Randomness Extraction Beyond the Classical World

Kai-Min Chung
Academia Sinica, Taiwan
kmchung@iis.sinica.edu.tw

Randomness is an extremely useful resource in diverse fields in computer science, such as randomized algorithms, distributed algorithms, and cryptography. In these fields, we often assume that perfect randomness are available. However, the assumption may not be realistic, since random sources available in our physical world tend to be correlated and biased. Furthermore, there is no way to ensure or verify this assumption.

Randomness extraction is a natural approach to bridge the gap, where we extract (almost) perfect randomness from weak random sources and assumptions. In this talk, I will present our recent progress on several randomness extraction approaches (beyond the "classical world").

Quantum-proof Seeded Extractors Classical seeded extractor [11] is the most well-studied notion in the classical world, which extracts perfect randomness from any weak random source with sufficient entropy using a very short *uniform* seed as a catalyst. In the quantum world, the goal is to extract randomness in presence of quantum side information about the classical source. Namely, we require the output to be close to uniform given the quantum side information. This is important for quantum cryptography and also necessary if we believe our world in quantum.

There have been a substantial line of research [9, 13, 14, 10, 16, 6, 5, 1] on the construction of quantum-proof seeded extractors. An important goal here is to minimize the seed length. In the classical setting, we know how to achieve optimal seed length (up to a constant factor) for all ranges of parameters (in particular, for low entropy source and small error). However, this remains elusive in the quantum setting, where the best known constructions have quadratic gap in the dependency on the error parameter.

We make progress on this problem by constructing the first quantum-proof seeded extractor with optimal seed length for a wide range of parameters. Specifically, our extractor achieves optimal seed length $O(\log(n/\epsilon))$ for any n-bit sources with min-entropy $k \geq n^{0.51}$ and error parameter $\epsilon \geq 2^{-k^{0.99}}$, and extracts $k^{0.99}$ almost uniform bits. We obtain our construction by revisiting the early "block-sampling-and-extraction" framework developed in the 90's [11, 15, 17], where we show that the framework can be made quantum-proof, and achieve the above parameters by a new win-win construction.

Quantum-proof Mutli-source Extractors Note that seeded extractors still require a short uniform seed. What if uniform randomness is not available? The notion of multi-source extractors provides a solution to extract randomness from two or more *independent* weak sources. In the quantum world, the situation is more challenging, since quantum side information of different sources may share entanglement, which may break independence of the sources, and introduce non-

classical effects such as non-local correlation and super-dense coding. It is a-prior not clear under what side information model randomness extraction remains feasible.

A natural model to prevent this issue is to restrict the side information to be independent as well. Let us refer to this as the *independent adversary* (IA) model. Interestingly, in the context of two-source extractors, Kasher and Kempe [8] (which is the only prior work we are aware of) also considered an incomparable *bounded storage* (BS) model, where the side information may share entanglement, but has restriction on their sizes. [8] showed that a classical two-source extractor of Dodis et al. [**?**] works in both IA and BS models, but relied on very different techniques.

We significantly improve our knowledge on this subject in several ways. First, we identify a unified side information model for multiple sources that generalizes both IA and BS models. Our model allows entanglement and removes the size restriction. Hence, we refer to it as the *general entanglement* (GE) model. The crux of the GE model is a new way of measuring quantum conditional min-entropy that avoids an *interference* issue in the presence of entangled side information. We next develop several generic techniques to prove GE security (i.e., show that a construction is quantum-proof in the GE model). The key step here is to establish "GE-OA security equivalence" for strong multi-source extractors, where OA (stands for one-sided) is a weak side information model that restricts the side information to depend on a single source. This allows us to reduce proving GE security to proving OA security, which is much easier. Based on our techniques, we are able to show that almost all classical two-source or multi-source extractors are either GE secure, or can be made GE secure with essentially the same parameters.

Physical Randomness Extractors (a.k.a. randomness amplification for arbitrary weak source) Note that independence is crucial for multi-source extractors, but is also an assumption that cannot be verified. What if we are paranoid about making such unverifiable assumption? Does randomness extraction remain feasible without assuming independence?

We observed that device-independent randomness amplification (DI-RA) protocols, introduced by the seminal work of Colbeck and Renner [3], provides a viable approach to this problem, where in addition to a classical random source, the extractor gets (classical) access to several *untrusted* (potentially quantum) devices. [3] constructed the first DI-RA protocol when the weak classical source is a Santha-Vazirani (SV) source with sufficiently small bias. Subsequent works [7, 2, 12] improved the allowed bias and reduced the number of required devices (often additionally assuming certain forms of conditional independence), but only focused on SV sources, which is highly structured and has high entropy.

We view this approach as a *physical randomness extractor* (PRE) that extracts from a "physical system" consisting of devices and a classical source, and explore the feasibility of randomness extraction from arbitrary weak min-entropy source without any structure or independence assumptions. We construct the first such PRE with quantum security that works for any weak sources with even a (sufficiently large) constant bits of min-entropy. Our construction is based on composing quantum-proof seeded extractors and randomness expansion protocols in a modular way. At the core of our security analysis is a security equivalence lemma to analyze the composition, which roughly states that the (quantum) security of any randomness expansion protocols remains to hold even if the seed is revealed to the adversary. Our equivalence lemma has found applications to analyze the security of unbounded randomness expansion [4]. However, the complexity of our protocol (as well as all known DI-RA protocols for SV sources) has inverse polynomial dependency on the error parameter ϵ. Thus, our protocol is only efficient (i.e., runs in polynomial time) when ϵ

is inverse polynomial, which is not suitable for cryptographic applications. Designing efficient PRE with cryptographic security, even for SV sources, remains an intriguing open question.

Finally, we note that the original motivation of [3] is from physics, which is formulated by [7] as a dichotomy theorem asserting that either our physical world is deterministic, or certifiably unpredictable events exist. Such physics interpretation (in its strong form) demands a more stringent notion of *no-signaling* security of the DI-RA protocols. We show the existence of such no-signaling secure PRE for any weak sources. This can be viewed as an optimal form of the dichotomy theorem (that for example, weaken the assumption of the existence of a sequence of weakly unpredictable binary events). Our PRE shares the same structure as above quantum secure version, but the security analysis becomes much more involved. For example, it can be shown that "no-signaling-proof" seeded extractor does not exists. Also, our equivalence lemma relies heavily on quantum structure, so it is not clear how to generalize it to the no-signaling setting. Therefore, we need to develop several new techniques to analyze our construction.

References

[1] A. Ben-Aroya and A. Ta-Shma. Better short-seed quantum-proof extractors. *Theor. Comput. Sci.*, 419:17–25, 2012.

[2] F. G. Brandão, R. Ramanathan, K. H. Andrzej Grudka, M. Horodecki, and P. Horodecki. Robust device-independent randomness amplification with few devices. *QIP 2014*, arXiv:1310.4544.

[3] R. Colbeck and R. Renner. Free randomness can be amplified. *Nature Physics*, 8:450–453, 2012.

[4] M. Coudron and H. Yuen. Infinite randomness expansion with a constant number of devices. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 427–436, 2014.

[5] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.*, 41(4):915–940, 2012.

[6] A. De and T. Vidick. Near-optimal extractors against quantum storage. In *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 161–170, 2010.

[7] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín. Full randomness from arbitrarily deterministic events. *Nature communications*, 4, 2013.

[8] R. Kasher and J. Kempe. Two-source extractors secure against quantum adversaries. *Theory of Computing*, 8(1):461–486, 2012.

[9] R. König, U. M. Maurer, and R. Renner. On the power of quantum memory. *IEEE Transactions on Information Theory*, 51(7):2391–2401, 2005.

[10] R. T. König and B. M. Terhal. The bounded-storage model in the presence of a quantum adversary. *IEEE Transactions on Information Theory*, 54(2):749–762, 2008.

[11] N. Nisan and D. Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.

[12] R. Ramanathan, F. G. Brandão, K. Horodecki, M. Horodecki, P. Horodecki, and H. Wojewódka. Randomness amplification against no-signaling adversaries using two devices. *Arxiv:1504.06313*, April 2015.

[13] R. Renner. Security of quantum key distribution. In *Ausgezeichnete Informatikdissertationen 2005*, pages 125–134, 2005.

[14] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, pages 407–425, 2005.

[15] L. J. Schulman and D. Zuckerman. Asymptotically good codes correcting insertions, deletions and transpositions. *IEEE Transactions on Information Theory*, 45(7):2552–2557, 1999.

[16] A. Ta-Shma. Short seed extractors against quantum storage. *SIAM J. Comput.*, 40(3):664–677, 2011.

[17] D. Zuckerman. Randomness-optimal oblivious sampling. *Random Structures and Algorithms*, 11:345–367, 1997.