Certifying the absence of quantum nonlocality

Carl A. Miller\textsuperscript{1,*} and Yaoyun Shi\textsuperscript{2,†}

\textsuperscript{1}Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA
\textsuperscript{2}Dept. of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA
(Dated: July 19, 2016)

Quantum nonlocality is an inherently non-classical feature of quantum mechanics and manifests itself through violation of Bell inequalities for nonlocal games. We show that in a fairly general setting, a simple extension of a nonlocal game can certify instead the absence of quantum nonlocality. Through contraposition, our result implies that a super-classical performance for such a game ensures that a player’s output is unpredictable to the other player. Previously such output unpredictability was known with respect to a third party.

Introduction. One of the most central and counter-intuitive aspects of quantum information theory is the ability for quantum players to outperform classical players at nonlocal games. In a nonlocal game for two players Alice and Bob, they are given inputs \(a\) and \(b\), respectively, and they produce outputs \(x\) and \(y\). The input pairs \((a, b)\) are drawn according to a fixed distribution, and a scoring function is applied to the joint input-output tuple \((a, b, x, y)\). When Alice and Bob use a classical strategy, they share a random variable \(r\) independent of the inputs, and decide their output deterministically from \(r\) and their input. In a quantum strategy, they share an entangled state and apply a local measurement determined by their input. A Bell inequality upper-bounds the maximum score that a classical strategy can achieve. There are multi-player 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. Such a violation of Bell inequality is referred to as quantum nonlocality (see [1] for a survey of this phenomenon).

We ask the question: is there any way to certify the absence of any non-classical quantum features? This question needs to be more precisely formulated, as otherwise it may appear trivially impossible. For example, when no Bell inequality is violated, we cannot conclude that Alice and Bob did not employ a quantum strategy. They could in principle still make use of quantum entanglement. For example, they could measure the same observable on a maximum entangled state to produce outputs that are always anti-correlated. This input-output correlation is clearly classical yet the process is (arguably) quantum.

In this work, we succumb to the postulate that quantum nonlocality is absent in quantum strategies of the following property. Operationally the strategy is equivalent to one where all the observables of a player commute with the joint state. We call such a strategy essentially classical. We show that the following simple extension of nonlocal game can indeed certify the absence of quantum nonlocality. After the nonlocal game is played, we give Alice’s input \(a\) to Bob and ask him to guess what Alice’s output was. Call this second task the guessing game. Our main theorem, stated informally, is the following. Let \(A\) be Alice’s local system.

Theorem 1 (Informal). If Bob succeeds with certainty in the guessing game, there is an isometry mapping Bob’s system to \(B' \otimes A'\) such that Bob’s strategy for the nonlocal game involves only \(B'\) and all Alice’s observables commute with the reduced state on \(AB'\). Consequently, the input-output correlation is classical.

Apart from the above foundational considerations, our investigation was also motivated by cryptography. A useful corollary of Bell inequality violation is that 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, even when the adversary knows the input. This is the basis for device-independent randomness expansion [2–11]. When two players play a game repeatedly and exhibit an average score above a certain threshold, their outputs must be highly random and can be post-processed into uniformly random bits. The produced uniform bits are random even conditioned on the input bits for the game (thus “expanding” the input randomness).

An important and challenging question arises: does a high score at a nonlocal game imply that one player’s output is random to the other player? Such a question is important for randomness expansion in a mutually distrustful 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. The contraposition of our result implies that a violation of Bell inequality in the nonlocal game necessarily requires that Alice’s output expands the input randomness, with respect to Bob. We discuss the implication on information erasure at the end of the paper.

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., [12], and the recent paper [13]).
Single-round games have also appeared in the literature where Bob is sometimes given only Alice’s input, and asked to produce her output (e.g., [14], [15]). We believe that the novelty of our scenario lies in the fact that we are proving that Alice’s output is uncertain to Bob after the execution of the game (when information has potentially been lost due to measurement).

Preliminaries. For any finite-dimensional Hilbert space $V$, let $L(V)$ denote the vector space of linear auto-morphisms of $V$. For any $M, N \in L(V)$, we let $\langle M, N \rangle$ denote $\text{Tr}[M^*N^*]$.

Throughout this paper we fix four disjoint finite sets $A, B, X, Y$, which denote, respectively, the first player’s input alphabet, the second player’s input alphabet, the first player’s output alphabet, and the second player’s output alphabet. A 2-player (input-output) correlation is a vector $(p_{xy}^{ab})$ of nonnegative reals, indexed by $a, b, x, y \in A \times B \times X \times Y$, satisfying

$$\sum_{x,y} p_{xy}^{ab} = 1$$

for all pairs $(a, b)$, and satisfying the condition that the quantities

$$p^a_x := \sum_y p_{xy}^{ab}, \quad p^b_y := \sum_x p_{xy}^{ab}$$

are independent of $b$ and $a$, respectively (no-signaling).

A 2-player game is a pair $(q, H)$ where

$$q: A \times B \to [0, 1]$$

is a probability distribution and

$$H: A \times B \times X \times Y \to [0, \infty)$$

is a function. If $q(a, b) \neq 0$ for all $a \in A$ and $b \in B$, the game is said to have a complete support. The expected score associated to such a game for a 2-player correlation $(p_{xy}^{ab})$ is

$$\sum_{a, b, x, y} q(a, b) H(a, b, x, y) p_{xy}^{ab}.$$

A 2-player strategy is a 5-tuple

$$\Gamma = (D, E, \{\{R^a_x\}_x\}_a, \{\{S^b_y\}_y\}_b, \gamma)$$

such that $D, E$ are finite dimensional Hilbert spaces, $\{\{R^a_x\}_x\}_a$ is a family of $X$-valued positive operator valued measures on $D$ (indexed by $A$), $\{\{S^b_y\}_y\}_b$ is a family of $Y$-valued positive operator valued measures on $E$, and $\gamma$ is a density operator on $D \otimes E$. The second player states $\beta^{xy}_{ab}$ of $\Gamma$ is defined by

$$\beta^{xy}_{ab} := \text{Tr}_D \left[ \sqrt{R^a_x \otimes S^b_y} \gamma \sqrt{R^a_x \otimes S^b_y} \right]$$

We define $\rho^a_a$ by the same expression with $S^b_y$ replaced by the identity operator. Define $\rho := \text{Tr}_D(\gamma) = \sum_x \rho^a_a$ for any $a$.

We say that the strategy $\Gamma$ achieves the 2-player correlation $(p_{xy}^{ab})$ if

$$p_{xy}^{ab} = \text{Tr}[\gamma(R^a_x \otimes S^b_y)]$$

for all $a, b, x, y$. If a 2-player correlation $(p_{xy}^{ab})$ can be achieved by a 2-player strategy then we say that it is a quantum strategy.

If $(p_{xy}^{ab})$ is a convex combination of product distributions (i.e., distributions of the form $(\rho_x^a \otimes r^b_y)$ where $\sum_x \rho^a_x = 1$ and $\sum_y r^b_y = 1$) then we say that $(p_{xy}^{ab})$ is a classical correlation. Note that if the underlying state of a quantum strategy is separable (i.e., it is a convex combination of bipartite product states) then the correlation it achieves is classical.

Congruent strategies. It is necessary to identify pairs of strategies that are essentially the same from an operational standpoint. We use a definition that is similar to definitions from quantum self-testing (e.g., Definition 4 in [16]).

A unitary embedding from a 2-player strategy

$$\Gamma = (D, E, \{\{R^a_x\}_x\}_a, \{\{S^b_y\}_y\}_b, \gamma)$$

to another 2-player strategy

$$\Gamma' = (\tilde{D}, \tilde{E}, \{\{\tilde{R}^a_x\}_x\}_a, \{\{\tilde{S}^b_y\}_y\}_b, \tilde{\gamma})$$

is a pair of unitary embeddings $i: D \hookrightarrow \tilde{D}$ and $j: E \hookrightarrow \tilde{E}$ such that $\tilde{\gamma} = (i \otimes j) \gamma (i \otimes j)^*$, $\tilde{R}^a_x = i^* \tilde{R}^a_x i$, and $\tilde{S}^b_y = j^* \tilde{S}^b_y j$.

Additionally, if $\Gamma$ is such that $D = D_1 \otimes D_2$, and $R^a_x = G_p^a \otimes I$ for all $a, x$, then we will call the strategy given by

$$(D_1, E, \{\{G^a_p\}_a\}_a, \{\{S^b_y\}_y\}_b, \text{Tr}_{D_2} \gamma)$$

a partial trace of $\Gamma$. We can similarly define a partial trace on the second subspace $E$ if it is a tensor product space.

We will say that two strategies $\Gamma$ and $\Gamma'$ are congruent if there exists a sequence of strategies $\Gamma = \Gamma_1, \ldots, \Gamma_n = \Gamma'$ such that for each $i \in \{1, \ldots, n - 1\}$, either $\Gamma_{i+1}$ is a partial trace of $\Gamma_i$, or vice versa, or there is a unitary embedding of $\Gamma_i$ into $\Gamma_{i+1}$, or vice versa. This is an equivalence relation. Note that if two strategies are congruent then they achieve the same correlation.

Essentially classical strategies and statement of Main Theorem. We are ready to define the key concept in this paper and to state formally our main theorem.

Definition 2. A quantum strategy $(6)$ is said to be essentially classical if it is congruent to one where $\gamma$ commutes with $R^a_x$ for all $a$ and $a$.

We are interested in strategies after the application of which Bob can predict Alice’s output given her input. This is formalized as follows. If $\chi_1, \ldots, \chi_n$ are positive semidefinite operators on some finite dimensional Hilbert space $V$, then we say that $\{\chi_1, \ldots, \chi_n\}$ is perfectly distinguishable if $\chi_i$ and $\chi_j$ have orthogonal support for any
This is equivalent to the condition that there exists a projective measurement on $V$ which perfectly identifies the state from the set $\{\chi_1, \ldots, \chi_n\}$.

**Definition 3.** A quantum strategy (6) allows perfect guessing (by Bob) if for any $a, b, y$, $\{\rho_{ab}^{xy}\}_x$ is perfectly distinguishable.

**Theorem 4** (Main Theorem). A strategy for a complete-support game is essentially classical if it allows perfect guessing.

We make two remarks before proving Main Theorem. First, the converse of the statement is not true. This is because even in a classical strategy, Alice’s output may depend on some local randomness, which Bob cannot perfectly predict.

Second, it is easy to see that the correlation of an essentially classical strategy must be classical.

**Proposition 5.** The correlation achieved by an essentially classical strategy must be classical.

Thus a corollary of Main Theorem is the following.

**Corollary 6.** If a strategy for a complete-support game allows perfect guessing, the correlation achieved must be classical.

Assertions of this sort are common in device-independent quantum cryptography — see, e.g., [5, 12, 17]. For completeness, we include the proof for the above proposition.

**Proof Proposition (5):** We need only to consider the case that $\gamma$ commutes with $R_{a}^{x}$ for all $a, x$. For each $a \in \mathcal{A}$, let $V_a = \mathbb{C}^{x_a}$, and let $\Phi_a : L(D) \rightarrow L(V_a \otimes D)$ be the nondestructive measurement defined by

$$\Phi_a(T) = \sum_{x \in x_a} |x\rangle \langle x| \otimes \sqrt{R_{a}^{x}T\sqrt{R_{a}^{x}}}. \quad (12)$$

Note that by the commutativity assumption, such operation leaves the state of $DE$ unchanged.

Without loss of generality, assume $\mathcal{A} = \{1, 2, \ldots, n\}$. Let

$$\Lambda \in L(V_1 \otimes \cdots \otimes V_n \otimes D \otimes E) \quad (13)$$

be the state that arises from applying the superoperators $\Phi_1, \ldots, \Phi_n$, in order, to $\gamma$. For any $a \in \{1, 2, \ldots, n\}$, the reduced state $\Lambda_{V_a \otimes D}$ is precisely the same as the result of taking the state $\gamma$, applying the measurement $\{R_{a}^{x}\}_x$ to $D$, and recording the result in $V_a$. Alice and Bob can therefore generate the correlation $\{\rho_{ab}^{xy}\}$ from the marginal state $\Lambda_{V_1, \ldots, V_n \otimes D \otimes E}$ alone (if Alice possesses $V_1, \ldots, V_n$ and Bob possesses $E$). Since this state is classical on Alice’s side, and therefore separable, the result follows.

**Proving Main Theorem.** We sketch the outline of the proof. Fix an arbitrary measurement $R_a := \{R_{a}^{x}\}_x$ for Alice. First, we show that $R_a$ induces a projective measurement $Q_a := \{Q_{a}^{x}\}_x$ on Bob’s system. Next, we argue that $Q_a$ commutes with Bob’s own measurement $S_b := \{S_{b}^{y}\}_y$ for any $b$. This allows us to isometrically decompose Bob’s system into two subsystems $E_1 \otimes E_2$, such that $S_b$ acts trivially on $E_2$, while $E_2$ alone can be used to predict $x$ given $a$. The latter property allows us to arrive at the conclusion that $R_a$ commutes with $\gamma_{DE_1}$.

We will need the following lemma, which is commonly used in studying two-player quantum strategies. The proof was sketched in [18] (see also Theorem 1 in [19]).

**Lemma 7.** Let $V$ be a finite-dimensional Hilbert space and let $\{M_j\}$ and $\{N_k\}$ be sets of positive semidefinite operators on $V$ such that $M_jN_k = N_kM_j$ for all $j, k$. Then, there exists a unitary embedding $i : V \rightarrow V_1 \otimes V_2$ and positive semidefinite operators $\{M_j\}_j$ on $V_1$ and $\{N_k\}_k$ on $V_2$ such that $M_j = i^*(M_j \otimes I)i$ and $N_k = i^*(I \otimes N_k)i$ for all $j, k$. 

**Proof Main Theorem 4:** Express $\Gamma$ as in (6). Without loss of generality, we may assume that $\text{Supp} \rho = E$. By the assumption that $\Gamma$ allows perfect guessing, for any $a$, the second-player states $\{\rho_{ab}^{xy}\}_x$ must be perfectly distinguishable (since otherwise the post-measurement states $\{\rho_{ab}^{xy}\}_x$ would not be). Therefore, we can find projective measurements $\{Q_{a}^{x}\}_x$ on $E$ such that

$$Q_{a}^{x} \rho Q_{a}^{x} = \rho_{a}^{x}. \quad (14)$$

We have that the states

$$\rho_{ab}^{xy} = \sqrt{S_{b}^{y}}Q_{a}^{x}\rho Q_{a}^{x}\sqrt{S_{b}^{y}} \quad (15)$$

are orthogonal for any $x \neq x'$. Since $\text{Supp} \rho = E$, we have $c \rho \leq \rho$ for some $c > 0$. Therefore,

$$\langle \sqrt{S_{b}^{y}}cQ_{a}^{x}\sqrt{S_{b}^{y}} \mid \sqrt{S_{b}^{y}}cQ_{a}^{x}\sqrt{S_{b}^{y}} \rangle = 0, \quad (17)$$

which implies, using the cyclicity of the trace function,

$$\left\| Q_{a}^{x}S_{b}^{y}Q_{a}^{x} \right\|_2 = 0. \quad (18)$$

Therefore, the measurements $\{Q_{a}^{x}\}_x$ and $\{S_{b}^{y}\}_y$ commute for any $a, b$.

By Lemma 7, we can find a unitary embedding $i : E \rightarrow E_1 \otimes E_2$ and such that $S_{b}^{y} = i^*(S_{b}^{y} \otimes I)i$ and $Q_{a}^{x} = i^*(I \otimes Q_{a}^{x})i$, for measurements $\{S_{b}^{y}\}_y$ and $\{Q_{a}^{x}\}_x$. With

$$\gamma = (I_D \otimes i)\gamma (I_D \otimes i^*), \quad (19)$$

the strategy $\Gamma$ embeds into the strategy

$$\Gamma' := \left( D, E_1 \otimes E_2, \{\{R_{a}^{x}\}_x\}_a, \{S_{b}^{y} \otimes I_{E_2}\}_y \right) \cup \gamma.$$

Under the strategy $\Gamma'$, the unmeasured system $E_2$ can be used by any third party to perfectly guess Alice’s output given her input, using the projective measurements \( \{ \mathcal{Q}_a^x \}_x \).

Since $\Gamma'$ is congruent to
\[
\Gamma := \left( D, E_1, \{ R_a^x \}_x, \{ \mathcal{S}_y^b \}_y, \gamma_{DE_1} \right),
\]
in order to conclude that $\Gamma$ is essentially classical, we need only to show that $\gamma_{DE_1}$ commutes with $R_a^x$ for all $a,x$.

To that end, we claim that for any $a,x,x'$, and any eigenstate $|\phi\rangle$ of $\gamma_{DE_1}$, there exists a positive eigenvalue,
\[
R_a^x |\phi\rangle = \mathcal{Q}_a^x |\phi\rangle.
\]
Thus with $\phi = |\phi\rangle\langle\phi|$, $R_a^x |\phi\rangle = \mathcal{Q}_a^x |\phi\rangle = \mathcal{Q}_a^x |\phi\rangle = \gamma_{DE_1} R_a^x,
\]
Therefore
\[
R_a^x \gamma_{DE_1} = \gamma_{DE_1} R_a^x.
\]
This completes the proof.

**Blind randomness expansion.** Untrusted-device quantum randomness expansion, as proposed in [2] proceeds as follows. A user begins with a seed $S$ (a uniformly random bit string) and two or more untrusted input-output device components $D_1, \ldots, D_n$. He uses the devices $N$ times, generating independent random inputs each time using the seed $S$. If the outputs of the devices over these trials form an average correlation that significantly non-classical, then the user assumes that the outputs are at least partially random. He then applies a randomness extractor (using additional seed) to obtain the output of the protocol, $T$, also expressed as a bit string. Under some conditions it has been shown that this protocol is secure — more precisely, the distribution of $ST$ is close (up to negligible error) to a uniform distribution, even from the perspective of an adversary who possesses a system $E$ that was initially entangled with $D_1, \ldots, D_n$ [5, 10, 11].

In the interest of minimizing resources and trust, we can instead pose the problem of *blind* randomness expansion. Suppose $n=2$. Can the outputs of such a protocol be proved secure even against an adversary who, along with his quantum side information, possesses the device component $D_2$?

Corollary 6 can be interpreted as a first step towards blind randomness expansion. It shows that if the devices $(D_1, D_2)$ exhibit a superclassical correlation, then there is some degree of unpredictability in the outputs of $D_1$, even from the perspective of an adversary who possesses $D_2$. A natural next step towards blind randomness expansion is to try to put a lower bound on the min-entropy of the first-player’s output from the perspective of the second player, as a function of the achieved correlation $(p_{xy}^{ab})$. Here, some divergences between the blind scenario and the ordinary scenario begin to appear.

Consider the CHSH game. If the correlation of two devices $D = (D_1, D_2)$ is $(p_{xy}^{ab})$, then the expected score for the CHSH game is
\[
\frac{1}{4} \sum_{a,b,x,y \in \{0,1\}} p_{xy}^{ab}.
\]
The best possible winning probability that can be achieved by a classical correlation is $3/4$, while the best possible winning probability that can be achieved by a quantum correlation is $\frac{3}{2} + \frac{\sqrt{2}}{4} \approx 0.853 \ldots$. By Corollary 6, any score above $3/4$ implies that the first player’s output is partially unpredictable to the second. (The same holds for any complete-support game.)

Self-testing for the CHSH game [20–22] implies that any quantum strategy that achieves the optimal score $\frac{3}{2} + \frac{\sqrt{2}}{4}$ is congruent to the following strategy (in which we use the notation $|\theta\rangle \in \mathbb{C}^2$ to denote the vector $\cos \theta |0\rangle + \sin \theta |1\rangle$, and let $\Phi^+ = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$):
\[
\begin{align*}
\gamma &= \Phi^+ \Phi^{+*} \\
R_0 &= |0\rangle \langle 0| \\
R_1 &= |\frac{\pi}{4}\rangle \langle \frac{\pi}{4}| \\
S_0 &= |\frac{\pi}{8}\rangle \langle \frac{\pi}{8}| \\
S_1 &= |\frac{5\pi}{8}\rangle \langle \frac{5\pi}{8}|.
\end{align*}
\]
Since the state of this strategy is pure, any environment state is trivial. The correlation $(p_{xy}^{ab})$ for this strategy has $p_{a}^{x} = 1/2$ for all $a, x \in \{0,1\}$, and so the min-entropy of the first player’s output (even from the perspective of an adversary who possess quantum side information and knows $a$) is $-\log_2(1/2) = 1$.

On the other hand, the second player has more information than an external adversary. For example, when $a = b = 0$, the second player states are
\[
\begin{align*}
\rho_{00} &= \left( \frac{1}{2} + \frac{\sqrt{2}}{4} \right) |\frac{\pi}{8}\rangle \langle \frac{\pi}{8}| - \frac{\sqrt{2}}{4} |\frac{5\pi}{8}\rangle \langle \frac{5\pi}{8}| \\
\rho_{01} &= \left( \frac{1}{2} - \frac{\sqrt{2}}{4} \right) |\frac{\pi}{8}\rangle \langle \frac{\pi}{8}| - \frac{\sqrt{2}}{4} |\frac{5\pi}{8}\rangle \langle \frac{5\pi}{8}| \\
\rho_{10} &= \left( \frac{1}{2} + \frac{\sqrt{2}}{4} \right) |\frac{\pi}{8}\rangle \langle \frac{\pi}{8}| - \frac{\sqrt{2}}{4} |\frac{5\pi}{8}\rangle \langle \frac{5\pi}{8}| \\
\rho_{11} &= \left( \frac{1}{2} - \frac{\sqrt{2}}{4} \right) |\frac{\pi}{8}\rangle \langle \frac{\pi}{8}| - \frac{\sqrt{2}}{4} |\frac{5\pi}{8}\rangle \langle \frac{5\pi}{8}|.
\end{align*}
\]
If the second player wishes to guess the first player’s output, his best strategy is to guess $x = 0$ if his state is $|\pi/8\rangle$ and to guess $x = 1$ if his state is $|5\pi/8\rangle$. (This is equivalent to predicting that his own output $y$ agrees with $x$.) Similar results hold for other input combinations, and thus the min-entropy of the first player’s output from the second player’s perspective is $-\log_2(\frac{1}{2} + \frac{\sqrt{2}}{4}) < 1$. Thus, while one-shot blind randomness expansion is achieved for the same class of correlations as ordinary randomness expansion, the certified min-entropy may be different.
Further directions. A natural next step would be to prove a robust version of Main Theorem 4, or just Corollary 6. This could lead to one-shot rate curves for blind randomness expansion (similar to, e.g., Figure 2 of [3]). It may require an appropriate quantity describing the amount of nonlocality (or the deviation from being essentially classical). Since the proof relies centrally on the commutativity of certain measurements, the notion of approximate commutativity [23, 24] may be useful. A strong robust version for the Corollary would state that for any $\delta > 0$, there exists $\epsilon > 0$ such that if the winning probability exceeds that of the optimal classical strategy by $\delta$, the guess probability must be $\leq 1-\epsilon$. For robust self-testing games, a weaker version follows where only sufficiently large $\delta$ is considered. Proving the general robust version appears to be challenging.

Another aspect of Corollary 6 is that it contains a notion of certified erasure of information. Note that in the CHSH 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 [13, 25]. An interesting research avenue is 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 [26], an interesting class that unifies Bell inequalities (constraints on spatially separated measurements) with Leggett-Garg inequalities (constraints on sequential measurements). In [27] such correlations are used for ordinary (non-blind) randomness expansion. Another interesting avenue is to explore how our techniques could be applied to more general sequential nonlocal games.

Acknowledgments. The first author thanks Marcin Pawłowski and Stefano Pironio for helpful information. This research was supported in party by US NSF Awards 1500095, 1216729, 1526928, and 1318070.

* carlmi@umich.edu
** shiyy@umich.edu

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

[2] R. Colbeck, Ph.D. thesis, University of Cambridge (2006).

[3] 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, et al., Nature 464, 1021 (2010).

[4] R. Colbeck and A. Kent, Journal of Physics A: Mathematical and Theoretical 44, 095305 (2011), URL http://stacks.iop.org/1751-8121/44/i=9/a=095305.

[5] U. V. Vazirani and T. Vidick, in Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012, edited by H. J. Karloff and T. Pitassi (ACM, 2012), pp. 61–76, ISBN 978-1-4503-1245-5, URL http://dl.acm.org/citation.cfm?id=2213977.

[6] S. Pironio and S. Massar, Phys. Rev. A 87, 012336 (2013), URL http://link.aps.org/doi/10.1103/PhysRevA.87.012336.

[7] S. Fehr, R. Gelles, and C. Schaffner, Phys. Rev. A 87, 012335 (2013), URL http://link.aps.org/doi/10.1103/PhysRevA.87.012335.

[8] M. Coudron, T. Vidick, and H. Yuen, in Proceedings of APPROX 2013 and RANDOM 2013 (Springer, 2013), vol. 8096 of Lecture Notes in Computer Science, pp. 468–483.

[9] M. Coudron and H. Yuen, in Proceedings of the 46th Annual ACM Symposium on Theory of Computing (2014), pp. 427–436.

[10] C. A. Miller and Y. Shi, in Proceedings of the 46th Annual ACM Symposium on Theory of Computing (2014), pp. 417–426.

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

[12] M. Pawłowski, Physical Review A 82, 032313 (2010).

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

[14] U. Vazirani and T. Vidick, in Proceedings of The 5th Innovations in Theoretical Computer Science (ITCS) (2014), arXiv:1210.1810v2.

[15] T. Vidick, in Proceedings - Annual IEEE Symposium on Foundations of Computer Science (FOCS) (2013), pp. 766–755.

[16] M. McKague, Interactive proofs for bqp via self-tested graph states, arXiv:1309.5675v2 (2015).

[17] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007), URL http://link.aps.org/doi/10.1103/PhysRevLett.98.230501.

[18] B. Tsirelson, Bell inequalities and operator algebras, http://www.tau.ac.il/~tsirel/download/bellopalg.pdf.

[19] V. B. Scholz and R. F. Werner (2008), arXiv:0812.4305v1.

[20] M. McKague, T. H. Yang, and V. Scarani, Journal of Physics A: Mathematical and Theoretical 45, 455304 (2012), URL http://stacks.iop.org/1751-8121/45/i=45/a=455304.

[21] B. W. Reichardt, F. Unger, and U. Vazirani, Nature 496, 456 (2013).

[22] C. A. Miller and Y. Shi, in 8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2013, May 21-23, 2013, Guelph, Canada, edited by S. Severini and F. G. S. L. Brandão (Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2013), vol. 22 of LIPIcs, pp. 254–262, ISBN
[23] N. Ozawa, Journal of Mathematical Physics 54 (2013).
[24] M. Coudron and T. Vidick, Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP) (2015), chap. Interactive Proofs with Approximately Commuting Provers, pp. 355–366.

[25] D. Unruh, J. ACM 62, 49:1 (2015), ISSN 0004-5411, URL http://doi.acm.org/10.1145/2817206.
[26] R. Gallego, L. E. Wurflinger, R. Chaves, A. Acin, and M. Navascues, New Journal of Physics 16 (2014).
[27] F. J. Curchod, M. Johansson, M. J. Hoban, P. Wittek, and A. Acin, Unbounded randomness certification using sequences of measurements, arXiv:1510.03394v1 (2015).