Randomness expansion from untrusted quantum devices

Carl A. Miller, joint work with Yaoyun Shi

Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48109, USA
carlmi,shiyy@umich.edu

Is it possible to obtain provable random numbers from an untrusted source? This question, if it can be answered affirmatively, is of great importance in cryptography, where random numbers are ubiquitous and it is necessary to guard against highly intelligent adversaries. Bad randomness is a problem: researchers have broken a large number of RSA keys on the internet due to insufficient randomness [8, 9].

There are current solutions which generate random numbers from a physical source — possibly in combination with pseudorandom generators — but these solutions require a level of trust in the randomness of the source. NIST Special Publication 800-90B [1], which is commonly used and prescibes methods for testing sources of randomness, says the following:

> *The development of entropy sources that provide unpredictable output is difficult, and providing guidance for their design and validation testing is even more so. The testing approach defined in this Recommendation assumes that the developer understands the behavior of the entropy source and has made a good-faith effort to produce a consistent source of entropy.*

The question is whether random numbers can be generated *even in the absence of good faith*. Quantum technology offers a unique opportunity to address this question: Bell inequality violations are proofs of quantum, and therefore random, behavior. This talk will cover the current results on untrusted-device randomness expansion and give a primer on the tools that we have used in our work [10, 11].

In 2006, Roger Colbeck proposed (without proof) a protocol for randomness expansion from untrusted devices [3, 4]. The scheme involves repeatedly testing the devices with a Bell inequality and, if a violation is achieved on average, using the outputs of the devices to create randomness. We will use a version of such a protocol from [5], [14] which is shown in Figure 1. The protocol includes adjustable parameters: N (an integer) and δ, s, t (positive real numbers).

After Colbeck's thesis, papers appeared on similar protocols [12, 13, 7, 5] showing that the output string at the end of the protocol is indeed nearly uniformly random, but they showed this only against a classical adversary (i.e., an adversary who does not have quantum memory). [14] took a major step forward (continued in [6]) by showing security against a quantum adversary, but their protocol was not robust (i.e., its abort-condition is exact rather than approximate, so an honest-but-noisy device will probably abort). The challenge we addressed in our work is to prove robustness *and* security against a full quantum adversary. This problem led us to some new tools and interesting mathematics.

Proving security for Protocol R comes down to showing that, after step 4 in Protocol R, the collected outputs of the device, which we denote by Y, contains at least tN extractable bits—even

A classical user Alice, possesses a quantum device D consisting of multiple components $D_1, \ldots, D_n$, and also an initial random string X. A nonlocal game G is chosen.

1. Alice simulates a biased $(\delta, 1-\delta)$-coin flip (using X) to produce a bit g.
2. If $g = 0$, then a fixed input sequence a is given to D and the outputs are recorded.
3. If $g = 1$, then the game G is played with D and the outcome ("win" or "lose") is recorded.
4. Steps $1-3$ are repeated $(N-1)$ more times.
5. If the total number of game-wins was less than $s\delta N$, the protocol **aborts**. Otherwise, the protocol **succeeds**, and a classical randomness extractor is applied to the recorded outputs to produce tN bits (the final result).

Figure 1: Protocol R

in the presence of a quantum adversary. How do we measure the number of extractable bits? A canonical measure of randomness of a state ρ is the von Neumann entropy: $S(\rho) = -\mathrm{Tr}[\rho \log \rho]$. We cannot use this measure directly—it is intended for the IID setting and will only guarantee extractable bits in the case where multiple identical copies of the state ρ are available. But consider instead the quantity

$$H_{1+\epsilon}(\rho) \quad = \quad -\frac{1}{\epsilon}\mathrm{Tr}[\rho^{1+\epsilon}], \tag{0.1}$$

which tends to $S(\rho)$, for fixed ρ, as ϵ tends to zero. This is the Renyi entropy of the eigenvalues of ρ. If we can show a lower bound on this quantity, then a lower bound on the number of extractable bits of ρ follows (with a penalty term that increases as $\epsilon \to 0$).

One of the central insights of our work is that randomness can be proved via certain known properties of the operator function $M \mapsto \mathrm{Tr}[M^{1+\epsilon}]$ — or equivalently, properties of its close cousin, the Schatten norm:

$$\|M\|_{1+\epsilon} \quad = \quad \left(\mathrm{Tr}[M^{1+\epsilon}]\right)^{\frac{1}{1+\epsilon}}. \tag{0.2}$$

Using an older result [2] about the geometry of $\|\cdot\|_{1+\epsilon}$, we prove the following, which compares the state-disturbance caused by a measurement to the amount of randomness produced by the measurement.

Proposition 1. *Let ρ be the initial state of D, and let $\{R_0, \ldots, R_n\}$ be the measurement performed for input a (which we assume to be projective) and let $\rho' = \sum_i R_i \rho R_i$ denote the post-measurement state. Then,*

$$\frac{\|\rho'\|_{1+\epsilon}}{\|\rho\|_{1+\epsilon}} \quad \leq \quad 1 - \frac{\epsilon}{2n} \cdot \frac{\|\rho' - \rho\|_{1+\epsilon}}{\|\rho\|_{1+\epsilon}} + O_n(\epsilon^2). \tag{0.3}$$

We can interpret this proposition by saying that there are two possibilities: either ρ was close to the post-measurement state ρ' to begin with, which means that the device approximates a device that yields classically-predictable outputs on input a, or there is a positive lower bound on the amount of randomness that was produced by the measurement $\rho \mapsto \rho'$.

This proposition can be used as a basis for security results. Let us say that a continuous increasing real-valued function f is a *rate curve* for the game G if any values s, t satisfying $t < f(s)$ make Protocol R secure. In other words, a rate curve lower-bounds the rate of extractable bits produced in Protocol R, as a function of the abort threshhold s. Let W_G denote the supremum of all winning-probabilities for G among quantum devices, and let $W_{G,a}$ denote the supremum just among those that give deterministic outputs on input a. Our main results can be summarized as follows.

Theorem 1. *Let G be a nonlocal game. Then:*

1. *There exists a rate curve $f_G\colon [0,1] \to \mathbb{R}$ for G such that $f(s) > 0$ for any $s > W_{G,a}$.*
2. *If G belongs to the class of **binary XOR games that are strong self-tests**, then there exists a rate curve $f'_G\colon [0,1] \to \mathbb{R}$ which satisfies $f(W_G) = 1$.*

Assertion 1 in the theorem applies to any nonlocal game G. Clearly Protocol R becomes insecure for any abort threshhold below $W_{G,a}$, so the condition on the positive values of f_G is in fact the best possible. Assertion 2 applies to a specific class of games which includes the CHSH game and the GHZ game (see [11]) and asserts that there is a rate curve that tends to 1 as s tends to the optimal score.

Both results are proved using an extensive inductive argument—roughly speaking, we show that the $(1+\epsilon)$-Schatten norm of the state of the device D taken together with the outputs decreases exponentially with N, and this implies a lower bound on the number extractable bits produced at step 4.

Let us consider what these assertions imply in the case of the CHSH game, shown in Figure 2. An elementary proof shows that $W_{CHSH,00}$ is equal to 0.75, while the optimal quantum score for CHSH is $\frac{1}{2} + \frac{\sqrt{2}}{4} = 0.853\ldots$. Our result implies that any score threshhold s between these two quantities yields secure randomness expansion — a noise tolerance of 10.3%! Meanwhile, if s approaches $\frac{1}{2} + \frac{\sqrt{2}}{4}$ then the bit-rate t can approach 1.

We note that by choosing δ to be appropriately small with respect to N, we can execute Protocol R with only a polylogarithmic seed—thus, it exponentially expands the seed.

	$O_1 \oplus O_2 = 0$	$O_1 \oplus O_2 = 1$
$I_1 I_2 = 00$	win	lose
$I_1 I_2 = 01$	win	lose
$I_1 I_2 = 10$	win	lose
$I_1 I_2 = 11$	lose	win

Figure 2: The two-player CHSH game. (I_1, I_2 = inputs, O_1, O_2 = outputs.)

Summing up, it is possible to produce true randomness from a device that is both significantly noisy *and* untrusted, and the only assumption is non-communication. Even a computationally all-powerful adversary with quantum memory cannot break the security. This approach provides a compelling alternative to the existing solutions for random number generation.

It would be interesting to explore whether and how the techniques above can be applied to other cryptographic tasks — they can already be applied, for example, to untrusted-device QKD [11]. We are also interested in refining the simple model used above (i.e., where each component is a single black box, and noise is measured by only one quantity) to a more realistic model, which could yield a theory more directly amenable to experiment.

References

[1] Recommendation for the entropy sources used for random bit generation, August 2012. NIST Special Publication 800-90B.

[2] K. Ball, E. Carlen, and E. Lieb. Sharp uniform convexity and smoothness inequalities for trace norms. *Inventiones mathematicae*, 115:463–482, 1994.

[3] R. Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2006.

[4] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[5] M. Coudron, T. Vidick, and H. Yuen. Robust randomness amplifiers: Upper and lower bounds. In P. Raghavendra, S. Raskhodnikova, K. Jansen, and J. D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, volume 8096 of *Lecture Notes in Computer Science*, pages 468–483. Springer, 2013.

[6] M. Coudron and H. Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 427–436, 2014.

[7] S. Fehr, R. Gelles, and C. Schaffner. Security and composability of randomness expansion from Bell inequalities. *Phys. Rev. A*, 87:012335, Jan 2013.

[8] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Security Symposium*, 2012.

[9] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter. Ron was wrong, Whit is right. *IACR Cryptology ePrint Archive*, 2012:64, 2012.

[10] C. A. Miller and Y. Shi. General security for randomness expansion. arXiv:1411.6608.

[11] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. arXiv:1402.0489.

[12] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010.

[13] S. Pironio and S. Massar. Security of practical private randomness generation. *Phys. Rev. A*, 87:012336, Jan 2013.

[14] U. V. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In H. J. Karloff and T. Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 61–76. ACM, 2012.