806.3984v2.

[39] P. J. Coles, L. Yu, and M. Zwolak, (2011), arXiv:1105.4865v2.

[40] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, (2012), arXiv:1112.0543v1.

[41] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Physical Review A **83**, 062338 (2011), arXiv:1006.4859v5.

[42] M. Christandl and A. Winter, IEEE Transactions on Information Theory **51**, 3159 (2005), arXiv:quant-ph/0501090v2.

[43] H.-K. Lo, Physical Review A **56**, 1154 (1997).

[44] H.-K. Lo and H. F. Chau, Physical Review Letters **78**, 3410 (1997).

[45] H. Chau and H.-K. Lo, Fortschritte der Physik **46**, 507 (1998), republished in 'Quantum Computing, where do we want to go tomorrow?' edited by S. Braunstein, arXiv:quant-ph/9709053v2.

[46] D. Mayers, Physical Review Letters **78**, 3414 (1997).

[47] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Physical Review Letters **97**, 250501 (2006), arXiv:quant-ph/0609237v2, quant-ph/0609237 .

[48] G. D'Ariano, D. Kretschmann, D. Schlingemann, and R. Werner, "Quantum bit commitment revisited: the possible and the impossible," (2007), arXiv:quant-ph/0605224v2.

[49] U. Maurer, Journal of Cryptology **5**, 53 (1992).

[50] C. Cachin and U. M. Maurer, in *Proceedings of CRYPTO 1997*, Lecture Notes in Computer Science (1997) pp. 292–306.

[51] S. Dziembowski and U. Maurer, in *Proceedings of EUROCRYPT*, Springer Lecture Notes in Computer Science (2004) pp. 126–137.

[52] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Proceedings of 46th IEEE Symposium on Foundations of Computer Science* (2005) pp. 449–458, arXiv:quant-ph/0508222v2.

[53] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Proceedings of CRYPTO 2007*, Springer Lecture Notes in Computer Science (2007) pp. 360–378, arXiv:quant-ph/0612014v2.

[54] S. Wehner, C. Schaffner, and B. Terhal, Physical Review Letters **100**, 220502 (2008), arXiv:0711.2895v3.

[55] C. Schaffner, B. Terhal, and S. Wehner, Quantum Information & Computation **9**, 11 (2008), arXiv:0807.1333v3.

[56] R. König, S. Wehner, and J. Wullschleger, IEEE Trans-

actions on Information Theory - To appear (2009), arXiv:0906.1030v3.

[57] M. Berta, F. Brandao, M. Christandl, and S. Wehner, "Entanglement cost of quantum channels," (2011), arXiv:1108.5357v2.