Quantum-proof multi-source randomness extractors in the Markov model[*]

(Abstract submitted to QCrypt 2016)

Rotem Arnon-Friedman, Christopher Portmann, and Volkher B. Scholz

Institute for Theoretical Physics, ETH-Zürich, CH-8093, Zürich, Switzerland

Abstract

Randomness extractors, widely used in classical and quantum cryptography as well as in device independent randomness amplification and expansion, are functions which generate almost uniform randomness from weak sources of randomness. In the quantum setting one must take into account the quantum side information held by an adversary which might be used to break the security of the extractor. In the case of seeded extractors the presence of quantum side information has been extensively studied. For multi-source extractors one can easily see that high conditional min-entropy is not sufficient to guarantee security against arbitrary side information, even in the classical case. Hence, the interesting question is under which models of side information multi-source extractors remain secure. In this work we suggest a natural model of side information, which we call the Markov model, and prove that any multi-source extractor remains secure in the presence of quantum side information of this type (albeit with weaker parameters). This improves on previous results in which more restricted models were considered and the security of only some types of extractors was shown.

Motivation

Randomness extractors are of great importance in many applications, ranging from derandomization to device-independent quantum cryptography. The goal of a randomness extractor is to generate (almost) uniform randomness from weak sources of randomness. A weak source is usually modelled as a distribution X over $\{0,1\}^n$ such that the min-entropy of X is lower bounded by k: $H_{\min}(X) \geq k$. That is, the source is defined via a probability distribution for which the probability of any string $x \in \{0,1\}^n$ is at most 2^{-k}. The idea is then to apply a randomness extractor to the weak source, such that the output source Y is indistinguishable from a uniformly random source.

Unfortunately, no deterministic function can extract the randomness from all sources with a given min-entropy, even for sources with high min-entropy [2,3]. The most common ways to avoid this problem are to consider seeded extractors and multi-source extractors. In the case of seeded extractors one uses an additional truly uniform (but short) and independent seed, together with the weak source, as the input to the extractor (see, e.g., [3–5]).

Multi-source randomness extractors are of special importance in applications where a uniform seed is not available (e.g., in quantum randomness amplification protocols). In the multi-source case, instead of starting with one weak source X, one considers several *independent* weak sources $X_1, X_2, \dots, X_l$ for some $l \geq 2$, with $H_{\min}(X_i) \geq k_i$ for $i \in [l]$, as the input to the extractor (see, for example, [6–10]).

In all types of extractors the randomness present in the weak sources must be lower bounded for the extractor to work (i.e., a bound on the min-entropy is given as a promise). However, this randomness inherently depends on the information one has about the weak sources, or to put differently, on the *side information* about the sources. For example, extractors are widely used for privacy amplification in cryptographic tasks. There, the starting point is that an adversary holds some side information E about the source such that the *conditional* min-entropy is bounded: $H_{\min}(X|E) > k$. The extractor is then used to transform X to a key Y, which should be close to uniform even conditioned on the side information E. If the extractor fulfils this requirement it is said to be secure.

[*] Full version [1]: `http://arxiv.org/abs/1510.06743`

For applications in quantum cryptography and information theory one should consider adversaries with quantum side information and ask whether an extractor remains secure even in the presence of such side information. For seeded extractors this question has been extensively studied. In [11] it was shown that all one-bit output extractors remain secure against quantum side information. It is still unknown whether all multi-bit output extractors remain secure, but several constructions of seeded extractors with good parameters were shown to work also in the presence of quantum side information [12–15].

When considering multi-source extractors things get more complicated, even in the classical case. To see this, consider any one-bit output two-source extractor and let the adversary hold as side information the output of the extractor $Y = \mathrm{Ext}\left(X_1, X_2\right)$. As this is just one bit, $H_{\min}\left(X_1|Y\right) \geq k_1 - 1$ and $H_{\min}\left(X_2|Y\right) \geq k_2 - 1$. Furthermore, as the sources are independent even $H_{\min}\left(X_1|YX_2\right)$ and $H_{\min}\left(X_2|YX_1\right)$ remain high. Nevertheless, the extractor fails to produce an output which looks uniform given the side information.

This implies that one cannot expect to have multi-source extractors which are secure against any classical or quantum side information and thus raises the question: *under which assumptions on the structure of the sources and the side information $X_1 \cdots X_l E$ do multi-source extractors remain secure even in the presence of E?* The main objective of this work is to answer this question. In particular, we define a natural condition on the sources and the side information for which *all* multi-source extractors remain secure in the presence of both classical and quantum side information, but with an increase in the error of the extractor—the distance from uniform of the output.

Related work. [16] initiated the study of multi-source extractors in the presence of side information. They considered the case of two sources and an unentangled quantum adversary. More specifically, given the two independent sources X_1 and X_2, an unentangled adversary can hold side information in a tensor product form $\rho_{C_1} \otimes \rho_{C_2}$ such that $H_{\min}(X_i|C_1C_2) = H_{\min}(X_i|C_i) \geq k_i$. In this way, the side information does not break the independence of the sources[1]. It was proven in [16] that any *one-bit output* two-source extractor remains secure in the presence of unentangled side information. They further show that a specific construction of a multi-bit output two-source extractor, that of [7], is also secure in the considered model, by reducing it to the one-bit case.

Recently, another model for an adversary was considered in [17]. For simplicity, we explain here the model for the case of two sources only. There, the side information of the adversary must be created in the following way: in the beginning the adversary can have any bipartite quantum state $\rho_{E_1E_2}$, independent of the sources. To create her final side information $\rho_{C_1C_2}$, she can correlate her state with the sources by performing an independent "leaking operation" from each source to one of the subsystems. That is, the leaking operation is a map for $i \in \{1, 2\}$, $\Phi_i : \mathrm{L}(X_i \otimes E_i) \to \mathrm{L}(X_i \otimes C_i)$ and the final state $\rho_{X_1X_2C_1C_2}$ can be written as $\rho_{X_1X_2C_1C_2} = \Phi_1 \otimes \Phi_2(\rho_{X_1X_2E_1E_2})$. For the relevant conditions on the min-entropy see [17]. It was proven in [17] that for multi-source extractors which are strong[2] in all but one source, this complex adversarial leaking operation is in fact equivalent to providing the adversary with side information about only one source. They prove that several known extractor constructions are still secure when the adversary holds quantum side information about one of the sources—with an increase in the error of the extractor.

Our contribution – the results and their importance

Our first contribution is a new definition of a quantum-proof multi-source extractor, which is simpler than previous proposals, and simultaneously more general than all known definitions of extractors for which constructions exist. The original classical extractor definition requires the sources to be independent, i.e., in the two-source case one must have $I(X_1 : X_2) = 0$, where $I(\cdot : \cdot)$ denotes the mutual information. If an

[1] [16] also considered another model for the adversary, called the bounded storage model, in which an (unproven) assumption is made on the size of the adversary's storage capacity. In this work we consider only the more general case, where there is no bound on the adversary's memory. For more details see [16].

[2] An extractor is said to be strong in a set of its sources if even conditioned on all the sources in this set the output cannot be distinguished from uniform (see formal definition in [1]).

adversary is present and holds some side information E, we require that the two sources be independent from the point of view of this adversary, i.e., $I(X_1 : X_2|E) = 0$. This definition is valid for both classical and quantum side information E. This means that the sources and the side information should form a *Markov chain* $X_1 \leftrightarrow E \leftrightarrow X_2$. For the case of more than two sources a similar Markov-type condition can be defined and we say that the sources and the side information are in the *Markov model.* The formal definitions are in [1].

Compared to previous definitions of quantum-proof multi-source extractors, this has several advantages. First, it is more general than the previous work of [16], as product side information is a special cases of Markov chains. Moreover, we consider it much more natural to put a requirement on the structure of the global state $\rho_{X_1 X_2 E}$, instead of describing permissible adversarial strategies or leaking models that generate the side information E as in [17]. Finally, Markov chains arise naturally in certain applications.

Our second and main contribution is to prove that *all* extractors (weak and strong) remain secure in this model, both in the classical and quantum case, albeit with weaker parameters. More specifically:

Theorem. *Any $(k_1, \dots, k_l, \varepsilon)$-[strong] l-source extractor is a $\left(k_1 + \log\frac{1}{\varepsilon}, \dots, k_l + \log\frac{1}{\varepsilon}, \sqrt{(l+1)\varepsilon 2^{(m-2)}}\right)$-[strong] quantum-proof l-source extractor in the Markov model, for m the output length of the extractor.*

The formal definitions of the extractors are given in [1]. The important thing to note is that the min-entropy of the sources needs to be just $\log\frac{1}{\varepsilon}$ higher (this is the same in the classical case as well). The error itself is $\sqrt{(l+1)\varepsilon 2^{(m-2)}}$ where l is the number of sources and m is the number of output bits of the considered extractor. This matches exactly the bound proven in [16, Corollary 27] for the restricted case of unentangled side information, $l = 2$, and $m = 1$. We note that this is also an improvement over the constructions in the model of [17], for which the error in [17, Theorem 5.3] for $l = 2$ is of the form $2^m\sqrt{\varepsilon}$, i.e., an order of $\sqrt{2^m}$ worse than ours. In fact, by using our results it is easy to improve the one of [17] and to show that the extractors considered there actually perform better than proven.

Apart from presenting the Markov model and proving the theorem above, we also contribute on the technical level. While both [16, 17] use the techniques of [11] for the one-bit output case and then extend it using a quantum XOR lemma [16], we use a completely different proof technique which is based on the recent work of [18]. The advantage of our technique is that it also applies to weak extractors, whereas the techniques of [17] require the extractors to be strong in order to prove that they are secure.

Identifying under which assumptions on the structure of the sources and the side information held by a quantum adversary multi-source extractors remain secure is especially important for tasks such as device-independent randomness amplification (DIRA), where one does not have a uniform seed to perform extraction. As far as we are aware, all current security proofs for DIRA with constant number of devices either achieve security only against classical adversaries or heavily suffer from other restrictive assumptions due to use of classical multi-source extractors. Hence, our work can serve as a starting point for finding DIRA protocols which can be proven secure against quantum adversaries. (See [1] for more details).

Main ideas of the proof. The first main idea of the proof is that instead of considering classical sources one can consider *multipartite quantum states* from which the sources can be created by local measurements. This local structure is used in the next steps to "enforce" the same local structure on the side information of the adversary (note that while, when studying extractors per-se, it seems a bit weird to transform the classical sources to quantum ones, when considering the applications in quantum cryptography this is pretty natural as the classical sources anyhow emerge from some quantum process that usually has the relevant multipartite structure). Next, we employ ideas from [18] where the security definition of the extractor is rewritten using operators inequalities. Finally, we show that this new security definition can be seen as a specific distinguishing strategy when using classical side information of a specific simple form, and by this reduce the quantum problem to a classical one. That is, security against classical side information implies security against quantum side information in the Markov model.

References

[1] Rotem Arnon-Friedman, Christopher Portmann, and Volkher B Scholz. Quantum-proof multi-source randomness extractors in the markov model. *arXiv preprint arXiv:1510.06743*, 2015.

[2] Miklos Santha and Umesh V Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33(1):75–87, 1986.

[3] Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77(67-95):10, 2002.

[4] Russell Impagliazzo, Leonid A Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 12–24. ACM, 1989.

[5] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.

[6] Umesh V Vazirani. Strong communication complexity or generating quasi-random sequences from two communicating semi-random sources. *Combinatorica*, 7(4):375–392, 1987.

[7] Yevgeniy Dodis, Ariel Elbaz, Roberto Oliveira, and Ran Raz. Improved randomness extraction from two independent sources. In *Approximation, randomization, and combinatorial optimization. Algorithms and techniques*, pages 334–344. Springer, 2004.

[8] Ran Raz. Extractors with weak random seeds. In *Proceedings of the 37th Symposium on Theory of Computing, STOC '05*, pages 11–20. ACM, 2005.

[9] Anup Rao. Extractors for a constant number of polynomially small min-entropy independent sources. *SIAM Journal on Computing*, 39(1):168–194, 2009.

[10] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 22, page 119, 2015.

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

[12] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, pages 407–425. Springer, 2005.

[13] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):915–940, 2012.

[14] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, August 2011. A preleminary version appeared at ISIT 2010.

[15] Masahito Hayashi and Toyohiro Tsurumaru. More efficient privacy amplification with less random seeds via dual universal hash function. *arXiv preprint arXiv:1311.5322*, 2013.

[16] Roy Kasher and Julia Kempe. *Two-source extractors secure against quantum adversaries.* Springer, 2010.

[17] Kai-Min Chung, Xin Li, and Xiaodi Wu. Multi-source randomness extractors against quantum side information, and their applications. *arXiv preprint arXiv:1411.2315*, 2014.

[18] Mario Berta, Omar Fawzi, and Volkher B Scholz. Quantum-proof randomness extractors via operator space theory. *arXiv preprint arXiv:1409.3563*, 2014.