# Universal security for randomness expansion

Carl A. Miller and Yaoyun Shi

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

Full version: arXiv:1411.6608

**Abstract**

We show that any spatially separated multi-part quantum device demonstrating nonlocality can be used in an untrusted-device protocol for randomness expansion with unconditional quantum security. A consequence is that the noise tolerance for secure randomness expansion only needs to be small enough that it rules out deterministic behavior of the device. This greatly reduces the requirement on implementation precision. For example, for the CHSH game, the noise can be 10.3%, compared with 1.5% in the previous bound. We also show that similar results hold with nonlocality replaced by the broader concept of contextuality, and the spatial separation requirement replaced by the broader compatibility requirement. This is the first full quantum security proof for contextuality-based randomness expansion.

For both nonlocality and contextuality, we have identified the minimum device requirement. Our results imply in particular the equivalence of quantum security with classical security for the protocols considered. Our main technical contribution is a strong Schatten-norm uncertainty principle which applies to arbitrary pairs of noncommuting binary measurements.

# 1 Motivation

Randomness is indispensable for modern day information processing. It captures the essence of secrecy. This is because a message being secretive means precisely that it is random to the adversary. It also drives randomized algorithms (such as physics simulation), besides many other applications. However most practical random number generators (RNG) are heuristics without theoretical guarantees. There are known vulnerabilities in the methods currently in use [9].

More recently, RNGs based on quantum measurements have emerged in the market. While a (close to) perfect implementation of certain measurements can theoretically guarantee randomness, current technology is still far from reaching that precision. This raises a serious question: would the implementation imperfections open the door to adversary attacks? An additional concern is, even if in the future when the implementation technology is satisfactory, could there be "backdoors" in the generator inserted by a malicious party? It is difficult for the user, as a classical being, to directly verify the inner-working of the quantum device.

Those considerations motivated the study of untrusted-device quantum protocols, which are deterministic procedures interacting with (necessarily) multiple "untrusted" quantum devices. The user makes no prior assumptions about inner-workings of the devices. In particular, the devices may be entangled among themselves, or even with the external adversary. This protocol includes a certification procedure which decides whether the outputs should be "accepted" or "rejected." Ideally, two types of errors should be minimized. The "completeness error" is the chance of rejecting an honest implementation (that is, a correct implementation with a possible limited amount of noise, or device deficiency), and the "soundness error" is the chance of accepting when the generated output is not uniformly random.

An untrusted-device protocol necessarily needs a classical input $X$ to begin with that is not fully known to the adversary-device system. In this paper we assume that $X$ is a small uniformly random seed, and our goal is to expand it into a much longer output which is also (nearly) uniformly random. This is *randomness expansion* (or "seeded" extraction in the terminology of [3]).

In his Ph.D. thesis [4], Colbeck formulated the problem of randomness expansion and proposed protocols based on quantum non-local games. New protocols and security analyses followed. Several authors proved classical security only [13, 8, 14, 5]. Vazirani and Vidick [16] was the first to prove full quantum security. Their protocol is also exponentially expanding using just two non-communicating devices. In [12], the present authors developed a different approach for the security analysis, and proved quantum security together with several new desirable properties including robustness (i.e., the honest implementation being imperfect), cryptographic security, and unit size quantum memory requirement for each device.

In [12] and in the current paper, we work with the "spot-checking protocol" developed in [16] and [5]. Informally, the protocol proceeds as follows: an $n$-player nonlocal game $G$ is chosen, and a specific $n$-letter input string $(a_1, \ldots, a_n)$ from the game is selected. We suppose the existence of an untrusted $n$-part quantum device $D$. At each round of the protocol, the user choses a bit $g \in \{0, 1\}$ according to a biased $(1 - q, q)$ distribution (with $q > 0$ small). If $g = 1$ ("game round"), she plays the game with $D$; if $g = 0$ ("generation round") she merely gives the input string $\mathbf{a} = (a_1, \ldots, a_n)$ to $D$. At the end of the protocol, the total number of wins during game rounds is computed, and if it is above a certain threshold ("acceptance threshold"), the user accepts the results and applies a randomness extractor to the outputs of $D$ to produce the final outputs of the protocol. (In the full version we refer to this as "Protocol R.")

In the current work, we ask the following:

**Question:** What is the minimum requirement for a device to guarantee quantum security in an untrusted-device randomness expansion protocol?

Our goal is to identify the essential features that guarantee full security. This leads to several more specific questions.

*What is the broadest class of devices that can be used securely? In particular, is entanglement necessary?* The analysis in [12] only applies to devices that perform well at a specific class of games (binary XOR games). Beyond enlarging this class, there have been proposals and experiments for randomness expansion using the notion of *contextuality* without non-local games [10, 1, 15, 6]. No full quantum-security proof for those contextuality-based protocols is known.

*What is the largest amount of noise tolerable?* The answer to this question is important for the implementation. The analysis in [12] requires that the noise be a sufficiently small constant. For example, for the well-known CHSH game, the level of noise with quantum-security guarantee implied by [12] is $\sim$ 1.5%, which is still challenging for experimental implemention and is far smaller than the full classical-quantum gap, which is $\cos^2 \frac{\pi}{8} - \frac{3}{4} \approx 10.3\%$.

*Are there protocols that are classically secure but not quantum-secure?* If only *classical* security (i.e., security against an adversary who does not have quantum memory) is required, then the noise tolerance and class of games are already well understood [5]. This raises the question of whether there could be protocols that are classically secure but not quantum secure. Indeed, there are classical-quantum states $(A, E)$ such that $A$ and $E$ are highly correlated, but to a "classical" adversary (i.e., one who is forced to make a measurement on $E$ before using it to eavesdrop on $A$) the two systems appear almost independent (see, e.g., [7]). Could such systems occur as outputs in randomness expansion?

## 2 Our contributions

The result of this paper answers each of the questions above. We use the notion of a **contextuality game**, which is a generalization of nonlocal games broad enough to encompass all Kochen-Specker inequalities. For any contextuality game $G$, and chosen input $\mathbf{a}$, denote by $\mathfrak{w}_G^*$ the optimal quantum winning probability. Let $\mathfrak{w}_G^{\mathbf{a}}$ denote the optimal winning probability among all quantum strategies that produce *deterministic output on input* $\mathbf{a}$. Refer to $\delta_G^{\mathbf{a}} := \mathfrak{w}_G^* - \mathfrak{w}_G^{\mathbf{a}}$ as the quantum-deterministic gap of $G$ on $\mathbf{a}$. We define Protocol K, an analogue of Protocol R for contextuality games. We prove the following.

**Theorem 2.1** (Main Theorem; Informal)**.** *Let $(G, \mathbf{a})$ be a contextuality game with selected input. Let $u$ (the **acceptance threshhold**) be a real number between $\mathfrak{w}_G^{\mathbf{a}}$ and $\mathfrak{w}_G^*$. Then, when Protocol K is executed (with $G, \mathbf{a}, u$ as parameters), it produces (asymptotically) at least $f(u)N$ quantum-proof extractable bits in $N$ rounds, where*

$$f(u) \quad = \quad 2(\log e)(u - \mathfrak{w}_G^{\mathbf{a}})^2. \tag{2.1}$$

The same result holds for Protocol R and nonlocal games.

The crucial aspect of this theorem is that the function $f$ is nonzero over the whole interval $(\mathfrak{w}_G^{\mathbf{a}}, \mathfrak{w}_G^*)$. Therefore quantum security is achieved whenever the acceptance threshhold $u$ lies in this interval. Of course, any acceptance threshold less than $\mathfrak{w}_G^{\mathbf{a}}$ cannot guarantee security, since the device could give deterministic outputs during all generation rounds. So the range of security threshholds $(\mathfrak{w}_G^{\mathbf{a}}, \mathfrak{w}_G^*)$ cannot be made larger. One can show that any super-classical device for a game $G'$ can be used for playing a restricted game $G$ with a positive quantum-deterministic gap on some input. Thus being super-classical is the minimum device requirement.

Answers to the other questions also follow. The largest allowable noise tolerance is the quantum-deterministic gap $\delta_G$, and the class of contextuality games that are usable are precisely those for which $\delta_G > 0$. Classical security *is* equivalent to quantum security for spot-checking protocols. (The number of quantum-proof extractable bits is at least linearly related to the number of classically-proof bits.) Entanglement is not necessary for randomness expansion, provided that contextuality can be used as a basis for security.

We note that in the context of binary XOR games, Theorem 2.1 is complementary (neither stronger nor weaker) to Corollary I.3 from [12]. The rate curve (2.1) in Theorem 2.1 is nonzero over a larger interval, but the rate curve in Corollary I.3 approaches a rate of 1 as the acceptance threshhold approaches $\mathfrak{w}_G^*$ (which is not true of (2.1)). It is an open problem to determine the optimal rate curves for Protocol R and Protocol K.

**Outline and proof techniques.** We summarize the new ingredients in this paper. The main technical contribution of this paper is a new universal uncertainty principle for the Schatten norm $\|\cdot\|_{1+\epsilon}$. Once introduced into the framework of [12] (in place of the old uncertainty principle, Theorem E.2), the new principle implies the strong security claims above.

Let $H$ be a quantum system in state $\tau$, and let $\{\tau_0, \tau_1\}$ and $\{\tau_+, \tau_-\}$ be states of $H$ arising from anticommuting measurements on $H$. Suppose for simplicity that $\|\tau\|_{1+\epsilon} = 1$. Then, we prove the following.

$$\left\| \begin{bmatrix} \tau_0 & \\ & \tau_1 \end{bmatrix} \right\|_{1+\epsilon} \leq 1 - \frac{\epsilon}{2} \left(1 - 2 \left\|\tau_-\right\|_{1+\epsilon}\right)^2 + O(\epsilon^2). \tag{2.2}$$

The critical aspect of this inequality is that the function on the right hand side (which determines the rate curve (2.1) is bounded below 1 as long as $\|\tau_-\|_{1+\epsilon}$ is bounded away from $1/2$. The basis for this assertion is the *uniform convexity* of the Schatten norm [2]. Specifically, we exploit the uniform convexity of the function

$$g(t) = \left\| \begin{bmatrix} \tau_0 & tX \\ tX^* & \tau_1 \end{bmatrix} \right\|_{1+\epsilon} \tag{2.3}$$

where $\tau = \begin{bmatrix} \tau_0 & X \\ X^* & \tau_1 \end{bmatrix}$, and use the fact that $\|X\|_{1+\epsilon}$ approximately exceeds $(1 - 2\|\tau_-\|_{1+\epsilon})$.

Having proved (2.2), the next step is to generalize the class of measurements that can be used. In [12] we focused just on measurements that are *partially trusted* (i.e., partially anti-commuting), but this too can be extended. A quantity that is used in other uncertainty principles (e.g. [11]) to measure the non-commutativity of a pair of POVMs $\{A_0, A_1\}, \{A_2, A_3\}$ is the following:

$$d = \max_{\substack{i \in \{0,1\} \\ j \in \{2,3\}}} \left\| \sqrt{A_i} \sqrt{A_j} \right\|^2 \tag{2.4}$$

The use of this term is the crucial step for closing the quantum-classical gap. We prove a version of (2.2) which incorporates $d$.

We state a new protocol (Protocol U) which phrases randomness expansion with minimal assumptions: we need only a device $D$ which has one of two measurement settings at each round ($\{A_0^{(n)}, A_1^{(n)}\}$ or $\{A_2^{(n)}, A_3^{(n)}\}$) such that the commutativity parameters (2.4) have a uniform upper bound. The uncertainty principle (2.2) implies security for Protocol U, which specializes to provide the proof of security for Protocol K.

Our proof (like that of [12]) suggests a deep relationship between quantum security and the geometry of the Schatten norm. This is an avenue that would be good for further exploration.

## References


[1] A. Abbott, C. Calude, J. Conder, and K. Svozil. Strong kochen-specker theorem and incomputability of quantum randomness. *Physical Review A*, 86(062109), 2012.

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

[3] K.-M. Chung, X. Wu, and Y. Shi. Physical randomness extractors. arXiv:1402.4797, 2014.

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

[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] D. Deng, C. Zu, X. Chang, P. Hou, H. Yang, Y. Wang, and L. Duan. Exploring quantum contextuality to generate true random numbers, 2013. arXiv:1301.5364v2.

[7] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal. Locking classical correlations in quantum states. *Physical Review Letters*, 92(067902), 2004.

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

[9] 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.

[10] K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, M. Pawlowski, and M. Bourennane. Contextuality offers device-independent security, 2010. arXiv:1006.0468v1.

[11] M. Krishna and K. Parathasarathy. An entropic uncertainty principle for quantum measurements. *Sankhya: The Indian Journal of Statistics, Series A*, 64:842–851, 2002.

[12] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, 2014. arXiv:1402.0489v2.

[13] 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.

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

[15] M. Um, X. Zhang, J. Zhang, Y. Wang, S. Yangchao, D.-L. Deng, L.-M. Duan, and K. Kim. Experimental certification of random numbers via quantum contextuality. *Scientific Reports*, page 1627, Apr 2013.

[16] 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.