QUANTUM-PROOF RANDOMNESS EXTRACTORS VIA OPERATOR SPACE THEORY

MARIO BERTA, OMAR FAWZI, AND VOLKHER B. SCHOLZ

Abstract. Randomness extractors are an important building block for classical and quantum cryptography as well as for device independent randomness amplification and expansion. It is known that some constructions are quantum-proof whereas others are provably not [Gavinsky *et al.*, STOC'07]. We argue that the theory of operator spaces offers a natural framework for studying to what extent objects are quantum-proof: we first rephrase the definition of extractors as a bounded norm condition between normed spaces, and then show that the presence of quantum adversaries corresponds to a completely bounded norm condition between operator spaces. Using semidefinite programming (SDP) relaxations of this completely bounded norm, we recover all known classes of quantum-proof extractors as well as derive new ones. Furthermore, we provide a characterization of randomness condensers (which correspond to a generalization of extractors) and their quantum-proof properties in terms of two-player games.

Full Technical Version: arXiv:1409.3563.

Introduction. In cryptographic protocols such as key distribution and randomness expansion, it is often possible to guarantee that an adversary's knowledge about the secret N held by honest players is bounded. The relevant quantity in many settings is the adversary's guessing probability of the secret N given all his knowledge. However, the objective is usually not to create a secret that is only partly private but rather to create a (possibly smaller) secret that is almost perfectly private. The process of transforming a partly private string N into one that is almost uniformly random M from the adversary's point of view is called privacy amplification [2, 1]. In order to perform privacy amplification, we apply to N a function chosen at random from a set of functions $\{f_s\}$ that has the property of being a randomness extractor.

Randomness extractors are by now a standard tool used in many classical and quantum protocols. They are for example an essential ingredient in quantum key distribution and device independent randomness expansion protocols [18, 20]. For such applications, it has been realized [18] that it is crucial to explicitly consider quantum adversaries. It is by no means obvious that a quantum adversary also satisfying the guessing probability constraint on N would not be able to have additional knowledge about the output M.

We refer to extractors that work even in the presence of quantum adversaries as quantum-proof extractors. In general, quantum-proof extractors are poorly understood: we only know that some standard constructions [13, 14, 8] of extractors are quantum-proof and there is one example of an extractor (with quite bad parameters) that is not quantum-proof [9]. It is for example still consistent with our knowledge that all valid extractors are quantum-proof with only a mild (polynomial in the number of output bits) penalty on the error [19, Slide 84]. But it is also possible that there are extractors for which quantum adversaries lead to an exponentially better attack.

We believe that in the same way as communication complexity and multi prover games (Bell inequalities), the setting of randomness extractors provides a beautiful framework for studying the power and limitations of a quantum memory compared to a classical one. For example, in communication complexity one compares the power of quantum states on c qubits versus that of states on c bit for computing a function with distributed inputs. For randomness extractors, we compare the power of quantum-classical states ρ_{QN} satisfying $p_{\text{guess}}(N|Q) \leq p$ versus that of classical states satisfying $p_{\text{guess}}(N|C) \leq p$ in the task of distinguishing the output of a function from the uniform distribution.

In this submission, we argue that the theory of operator spaces, sometimes also called "quantized functional analysis", provides a natural arena for studying this question. Within this framework, we prove new stability statements, i.e. sufficient conditions for extractors to be quantum-proof. Our methods also allow us to recover all previously known results on quantum-proof extractors in a unified way: a natural semidefinite programming (SDP) relaxation of our characterization of quantum-proof extractors subsumes all the known methods. We mention that operator space theory has already

been successfully applied in the context of understanding Bell inequality violations; see [12, 11] and references therein. In fact, we even make this connection explicit by constructing for each condenser a two-player game whose ratio of the classical vs. the entangled value characterizes the stability properties of the condenser.

Extractors. As already mentioned, randomness extractors map a weakly random system into (almost) uniform random bits, with the help of perfectly random bits called the seed. We use $N = 2^n$ to denote the input system, $M = 2^m$ to denote the output system, and $D = 2^d$ to denote the seed system. A (k, ε)-extractor is then a family of functions $\{F_1, \ldots, F_D\}$ with $F_s : N \to M$ satisfying the following property. For any distribution P_N with $H_{\min}(N)_P := -\log p_{\text{guess}}(N)_P \geq k$ (here $p_{\text{guess}}(N)$ denotes the maximal probability of guessing N), we have

$$\frac{1}{D}\sum_{s=1}^{D} \left\| F_s(P_N) - \upsilon_M \right\|_{\ell_1} \leq \varepsilon \ , \tag{1}$$

where υ_M denotes the uniform distribution on M. This definition refers to strong extractors, which correspond to what is needed for many cryptographic applications.

For applications in classical and quantum cryptography (see, e.g., [18, 15]) and for constructing device independent randomness amplification and expansion schemes (see, e.g., [6, 17, 5, 7, 20]) we are interested if extractor constructions also work when the input source is correlated to another (possibly quantum) system Q. That is, we would like that for all quantum-classical input density matrices ρ_{QN} with conditional min-entropy $H_{\min}(N|Q)_\rho := -\log p_{\text{guess}}(N|Q)_\rho \geq k$ (here $p_{\text{guess}}(N|Q)$ denotes the maximal probability of guessing N given Q), we have

$$\frac{1}{D}\sum_{s=1}^{D} \left\| \mathrm{id}_Q \otimes F_s)(\rho_{QN}) - \rho_Q \otimes \upsilon_M \right\|_1 \leq \varepsilon. \tag{2}$$

If we restrict the system Q to be classical, it is simple to see by conditioning on the possible values of Q that this basically reduces to usual extractor condition (1) [14]. However, if Q is quantum, the condition (2) could be much stronger than condition (1). Extractors that satisfy the stronger condition (2) are called quantum-proof.

Norms, completely bounded norms and SDP's. For vectors in $\mathbb{R}^N$, the ℓ_1-norm is the sum of all absolute values of vector entries and the ℓ_∞-norm is the largest absolute value of vector entries. Both norms are useful for studying extractors, as the first norm encodes the normalization constraint (the inputs are probability distributions), while the second is just the exponential of the min-entropy. Linear maps between normed spaces are naturally equipped with norms, defined as the maximum norm of any output, given that the input has norm bounded by 1. Of course, the norms on the input and the output spaces can be different. Rewriting (1) as a condition on norms, we express the extractor condition as a condition on the norm of a linear map $\Delta[\{F_s\}] : \mathbb{R}^N \to \mathbb{R}^{MD}$. We refer to the full version [3] for more details on this.

In order to take into account quantum adversaries in terms of norms, we want to allow for correlations between the input and an arbitrary quantum system Q. The framework of operator spaces axiomatizes such scenarios: an operator space is a normed space equipped with a sequence of norms describing possible correlations to quantum systems. If we now study linear maps between normed spaces, we can naturally consider these maps to be maps between operator spaces by letting them act trivially on the quantum part. Of course, the norm of the linear maps might change, since we now also allow for correlations to the quantum part (at the input as well as at the output). The associated norm, defined as the supremum with respect to quantum systems of any dimension, is called the *completely bounded norm*, or just cb-*norm*. For the setting of extractors, we construct natural operator space structures such that the completely bounded norm of the linear map $\Delta[\{F_s\}]$ captures the property of being quantum-proof.

Theorem. The property of being quantum-proof can be formulated as a condition on a completely bounded norm defined with respect to a suitably chosen operator space.

We derive multiple applications from this finding that are summarized in Table 1. First, we are able to show using Grothendieck's inequality that when the min-entropy k is very close to n, all extractors are approximately quantum-proof. Interestingly, our bound quite tightly matches the known

Strong (k, ε)-extractor	Quantum-proof	with parameters	SDP relaxation
Random functions	?		x
One-bit output	✓ [14, Thm. 1]	$(k + \log(1/\varepsilon), c\sqrt{\varepsilon})$	✓
Small output	✓	$(k + \log(2/\varepsilon), c\sqrt{2^m\,\varepsilon})$	✓
High entropy	✓	$(k + 1, c2^{n-k}\varepsilon)$	✓
Spectral (e.g., two-universal hashing)	✓ [4, Thm. 4]	$(k, c\sqrt{\varepsilon})$	✓
Trevisan based	✓ [8, Thm. 4.6]	$(k + \log(1/\varepsilon), c\sqrt{\varepsilon})$	✓

TABLE 1. Stability results for strong extractors: input $N = 2^n$, output $M = 2^m$, seed $D = 2^d$, min-entropy k, error parameter ε, and c represent possibly different constants. Exact statements can be found in [3]. Note that the SDP relaxation recovers all known cases. References point to where the corresponding properties were shown first.

separation [9] between conditions (1) and (2). As a second application, we show that any extractor with small enough output (say constant or logarithmic in n) is approximately quantum-proof. This last statement is a generalization of a result [14] that shows that extractors with a single bit of output are quantum-proof. We emphasize that these results do not make any use of the structure of the functions F_s and thus hold for any valid extractor construction.

In order to understand our completely bounded norm condition, we study a SDP relaxation of this condition and find that all known stability results (including the new ones that we derive) are actually bounds on this SDP relaxation. In other words, the only known method for proving security against quantum adversaries is via this SDP. Quite surprisingly, we find that for a small set of randomly chosen function the value of this SDP is large with very high probability. This contrasts with the fact that such families of functions are the prototypical example of randomness extractors and define with high probability extractors with optimal parameters (satisfying condition (1)). This can be interpreted in two ways: either random functions are good candidates for a large separation between conditions (1) and (2), or that understanding how random functions behave in the presence of quantum side information requires completely new methods.

Theorem. The completely bounded norm characterizing quantum-proof extractors can be upper bounded by an SDP. For all known quantum-proof extractors, the SDP relaxation is approximately tight.

Condensers, Graphs and Games. Randomness condensers are obtained by weakening the condition on the output: it does not need to be close to the uniform distribution but only close to some distribution with min-entropy k'. When $k' = m$, this is exactly the condition for being a (k, ε)-extractor. The reason such objects are called condensers is that typically we want $k' \approx k$ but $m \ll n$ so that the entropy is condensed to a smaller space. As for extractors, one naturally defines quantum-proof condensers to be secure even in the presence of quantum adversaries.

The framework of normed spaces and operator spaces also allows to analyze to what extent condensers are quantum-proof. The input constraint is the same as in the extractor case, but slightly more work is needed to capture the output constraint. We refer to the full version [3] for a further technical discussion.

Using our characterization in terms of norms, we can show that evaluating the performance of a condenser corresponds to an instance of a well studied combinatorial problem, called bipartite densest subgraph [16]. The connection to graph theory also provides the first step towards our last result. Using techniques of Junge from [10] we can define a two-player game that exactly captures the property of being a (quantum-proof) condenser.

Theorem. To any condenser, we can associate a two-player game such that the classical (resp. entangled) value characterizes the error in the classical (resp. quantum) case.

In summary, we present a unifying approach to study the stability properties of pseudo-random objects against quantum adversaries, recovering all known results and providing new ones.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *Information Theory, IEEE Transactions on*, 41(6):1915–1923, 1995.

[2] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM journal on Computing*, 17(2):210–229, 1988.

[3] M. Berta, O. Fawzi, and V. B. Scholz. Quantum-proof randomness extractors via operator space theory. *Full technical version*, 2014. Available online: http://arxiv.org/abs/1409.3563.

[4] M. Berta, O. Fawzi, V. B. Scholz, and O. Szehr. Variations on classical and quantum extractors. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 1474–1478, 2014. DOI: 10.1109/ISIT.2014.6875078.

[5] F. G. Brandao, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki. Robust device-independent randomness amplification with few devices. 2013. Available online: http://arxiv.org/abs/1310.4544.

[6] K.-M. Chung, Y. Shi, and X. Wu. Physical randomness extractors. 2014. Available online: http://arxiv.org/abs/1402.4797.

[7] M. Coudron and H. Yuen. Infinite randomness expansion and amplification with a constant number of devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 427–436. ACM, 2014. Available online: http://dl.acm.org/citation.cfm?doid=2591796.2591873.

[8] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41:915–940, 2012. DOI: 10.1137/100813683.

[9] 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 *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, STOC '07, pages 516–525. ACM, 2007. DOI: 10.1145/1250790.1250866.

[10] M. Junge. Operator spaces and Araki-Woods factors: a quantum probabilistic approach. *IMRP. International Mathematics Research Papers*, pages Art. ID 76978–87, 2006.

[11] M. Junge and C. Palazuelos. Large violation of Bell inequalities with low entanglement. *Communications in Mathematical Physics*, 306:695–746, 2011. DOI: 10.1007/s00220-011-1296-8.

[12] M. Junge, C. Palazuelos, D. Pérez-García, I. Villanueva, and M. M. Wolf. Unbounded violations of bipartite Bell inequalities via operator space theory. *Communications in Mathematical Physics*, 300:715–739, 2010. DOI: 10.1007/s00220-010-1125-5.

[13] R. Konig, U. Maurer, and R. Renner. On the power of quantum memory. *Information Theory, IEEE Transactions on*, 51(7):2391–2401, 2005. DOI: 10.1109/TIT.2005.850087.

[14] R. Konig and B. Terhal. The bounded-storage model in the presence of a quantum adversary. *Information Theory, IEEE Transactions on*, 54:749–762, 2008. DOI: 10.1109/TIT.2007.913245.

[15] R. Konig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *Information Theory, IEEE Transactions on*, 58:1962–1984, 2012. DOI: 10.1109/TIT.2011.2177772.

[16] G. Kortsarz and D. Peleg. On choosing a dense subgraph. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 692–701. IEEE, 1993.

[17] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. 2014. Available online: http://arxiv.org/abs/1402.0489.

[18] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 2005. DOI: 10.1142/S0219749908003256.

[19] A. Ta-Shma. Extractors against classical and quantum adversaries. *Tutorial QCrypt*, 2013. Available online: http://2013.qcrypt.net/contributions/Ta-Shma-slides.pptx.

[20] U. Vazirani and T. Vidick. Certifiable quantum dice: Or, true random number generation secure against quantum adversaries. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 61–76, New York, NY, USA, 2012. ACM. DOI: 10.1145/2213977.2213984.

Institute for Quantum Information and Matter, Caltech, Pasadena, CA 91125, USA
E-mail address: berta@caltech.edu

LIP, ENS de Lyon, 69364 Lyon, France
E-mail address: omar.fawzi@ens-lyon.fr

Institute for Theoretical Physics, ETH Zurich, 8093 Zürich, Switzerland
E-mail address: scholz@phys.ethz.ch