数理解析研究所講究録
第 1744 巻 2011 年 42-47

Trevisan's extractor in the presence of quantum side information

Anindya De[1], Christopher Portmann[2], Thomas Vidick[1], and Renato Renner[3]

[1]Computer Science Division, University of California, Berkeley, CA, USA.
[2]Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, Tokyo, Japan.
[3]Institute for Theoretical Physics, ETH Zurich, Zurich, Switzerland.

Abstract

Randomness extraction involves the processing of purely classical information and is therefore usually studied in the framework of classical probability theory. However, such a classical treatment is generally too restrictive for applications, where side information about the values taken by classical random variables may be represented by the state of a quantum system. This is particularly relevant in the context of cryptography, where an adversary may make use of quantum devices. Here, we show that the well known construction paradigm for extractors proposed by Trevisan is sound in the presence of quantum side information.

We exploit the modularity of this paradigm to give several concrete extractor constructions, which, e.g, extract all the conditional (smooth) min-entropy of the source using a seed of length poly-logarithmic in the input, or only require the seed to be weakly random.

1 Introduction

Randomness extraction is the art of generating (almost) uniform randomness from any weakly random source X. More precisely, a *randomness extractor* (or, simply *extractor*) is a function Ext that takes as input X together with a uniformly distributed (and usually short) string Y, called the *seed*, and outputs a string Z. One then requires Z to be almost uniformly distributed whenever the min-entropy of X is larger than some threshold k, i.e.,

$$H_{\min}(X) \geq k \implies Z := \text{Ext}(X, Y) \text{ statistically close to uniform.} \tag{1}$$

The min-entropy of a random variable X is directly related to the probability of correctly guessing the value of X using an optimal strategy: $2^{-H_{\min}(X)} = \max_x P_X(x)$. Hence Criterion (1) can be interpreted operationally: if the maximum probability of successfully guessing the input of the extractor, X, is sufficiently low then its output is statistically close to uniform.

In most applications, such as privacy amplification [1], or simply when applying two extractors in succession[1] to the same input X, there is a notion of *side information*, which describes the information about the input which is contained in the environment, or accessible to an adversary. Notions of randomness such as the *guessing probability*, *min-entropy* or the *uniformity* of a random variable naturally always depend on the side information relative to which they are

[1] When applying two extractors in succession to the same input, with the goal that the two outputs are jointly uniform, the output of the first extractor needs to be considered as side information when analyzing the second extractor.

defined, and in particular one would like the output of the extractor to be uniform *with respect to the side information.* Hence we may make this requirement explicit in our formulation of Criterion (1) by denoting by E all side information with respect to which the extractor's output should be uniform:

$$H_{\min}(X|E) \geq k \implies Z := \mathrm{Ext}(X,Y) \text{ statistically close to uniform conditioned on } E, \quad (2)$$

where $H_{\min}(X|E)$ is the conditional min-entropy. This conditioning naturally extends the operational interpretation of the min-entropy to scenarios with side information, i.e., $2^{-H_{\min}(X|E)}$ is the maximum probability of correctly guessing X, given access to side information E [2].

Interestingly, the relationship between the two Criteria (1) and (2) depends on the physical nature of the side information E, i.e., whether E is represented by the state of a classical or a quantum system. In the case of purely classical side information, E may be modeled as a random variable and it is known that the two criteria are essentially equivalent. But in the general case where E is a quantum system, Criterion (2) is *strictly stronger* than (1): it was shown in [3] that there exist extractors that fulfill (1) but for which (2) fails (see also [4] for a discussion).

Since our world is inherently non-classical, it is of particular importance that (2) rather than the weaker Criterion (1) be taken as the relevant criterion for the definition of extractors. For example, in the context of cryptography, one typically uses extractors to generate secret keys, i.e., randomness that is uniform from an adversary's point of view. Even if the extractor itself is classical, nothing can prevent an adversary from storing information E in a quantum system, so Criterion (1) does not imply security. Randomness recycling is another simple example involving quantum side information. If we run a (simulation of) a quantum system E using randomness X, approximately $H_{\min}(X|E)$ bits of X can be reused. Applying a function Ext which has been shown to fulfill (1) but not (2) could result in an output Z which is still correlated to the system E.

Moreover, since it is known that the smooth conditional min-entropy precisely characterizes the optimal amount of uniform randomness that can be extracted from X while being independent from E [5], one may argue that Criterion (2) is indeed the correct definition for randomness extraction.

In particular, we would like to point out that the popular bounded storage model — in which the entropy of the source $H_{\min}(X|E)$ is lower-bounded by $H_{\min}(X) - H_0(E)$ and $H_0(E)$ denotes the number of qubits needed to store E — is strictly weaker: there are sources X and nontrivial side information E such that $H_{\min}(X) - H_0(E) \ll H_{\min}(X|E)$,[2] and extractors which are sound for any input with $H_{\min}(X) - H_0(E) \geq k$, but cannot be applied to all sources with $H_{\min}(X|E) \geq k$. An extractor which has only been proven sound in the bounded storage model can thus only extract $H_{\min}(X) - H_0(E)$ bits of uniform randomness instead of the optimal $H^{\varepsilon}_{\min}(X|E)$ bits. For the same reason in the purely classical case, no recent work defines classical extractors for randomness sources with side information stored in bounded classical memories.[3]

[2] This can easily be seen by considering the following example. Let X be uniformly distributed on $\{0,1\}^n$ and E be X with each bit flipped with constant probability $\varepsilon < 1/2$. Then $H_{\min}(X|E) = \Theta(n)$, but $H_{\min}(X) - H_0(E) = 0$.

[3] Restricting the class of randomness sources further than by bounding their min-entropy can have advantages, e.g., if we consider only bit-fixing sources, or sources generated by a random walk on a Markov chain, then the extractor can be deterministic. (See [6] for a brief overview of restricted families of sources studied in the literature.) There is however no known advantage (e.g., in terms of seed length) in considering only input sources with side information stored in memory of bounded size, whether it is classical or quantum memory.

Furthermore, in applications where extractors are used, the increased generality of the conditional min-entropy over the bounded storage model is often what is needed. For example in quantum key distribution, where extractors are used for privacy amplification [5], it is generally impossible to bound the adversary's memory size.

2 Related results

In the standard literature on randomness extraction, constructions of extractors are usually shown to fulfill Criterion (1), for certain values of the threshold k (see [7] as well as [6] for an overview). However, only a few constructions have been shown to fulfill Criterion (2) with arbitrary quantum side information E. Among them is two-universal hashing [5, 8] as well as constructions based on the sample-and-hash approach [4].

Recently, Ta-Shma [9] studied Trevisan's extractor construction [10] in the bounded quantum storage model. Although his proof requires the output length to be much smaller than the min-entropy of the original data, the result was a breakthrough because it, for the first time, implied the existence of "quantum-proof" extractors requiring only short seeds (logarithmic in the input length). More recently, two of the present authors [11] were able to improve the output length that Trevisan's extractor could provably extract in the presence of a quantum bounded-storage adversary, bringing it close to what is known for the case of classical adversaries. However, both these results are proved in the bounded quantum storage model, which, as discussed previously, only allows the extractor to output at most $H_{\min}(X)-H_0(E)$ bits. This expression can in general be arbitrarily smaller than $H_{\min}(X|E)$, and in some cases may even become 0 (or negative) for n-bit sources for which it is possible to extract $\Omega(n)$ bits of randomness.[2]

Subsequent to this work, Ben-Aroya and Ta-Shma [12] showed how two versions of Trevisan's extractor, shown quantum-proof in this paper, can be combined to extract a constant fraction of the min-entropy of an n-bit source with a seed of length $O(\log n)$, when $H_{\min}(X|E) > n/2$. This is better than the straightforward application of Trevisan's extractor analyzed here, which requires $O(\log^2 n)$ bits of seed for the same output size (but works for any $H_{\min}(X|E)$).

3 Our results

In this work, we show that the performance of Trevisan's extractor does not suffer in the presence of quantum side information. More precisely, we show that the output length of the extractor can be close to the optimal conditional min-entropy $H_{\min}(X|E)$. This is the first proof of security of an extractor with poly-logarithmic seed meeting Criterion (2) in the presence of arbitrary quantum side information.

More generally, we prove security of a whole class of extractors. It has been observed, by, e.g., Lu and Vadhan [13, 14], that Trevisan's extractor [10] (and variations of it, such as [15]) is a concatenation of the outputs of a one-bit extractor with different pseudo-random seeds. Since the proof of the extractor property is independent of the type of the underlying one-bit extractor (and to some extent the construction of the pseudo-random seeds), our result is valid for a generic scheme. We find that the performance of this generic scheme in the context of quantum side information is roughly equivalent to the (known) case of purely classical side information.

	Min-entropy	Output length	Seed length	Note
Corollary 5.4	any k	$m = k - 4\log 1/\varepsilon$	$d = O(\log^3 n)$	optimized output length
Corollary 5.6	$k = n^\alpha$	$m = n^{\alpha-\gamma}$	$d = O(\log n)$	optimized seed length
Corollary 5.11	$k = \alpha n$	$m = (\alpha - \gamma)n$	$d = O(\log^2 n)$	local extractor
Corollary 5.14	$k = n^\alpha$	$m = n^{\alpha-\gamma}$	$d = O(\log n)$	seed with min-entropy βd

Table 1: Plugging various weak designs and 1-bit extractors in Trevisan's construction, we obtain these concrete extractors. Here n is the input length, $\varepsilon = \text{poly}(1/n)$ the error, α and γ are arbitrary constants such that $0 < \gamma < \alpha \leq 1$, and $\frac{1}{2} < \beta < 1$ is a specific constant. The corollary numbers refer to the full version [17].

Our argument follows in spirit the work of De and Vidick [11]. Technically, the proof is essentially a concatenation of the two following ideas.

- In the first part of the original proof of Trevisan [10], it is shown that the ability to distinguish the extractor's output from uniform implies the ability to distinguish the output of the underlying one-bit extractor from uniform (a list-decodable code in Trevisan's original scheme). Ta-Shma has argued that this claim is still true in the context of quantum side information [9], by treating the adversary as an oracle and measuring its memory size by counting the queries to the oracle. We extend this result to the case of arbitrary quantum side information, where the entropy of the source is measured with the conditional min-entropy, and show that it still holds even if the seed of the underlying one-bit extractor is not fully uniform.
- This reduces the problem to proving that the one-bit extractor used in the construction is quantum-proof. However, because for one-bit extractors, the more general Criterion (2) is essentially equivalent to the usual Criterion (1), as shown by König and Terhal [16], the claim follows from known classical results on one-bit extractors with only a small loss in the error parameter.

This proof structure results in a very modular extractor construction paradigm, which allows arbitrary one-bit extractors and pseudo-random seeds to be "plugged in," producing different final constructions, optimized for different needs, e.g., maximizing the output length, minimizing the seed, or even using a non-uniform seed if the underlying one-bit extractor also uses a non-uniform seed. In Table 1 we give a brief overview of the final constructions proposed.

For proofs and details, we refer to the complete version of this paper [17].

References

[1] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 41(6):1915–1923, November 1995. [doi:10.1109/18.476316].

[2] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, 2009. [arXiv:0807.1338].

[3] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the 39th symposium on theory of computing, STOC '07*, pages 516–525. ACM, 2007. [doi:10.1145/1250790.1250866, arXiv:quant-ph/0611209].

[4] Robert König and Renato Renner. Sampling of min-entropy relative to quantum knowledge. eprint, 2007. [arXiv:0712.4291].

[5] Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, Swiss Federal Institute of Technology Zurich, September 2005. [arXiv:quant-ph/0512258].

[6] Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the European Association for Theoretical Computer Science*, 77:67–95, June 2002.

[7] David Zuckerman. General weak random sources. In *Proceedings of the 31st symposium on foundations of computer Science, FOCS '90*, pages 534–543. IEEE, 1990. [doi:10.1109/FSCS.1990.89574].

[8] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. In *Proceedings of 2010 international symposium on information theory, ISIT*, pages 2703–2707. IEEE, 2010. [doi:10.1109/ISIT.2010.5513652, arXiv:1002.2436].

[9] Amnon Ta-Shma. Short seed extractors against quantum storage. In *Proceedings of the 41st symposium on theory of computing, STOC '09*, pages 401–408. ACM, 2009. [doi:10.1145/1536414.1536470, arXiv:0808.1994].

[10] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001. [doi:10.1145/502090.502099].

[11] Anindya De and Thomas Vidick. Near-optimal extractors against quantum storage. In *Proceedings of the 42nd symposium on theory of computing, STOC '10*, pages 161–170, 2010. [doi:10.1145/1806689.1806713, arXiv:0911.4680].

[12] Avraham Ben-Aroya and Amnon Ta-Shma. Better short-seed extractors against quantum knowledge. eprint, 2010. [arXiv:1004.3737].

[13] Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology*, 17(1):27–42, 2004. [doi:10.1007/s00145-003-0217-1].

[14] Salil P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, 2004. [doi:10.1007/s00145-003-0237-x].

[15] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. *Journal of Computer and System Sciences*, 65(1):97–128, 2002. [doi:10.1006/jcss.2002.1824].

[16] Robert König and Barbara M. Terhal. The bounded-storage model in the presence of a quantum adversary. *IEEE Transactions on Information Theory*, 54(2):749–762, Feb 2008. [doi:10.1109/TIT.2007.913245, arXiv:quant-ph/0608101].

[17] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. eprint, 2009. [arXiv:0912.5514].