Randomness in nonlocal games between mistrustful players

Carl A. Miller and Yaoyun Shi*

Source paper: *Forcing classical behavior for quantum players* by C. Miller and Y. Shi (2016), attached.

One of the most central and counterintuitive aspects of quantum information theory is the ability for quantum players to outperform classical players at nonlocal games. There are multiplayer games for which an expected score can be achieved by quantum players that is higher than that which can be achieved by any classical or deterministic player (see [1] for a survey of this phenomenon). A useful corollary of this fact is that the quantum players that achieve such scores are achieving *certified* randomness. Their expected score alone is enough to guarantee that their outputs could not have been predictable to any external adversary. This is the basis for device-independent randomness expansion [3, 14, 4, 18, 15, 9, 6, 7, 12, 13]. When two players play a game repeatedly and exhibit an average score above a certain threshhold, their outputs must be highly random and can be postprocessed into uniformly random bits. The final bits are uniform even when conditioned on the input bits used for the game.

In this work we consider another question about randomness: does a high score at a nonlocal game imply that one player's output is random to the other player? For example, suppose that Alice and Bob play the CHSH game, where each is given randomly chosen input bits a and b, respectively, and the score awarded is 1 if their outputs $x, y \in \{0, 1\}$ satisfy $x \oplus y = a \wedge b$, and 0 otherwise. Suppose that after the game is played, Bob is given Alice's input bit a and asked to produce her output bit. Will he be able to do this successfully? Such a question is important for what we call *blind randomness expansion*, which is randomness expansion in a mutually mistrustful scenario: suppose that Bob is Alice's adversary, and Alice wishes to perform randomness expansion by interacting with him, while maintaining the security of her bits against him.

Aside from the desire to minimize trust assumptions in cryptography, blind randomness expansion is motivated by a resource problem: what is the least number of devices needed to achieve unbounded randomness expansion? The best proved answer is four [12, 2], but a blind randomness expansion protocol could be used to reduce the number to three. Proving security of blind randomness appears challenging from the perspective of known techniques. A satisfactory solution may lead to new insights on the nature of certifiable randomness and nonlocal games.

In this work we prove the following: if Bob can guess Alice's output after the game is played, then Alice's and Bob's expected score is no more than the classical threshhold. In fact we prove something stronger: in such a case, Alice's and Bob's strategy (i.e., their state and measurements) is equivalent to one in which a third party could perfectly guess Alice's output given her input. This result may be a good first step towards a security proof for blind randomness expansion (just as one-shot results were a step towards the security proof of ordinary randomness expansion — see, e.g., Appendix C in [3]).

*Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA.

Results. The central difficulty in the blind randomness expansion scenario is that, after the game is played, Bob has post-measurement states which he can try to use to guess Alice's output. Consider a two-player complete-support[1] game G with input alphabets $\mathcal{A}$ and $\mathcal{B}$ and output alphabets $\mathcal{X}$ and $\mathcal{Y}$. Suppose that the game is played by Alice and Bob, who use a strategy that involves making measurements on a bipartite (possibly entangled) system DE. Let β_{ab}^{xy} denote the unnormalized post-measurement states of Bob's system E. If Bob can perfectly guess Alice's output, that means that for any $a \in \mathcal{A}$, $b \in \mathcal{B}$, and $\mathcal{Y}$, the states $\{\beta_{ab}^{xy} \mid x \in \mathcal{X}\}$ are perfectly distinguishable (i.e., they have mutually orthogonal supports). What can be deduced from this condition?

We define a notion of *congruence* between quantum strategies, which is derived from quantum self-testing. Two strategies are congruent if they are related by expanding or shrinking the underlying systems D and E (without changing the state or the measurements) or if they are related by adding or dropping unmeasured ancillary systems. We show that if Bob can predict Alice's output perfectly, then their strategy is equivalent to one in which Bob's system has two separate parts ($E = E_1 \otimes E_2$), one of which is used to produce his output and the other of which is used to guess Alice's output. If the system E_2 is given to a third party, he can then use it to guess Alice's output given her input. Thus this theorem shows an equivalence between third-party guessing and second-party guessing (see Figure 1).

This equivalence is proved by first showing that Bob must be able to guess Alice's outputs using measurement that commute with the measurements he uses to produce his own output. We then apply the known fact (see [16]) that commutativity implies bipartitness for measurements on a finite-dimensional Hilbert space.

Figure 1: Left: Bob is given his input b and produces his output y, and is then given Alice's input a and produces a guess x' at her output. Right: Bob produces his output y while a separate party tries to guess Alice's output.

We also prove (Proposition 2 in the full paper) that if Alice's and Bob's strategy is such that a third-party can guess Alice's output given her input, then their score at G cannot be above the classical threshhold. (This is a general version of commonly-used results in device-independent quantum cryptography.) The following consequence is our main result.

Theorem 1. Suppose that Alice and Bob use a strategy for the game G such that each set $\{\beta_{ab}^{xy} \mid x \in \mathcal{X}\}$ of Bob's post-measurement states is perfectly distinguishable. Then, Alice's and Bob's original input-output distribution

$$p_{ab}^{xy} \quad := \quad \mathbf{P}(X = x, Y = y \mid A = a, B = b)$$

can be reproduced by a classical strategy.

[1] A game has complete support if all input pairs $(a, b) \in \mathcal{A} \times \mathcal{B}$ occur with nonzero probability.

An interpretation of this result is that requiring Bob to guess Alice's output effectively forces Alice and Bob to exhibit behavior that is classical.

Implications. Our theorem shows a primitive version of blind randomness expansion: If Alice and Bob achieve a superclassical input-output distribution, then Alice achieves at least some randomness against Bob. Our result on splitting Bob's system ($E \hookrightarrow E_1 \otimes E_2$) seems to suggest an equivalence between ordinary randomness expansion (i.e., against a third party) and blind randomness expansion. But the scenario becomes more complicated when we consider the degree of randomness in Alice's output. We discuss this in more detail in the full paper (in the section *Blind randomness expansion*).

For the CHSH game, there is a unique strategy achieving the optimal score ($\frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.853\ldots$). If Alice and Bob are using this strategy, Alice's output bit x is perfectly unpredictable to any third party – that is, the guessing probability to an external observer is $1/2$, even if the observer knows Alice's input. On the other hand, Bob's information is partially correlated to x (even after he executes his strategy) and if Bob were given Alice's input he could guess her output with probability $\frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.853\ldots$. Thus Alice's output is less random to Bob than it would be to an outside adversary. This suggests that although the necessary conditions for blind randomness expansion are the same, the rate at which randomness is produced may be different.

The blind randomness scenario appears to be different from ordinary randomness expansion and may require different techniques. A natural next step will be to prove a robust version of Theorem 1. Since our current proof depends on the fact that commutativity implies bipartiteness, it would be natural to consider some version of *approximate* commutativity. This appears to be an intricate topic (see section 4.1 of [5]).

Another aspect of our result is that it contains a notion of *certified erasure* of information. Note that in the optimal CHSH strategy example above, if Bob were asked before his turn to guess Alice's output given her input, he could do this perfectly. (Indeed, this would be the case in any strategy that uses a maximally entangled state and projective measurements.) Contrary to this, when Bob is compelled to carry out his part of the strategy before Alice's input is revealed, he loses the ability to perfectly guess Alice's output. Requiring a superclassical score from Alice and Bob amounts to forcing Bob to erase information. Different variants of certified erasure are a topic of current study [11, 17]. An interesting research avenue is to determine the minimal assumptions under which certified erasure is possible.

We also note that the scenario in which the second player tries to guess the first player's output after computing his own output fits the general framework of *sequential nonlocal correlations* [10], an interesting class that unifies Bell inequalities (constraints on spatially separated measurements) with Leggett-Garg inequalities (constraints on sequential measurements). In [8] such correlations are used for ordinary (non-blind) randomness expansion. Another interesting avenue is to explore sequential nonlocal games more deeply in the context of device-independent cryptography.

References

[1] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys. 86, 419*, 86(419), 2014.

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

[3] R. Colbeck. Quantum and relativistic protocols for secure multi-party computation. Ph. D. thesis, University of Cambridge, arXiv:0911.3814, 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 and T. Vidick. *Automata, Languages, and Programming: 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I*, chapter Interactive Proofs with Approximately Commuting Provers, pages 355–366. Springer Berlin Heidelberg, 2015.

[6] 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.

[7] 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.

[8] F. J. Curchod, M. Johansson, M. J. Hoban, P. Wittek, and A. Acin. Unbounded randomness certification using sequences of measurements. arXiv:1510.03394v1, October 2015.

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

[10] R. Gallego, L. E. Wurflinger, R. Chaves, A. Acin, and M. Navascues. Nonlocality in sequential correlation scenarios. *New Journal of Physics*, 16(033037), 2014.

[11] J. Kaniewski and S. Wehner. Device-independent two-party cryptography secure against sequential attacks. arXiv:1601.06752, January 2016.

[12] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 417–426, 2014.

[13] C. A. Miller and Y. Shi. Universal security for randomness expansion from the spot-checking protocol, 2015. arXiv:1411.6608.

[14] 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.

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

[16] V. B. Scholz and R. F. Werner. Tsirelson's problem. arXiv:0812.4305v1, 2008.

[17] D. Unruh. Revocable quantum timed-release encryption. *J. ACM*, 62(6):49:1–49:76, Dec. 2015.

[18] 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.