Randomness in nonlocal games between mistrustful players

Honghao Fu,[*] Carl A. Miller,[*,†] and Yaoyun Shi[‡]

Technical manuscripts: [1, 2].

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 [3] 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 [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]. 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). After the game is played, does Alice possess any information which is random to Bob, other than her input bit a? Stated differently, if Bob were given Alice's bit a after the game is played, can we prove that it is impossible for him to perfectly guess x?

If we can prove that Bob cannot guess Alice's output bit perfectly, then (a, x) is more random to Bob than a by itself, and we have shown that Bell inequalities also allow the expansion of *local* randomness. Local (rather than global) randomness is a resource in cryptographic scenarios in which two parties are cooperating but do not trust one another.

In the present work we prove a highly general result on the existence of local randomness, and also give an application (certified deletion from untrusted devices).

Quantifying local randomness. We prove the following (see Theorem 14 in [1]). Let $\omega_c(G)$ denote the optimal classical score for a game G.

Theorem 1.1. *Let G be a nonlocal game which has complete support (i.e., each input pair (a, b) occurs with nonzero probability). Suppose that Alice and Bob achieve an expected score of $\omega_c(G) + \epsilon$ at the game G. Then, after the game is concluded, Bob cannot recover Alice's output (given her input) with probability greater than $1 - \epsilon^2 / K_G$.*

[*] Joint Center for Quantum Information and Computer Science, 3100 Atlantic Bldg., University of Maryland, College Park, MD 20742, USA

[†] National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899, USA

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

The expression K_G denotes a constant defined by

$$K_G \quad = (9/4)\sum_{ab} \mathbf{P}(a)\mathbf{P}(a \mid b)^{-1}. \tag{1.1}$$

Global randomness (i.e., randomness in the outputs xy which vanishes when conditioning on either Alice's or Bob's information) is useful for cooperative tasks such as QKD, while local randomness is useful for tasks that do not involve full mutual trust (see., e.g., [16]). This result shows that these complementary resources must occur together.

There has been other work showing upper bounds on the probability that a third party can guess Alice's output after a game (e.g., [17], [18], [19]) and single-round games have appeared where Bob is sometimes given *only* Alice's input, and asked to produce her output (e.g., [20], [21], [22]). We believe the novelty of our scenario in comparison to these papers is that we consider the randomness of Alice's output after Bob has performed his part of a quantum strategy, and thus has potentially lost information due to measurement. The proof of Theorem 1.1 proceeds by supposing that Alice's outputs are highly predictable to Bob, and then performing a construction which approximately reduces the player's strategies to a separable one (thus showing that the original expected score cannot be much larger than $\omega_c(G)$). This can be thought of as an extension of arguments used in the three-party case [18].

While Theorem 1.1 is highly general, its downside is that the upper bound expressed on Bob's guessing probability is only slightly smaller than 1. We therefore show another method for achieving potentially stronger upper bounds which is based on the Navascues-Pironio-Acin hierarchy [23].

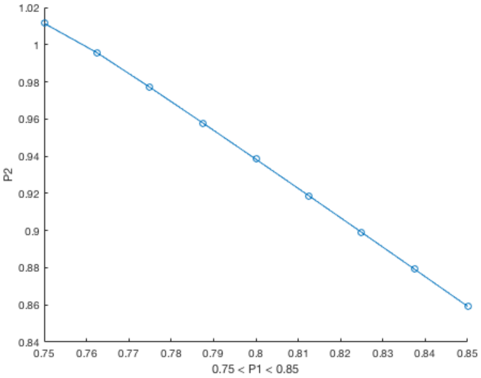


Figure 1: Upper bound on the guessing probability for the CHSH game.

The NPA hierarchy has been frequently used to constrain the behavior of quantum correlations — i.e., measurement outcomes arising from commuting sets of measurements $\{M_i^x\}_i, \{N_j^y\}_j$ on a quantum system Q. In our case, we must contend with the fact that not all the measurements are commuting: Bob's measurement when he guesses Alice's output may not commute with the measurement he performed on the first round. Fortunately, as observed by other authors [24, 25], the NPA hierarchy can be adapted to non-commuting cases. By a modification of the NPA hierarchy, we obtain the upper bound in Figure 1 on Bob's guessing probability as a function of the expected CHSH score. (See section 2 of [2].) This bound is tight up to 0.02.

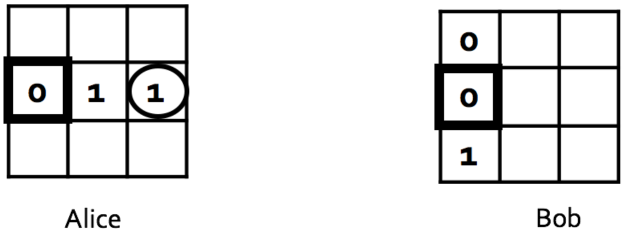
Figure 1 invites generalization to any games where the input and output alphabets are sufficiently small.

Certified deletion. Certified local randomness is a resource in any scenario in which two players are using untrusted devices and also do not trust one another. As an example application, we prove security for a simple *certified deletion* protocol.

In certified deletion, Alice wishes to prepare a secret classical message m, a classical key k, and a quantum encryption $\boxed{m}$ of m, satisfying two conditions. The first is that m can be perfectly recovered from $\boxed{m}$ and k. The second is that if Bob possesses $\boxed{m}$ only, there is a *deletion protocol* involving classical communication (only) between Alice and Bob which will allow Alice to guarantee that Bob has destroyed the message $\boxed{m}$. The security requirement is that after the deletion procedure is over, Bob will not be able to recover m even if he were given k.

Variants of this problem have been studied in other settings (e.g., [26] in a computational setting, [27, 16] in a bounded storage model). This problem is similar to oblivious transfer, but is strictly weaker, and thus known impossibility proofs for oblivious transfer do not apply.

Our results on local randomness suggest a way of performing certified deletion: proving that Alice's message m is inaccessible to Bob is equivalent to proving that m is locally random. To demonstrate this we prove security for a single-bit certified deletion protocol (Figure 3 in [2]).



In the Magic Square game, Alice is given a random row in a 3 × 3 grid and has to fill it in with bits that sum to an even number, and Bob is given a random column in a 3 × 3 grid and has to fill it in with bits that sum to an odd number. In order to win the game, the bits in overlapping squares (boxed) have to agree. We show that in any quantum strategy that wins with probability $1 - \epsilon$, any given off-column bit (circled) in Alice's row is almost perfectly unpredictable to Bob (see Corollary 3 in [2]). Thus the Magic Square game certifies near-perfect local randomness.

The protocol DEL in Figure 3 in [2] proceeds by first having Alice play her side of the Magic Square game N times with an untrusted device. Alice then chooses a random round i_s and records a random off-column bit m from the ith round. The key k consists of the round i_s and the number of the column she chose. The deletion procedure then consists of Bob playing his side of the Magic Square game and Alice confirming that the average score is above $1 - \epsilon$. We prove the following.

Theorem 1.2. *Assume that Protocol DEL succeeds with probability at least δ. Then, the probability that Bob can recover m given k is at most $\frac{1}{2} + F(\epsilon, N, \delta)$, where $\lim_{N\to\infty,\epsilon\to 0} F(\epsilon, N, \delta) = 0$.*

(See Theorem 4 in [2] for the full statement.) Our proof is based on the recent Magic Square rigidity result [28] and Azuma's inequality.

Further directions. A natural next step is to try to show that local randomness accumulates over multiple repetitions of a nonlocal game. Specifically, one could try prove that if a complete-support game G is repeated N times and achieves a superclassical score, then the smooth min-entropy of Alice's outputs is high even when conditioned on Alice's inputs and all of Bob's information. This would allow the generation of arbitrary amount of uniform local randomness (even from a noisy device). To our knowledge the current techniques for randomness expansion do not apply to this scenario (for example, [14] requires a Markov condition which is not satisfied in the blind case) but they invite extensions.

References

[1] Carl A. Miller and Yaoyun Shi. Randomness in nonlocal games between mistrustful quantum players. *Quantum Information & Computation*, 17(7&8):0595–0610, 2017.

[2] Honghao Fu and Carl A. Miller. Local randomness: Examples and application. arXiv:1708.04338, 2017.

[3] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys. 86, 419*, 86(419), 2014.

[4] R. Colbeck. Quantum and relativistic protocols for secure multi-party computation. Ph. D. thesis, University of Cambridge, arXiv:0911.3814, 2006.

[5] 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.

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

[7] Umesh V. Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In Howard J. Karloff and Toniann 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.

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

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

[10] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust randomness amplifiers: Upper and lower bounds. In *Proceedings of APPROX 2013 and RANDOM 2013*, volume 8096 of *Lecture Notes in Computer Science*, pages 468–483. Springer, 2013.

[11] Matthew Coudron and Henry 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.

[12] Carl A. Miller and Yaoyun 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] Carl A. Miller and Yaoyun Shi. Universal security for randomness expansion from the spot-checking protocol, 2015. arXiv:1411.6608.

[14] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. arXiv:1607.01796, 2016.

[15] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. arXiv:1607.01797, 2016.

[16] Jedrzej Kaniewski and Stephanie Wehner. Device-independent two-party cryptography secure against sequential attacks. *New Journal of Physics*, 18, May 2016.

[17] Marcin Pawlowski. Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations. *Physical Review A*, 82:032313, 2010.

[18] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. *SIAM Journal on Computing*, 40(3):848–877, 2011.

[19] Antonio Acín, Daniel Cavalcanti, Elsa Passaro, Stefano Pironio, and Paul Skrzypczyk. Necessary detection efficiencies for secure quantum key distribution and bound randomness. *Phys. Rev. A*, 93:012319, Jan 2016.

[20] Laura Mancinska. Maximally entangled states in pseudo-telepathy games. arXiv:1506.07080, June 2015.

[21] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. In *Proceedings of The 5th Innovations in Theoretical Computer Science (ITCS)*, 2014. arXiv:1210.1810v2.

[22] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. In *Proceedings - Annuel IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 766–755, 2013.

[23] Miguel Navascues, Stefano Pironio, and Antonio Acin. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10, 2008.

[24] Costantino Budroni, Tobias Moroder, Matthias Kleinmann, and Otfried Gühne. Bounding temporal quantum correlations. *Physical Review Letters*, 111(2):020403, 2013.

[25] Stefano Pironio, Miguel Navascués, and Antonio Acin. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on Optimization*, 20(5):2157–2180, 2010.

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

[27] Jeremy Riberio, Le Phuc Thinh, Jedrzej Kaniewski, Jonas Helsen, and Stephanie Wehner. Device-independence for two-party cryptography and position verification. arXiv:1606.08750, June 2016.

[28] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. arXiv:1512.02074v2, 2016.