An Elementary Proof of Private Random Number Generation from Bell Inequalities

Carl A. Miller*

National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899, USA
Joint Center for Quantum Information and Computer Science,
3100 Atlantic Bldg, University of Maryland, College Park, MD 20742, USA

(Dated: July 25, 2017)

The field of device-independent quantum cryptography has seen enormous success in the past several years, including security proofs for key distribution and random number generation that account for arbitrary imperfections in the devices used. Full security proofs in the field so far are long and technically deep. In this paper we show that the concept of the *mirror adversary* can be used to simplify device-independent proofs. We give a short proof that any bipartite Bell violation can be used to generate private random numbers. The proof is based on elementary techniques and is self-contained.

Quantum cryptography is based on, among other physical principles, the concept of *intrinsic randomness*: certain quantum measurements are unpredictable, even to adversary who has complete information about the protocol and the apparatus used. This intrinsic randomness allows a user to generate cryptographic keys that are guaranteed to be secure without the need for computational assumptions.

Device-independent quantum cryptography is based on a more specific observation: two or more devices that exhibit superclassical probability correlations (when blocked from communicating) must be making quantum measurements, and therefore must be exhibiting random behavior. This allows the generation of random numbers even when the devices themselves are not trusted. This idea has been used in multiple cryptographic contexts, including randomness expansion and amplification [1, 2], key distribution [3], and coin-flipping [4], and has been realized in experiment [5, 6].

Despite the simplicity of the central idea, proofs for device-independent quantum cryptography are challenging and took several years to develop. One of the central challenges is proving that the random numbers generated by a Bell experiment are secure even in the presence of quantum side information. (This level of security is necessary for quantum key distribution, and also for random number generation if one wishes to use the random numbers as inputs to another quantum protocol.) While classical statistical arguments can be used to show that the outputs of a Bell violation are unpredictable to a classical adversary (see., e.g., [7, 8]) these proofs do not carry over to the case of quantum side information because of the notion of information locking [9].

Known proofs of Bell randomness in the presence of quantum side information have used tools that are specific to the context: [10] uses reconstruction properties of quantum-proof randomness extractors, and [11–14] are based on inductive arguments centered on the quantum Renyi divergence function. Such proofs are long and mathematically complex. The recent paper [14] provides an easily adaptable framework for proving new results on randomness generation, but it is based on the entropy accumulation theorem [13], the proof of which is technically deep.

The goal of the current paper is provide a compact security proof of Bell randomness in the presence of quantum side information. The proof is based on the concept of the *mirror adversary* – the idea that a quantum adversary who attempts to guess the random numbers by mirroring the devices' measurements is almost as good as an optimal adversary. This idea was discussed in a previous paper by the author [15], and is essentially a reframing of the commonly used idea of pretty good measurements (see expression (7) below).

In the current paper the mirror adversary technique is combined with techniques drawn from other sources [16, 17] to give a compact proof of private random number generation from Bell experiments. (The paper does not attempt to maximize the performance parameters, which are suboptimal compared to [10–14].) The proof is self-contained, with material from other sources reproved as needed. The only assertions taken for granted in the proof are Azuma's inequality (see Theorem 7.2.1 in [18]) and Holder's inequality (see Corollary IV.2.6 in [19]).

The main result is the following (see Theorem 7).

Theorem 1 (Informal) *Suppose that two untrusted devices exhibit a Bell violation of $\delta > 0$ over N rounds. Then, $\Omega(N\delta^6)$ private random bits can be extracted from the outputs of the devices in polynomial time, using $O(N)$ bits of public randomness (that is, randomness known to the adversary but not the devices). The resulting private bits are secure against quantum side information.*

The mirror adversary technique is a general way of reducing security questions in the quantum context to classical statistical statements, and it is potentially useful for any cryptographic task in which security must be proved against a passive entangled adversary.

The author thanks Honghao Fu, Yi-Kai Liu, Ray Perlner, and Thomas Vidick for comments on this paper.

* camiller@umd.edu

Preliminaries. Throughout the paper, a *register* Z is a finite-dimensional Hilbert space with a fixed orthonormal basis (the elements of which we call *basic states*). A *state* ϕ of Z is a density operator on Z. Let $|Z| = \dim(Z)$. If $Z = Z_1 \otimes Z_2$ (which we may abbreviate as $Z = Z_1 Z_2$) we will write ϕ^{Z_1} for $\mathrm{Tr}_{Z_2}\phi$. If Z_2 is a register and e is a basic state of Z_2, then $\phi_e^{Z_1}$ denotes $\mathrm{Tr}_{Z_2}[\phi(I_{Z_1} \otimes |e\rangle\langle e|)]$. As a convenience, if X is an operator on Z and Y is an operator on Z_1, then the expression XY means $X(Y \otimes I_{Z_2})$ and the expression YX means $(Y \otimes I_{Z_2})X$.

We give a formalism for nonlocal games and the quantum strategies used in such games. We begin by formalizing measurements. An (N-fold) measurement strategy on a register Q is a family of positive operator-valued measures on Q of the form

$$\left\{ \left\{ F_{\mathbf{u}}^{\mathbf{t}} \right.{}_{\mathbf{t} \in \mathcal{T}^N} \right\}_{\mathbf{u} \in \mathcal{U}^N}, \tag{1}$$

where $\mathcal{T}$ and $\mathcal{U}$ are finite sets. Such a strategy is *sequential* if for any $t_1, \ldots, t_i \in \mathcal{T}$ and $\mathbf{u} \in \mathcal{U}^N$, the operator

$$F_{\mathbf{u}}^{t_1 \cdots t_i} := \sum_{t_{i+1} \cdots t_n} F_{\mathbf{u}}^{t_1 \cdots t_i t_{i+1} \cdots t_n} \tag{2}$$

is independent of the values of $u_{t+1} \cdots u_n$. (In such a case we can simply write $F_{u_1 \cdots u_i}^{t_1 \cdots t_i}$ for $F_{\mathbf{u}}^{t_1 \cdots t_i}$.) Sequential measurements model the behavior of a quantum player who receives inputs $u_1, \ldots, u_N$ and produces outputs $t_1, \ldots, t_N$ in sequence. In such a case, for any $u_1, \ldots, u_i$ and $t_1, \ldots, t_i$ for which $F_{u_1 \cdots u_i}^{t_1 \cdots t_i} \neq 0$, there is a 1-fold measurement strategy on Q given by

$$\left\{ \left\{ \left(F_{u_1 \cdots u_i}^{t_1 \cdots t_i} \right)^{-1/2} F_{u_1 \cdots u_{i+1}}^{t_1 \cdots t_{i+1}} \left(F_{u_1 \cdots u_i}^{t_1 \cdots t_i} \right)^{-1/2} \right\}_{t_{i+1}} \right\}_{u_{i+1}},$$

which defines the behavior of the player on the $(i+1)$st round conditioned on the inputs sequence $u_1, \ldots, u_i$ and output sequence $t_1, \ldots, t_i$ for the first i rounds. We call these the *conditional* measurement strategies induced by $\{\{F_{\mathbf{u}}^{\mathbf{t}}\}_{\mathbf{t}}\}_{\mathbf{u}}$.

An *r-player nonlocal game* H consists of the following data: (1) a finite set of input strings $\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_r$ and a finite set of outputs strings $\mathcal{O} = \mathcal{O}_1 \times \cdots \times \mathcal{O}_r$ (2) a probability distribution p on $\mathcal{I}$, and (3) a scoring function $L \colon \mathcal{I} \times \mathcal{O} \to \mathbb{R}$. For such a game, H^N denotes the N-fold direct product of H (i.e., the game the game played N times in parallel, with independently chosen inputs, and where the score is the sum of scores achieved on each of the N copies of the game).

A measurement strategy for H on a register Q is a measurement strategy on Q of the form $\{\{F_i^o\}_{o \in \mathcal{O}}\}_{i \in \mathcal{I}}$. Such a strategy is n-partite $Q = Q_1 \otimes \cdots \otimes Q_n$ and

$$F_i^o = F_{1,i_1}^{o_1} \otimes \cdots \otimes F_{n,i_n}^{o_n} \tag{3}$$

where $\{\{F_{k,i_k}^{o_k}\}_{o_k \in \mathcal{O}_k}\}_{i_k \in \mathcal{I}_k}$ are measurement strategies on Q_k for $k = 1, 2, \ldots, n$. A sequential measurement strategy for the game H^N is an *n-partite sequential measurement strategy* if all of its conditional strategies are n-partite. (This class of strategies models the behavior of players who must play the different rounds of the game in sequence, and who can communicate in between but not during rounds.)

If $\mathbf{F}$ is a strategy on a register Q, and ϕ is a state of Q, then we refer to the pair $(\mathbf{F}, \phi)$ simply as a (quantum) strategy for Q. Let $\omega(H)$ denote the supremum of the expected score at G among all quantum strategies.

Proposition 2 *Let H be an r-player nonlocal game whose scoring function has range $[-K, K]$, and let $(\mathbf{F}, \phi)$ be an n-partite sequential measurement strategy for H^N. Then, the probability that the score achieved by $(\mathbf{F}, \phi)$ exceeds $(\omega(H) + \delta)N$ is no more than*

$$e^{-N\delta^2/8K^2}. \tag{4}$$

Proof. For each $i = 1, 2, \ldots, N$, let W_i denote the score achieved on the ith round, and let

$$\overline{W}_i = E[W_i \mid W_{i-1} \cdots W_1]. \tag{5}$$

The sequence $\left(\sum_{j=1}^{i} (W_i - \overline{W}_i) \right)_{i=1}^{N}$ forms a Martingale, and thus by Azuma's inequality (noting that $\left| W_i - \overline{W}_i \right| \leq 2K$) the probability that

$$\sum_{i=1}^{N} (W_i - \overline{W}_i) > \delta N \tag{6}$$

is upper bounded by (4). Since $\overline{W}_i \leq w(H)$, the desired result follows. □

For convenience, we also make the following definition. A *Bell game* is a game G for which we make the following assumptions:

1. The input alphabets and output alphabets are all equal to $\{0, 1, 2, \ldots, n-1\}$ for some n. (We call n the "alphabet size.")
2. The input distribution is uniform.
3. The range of the scoring function is $[-1, 1]$.
4. The optimal classical score is 0.

Note that any Bell inequality can be put into this form (by an appropriate affine transformation of the scoring function).

The mirror adversary. If α is a quantum-classical state of a register QC (that is, a state of the form $\sum_c \alpha_c \otimes |c\rangle\langle c|$) then the *pretty good measurement* induced by α on Q is the C-valued measurement given by

$$\{(\alpha^Q)^{-1/2} \alpha_c^Q (\alpha^Q)^{-1/2}\}_{c \in C}. \tag{7}$$

This is a common construction. In the cryptographic context it can be thought of as a "pretty good" attempt by an adversary to use to Q to guess C.

Let ρ be a state of the register Q. Then, we can construct a purification for ρ as follows: let Q' be an isomorphic copy of Q, let $\Phi = \sum_e e \otimes e \in Q \otimes Q'$, where

Parameters:

- A 2-player Bell game G with alphabet size n.
- A real number $\delta > 0$ (the degree of Bell violation).
- Positive integers N (the number of rounds), and J (the output size).

1. A pure tripartite state ABE is prepared by Eve, and with A possessed by Alice, B possessed by Bob, and E possessed by Eve.
2. The referee generates uniformly random numbers $x_1, y_1 \in \{1, 2, \ldots, n\}$, gives them as input to Alice and Bob, respectively, who return outputs s_1, t_1. This is repeated $(N-1)$ times to obtain input sequences $x_1, \ldots, x_N$, $y_1, \ldots, y_N$ and output sequences $s_1, \ldots, s_N$, $t_1, \ldots, t_N$.
3. The referee checks whether the average score exceeds δ. If not, the protocol is aborted.
4. Let D be a 2-universal hash family from $\mathcal{S}^N$ to $\mathbb{F}_2^J$ with $|D| \leq 4\left|\mathcal{S}^N\right|^2$ (see subsection A 3 in the appendix). The referee chooses $F \in D$ at random and outputs $F(\mathbf{s})$.

FIG. 1. The random number generation protocol.

the sum is over all basic states of Q. (We call Φ the *Bell state* of QQ'.) Let $\hat{\rho}$ denote the projector onto the one-dimensional subspace of $Q \otimes Q'$ spanned by $(\sqrt{\rho} \otimes I_{Q'})\Phi$. We call $\hat{\rho}$ the *canonical purification* of ρ. Note that $\mathrm{Tr}_{Q'} \hat{\rho} = \rho$ while $\mathrm{Tr}_Q \hat{\rho} = \rho^\top = \overline{\rho}$.

The following proposition implies that a "pretty good" adversary in a Bell experiment simply mirrors the device's measurements. (As a consequence, if the devices' measurement were sequential, so are the adversary's.)

Proposition 3 *Let ρ be a state of a register Q, and let $\hat{\rho}$ be a state of registers QQ' which is a canonical purification of ρ. Let α be the state QC that arises from $\hat{\rho}$ by performing a measurement $\{R_c\}_{c \in \mathcal{C}}$ on Q' and storing the result in a register C. Then, the pretty good measurement induced by α on Q is isomorphic to $\{\overline{R}_c\}_{c \in \mathcal{C}}$.*

Proof. The state α is given by the expression $\alpha = \sum_c |c\rangle\langle c| \otimes \sqrt{\rho}\overline{R}_c\sqrt{\rho}$, and $\alpha^Q = \rho$. The pretty good measurement induced by α on Q is thus isomorphic to $\{\rho^{-1/2}\sqrt{\rho}\overline{R}_c\sqrt{\rho}\rho^{-1/2}\} = \{\overline{R_c}\}$. □

The next proposition, which is a modification of a result from [16], expresses the fact that if the pretty good measurement yields (almost) no information about a classical register C, then that register must be (almost) uniformly random. We state a version that will be useful in the device-independent context. Let Z denote a classical register with two basic states, *abort* and *succ*.

Proposition 4 *Let α be a state of a tripartite register QCZ which is classical on CZ. Let $\{R_z\}$ and $\{R_{cz}\}$ denote the pretty good measurements on Q:*

$$R_{cz} = (\alpha^Q)^{-1/2}\alpha^Q_{cz}(\alpha^Q)^{-1/2}, \tag{8}$$

$$R_z = (\alpha^Q)^{-1/2}\alpha^Q_z(\alpha^Q)^{-1/2}. \tag{9}$$

Let $f = \mathrm{Tr}[\alpha^Q_{succ} R_{succ}]$ and

$$f' = \sum_c \mathrm{Tr}[\alpha^Q_{c,succ} R_{c,succ}]. \tag{10}$$

Then,

$$\left\|\alpha^{QC}_{succ} - \alpha^Q_{succ} \otimes U_C\right\|_1 \leq \sqrt{f'\,|C| - f}, \tag{11}$$

where U_C denotes the completely mixed state on C.

The proof is given in the appendix. Note that the quantity f is the probability of the event that both $Z =$ *succ* and that an adversary who uses the pretty good measurement will guess that $Z =$ *succ*. The quantity f' is the probability that the previous event holds *and* the adversary guesses C. If $f' = f/|C|$ (that is, if the adversary's guess at C is no better than random) then the term on the right side of (11) is equal to zero.

Guessing games. The following is roughly the same as the construction of immunization games in [17]. Let $G = ((\mathcal{X}, \mathcal{Y}), (\mathcal{S}, \mathcal{T}), p, L)$ be a 2-player Bell game with alphabet size n, and let $K > 0$. Then we define a new 3-player game G_K as follows.

1. The input alphabets for the three players are $\mathcal{X}, \mathcal{Y}$ and $\mathcal{X} \times \mathcal{Y}$, respectively, and the output alphabets are $\mathcal{S}, \mathcal{T}$ and $\mathcal{S}$, respectively.
2. The probability distribution is uniform on triples of the form $(x, y, (x, y))$, with $x \in \mathcal{X}, y \in \mathcal{Y}$.
3. The score assigned to an input triple $(x, y, (x, y))$ and output triple (s, t, s') is $L(x, y, s, t)$ if $s = s'$, and is $(-K)$ otherwise.

Proposition 5 *For any Bell game G with alphabet size n, $\omega(G_K) \leq 4n/\sqrt{K}$.*

Let G be a Bell game and $(\rho, \mathbf{M}, \mathbf{N})$ a strategy for G.

1. The register AB is prepared in state ρ. For $i = 1, 2, \ldots, n$, Alice applies the measurement $\{M_i^s\}$ to A and records the result in a classical register S_i.
2. Referee gives Alice and Bob randomly chosen inputs $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively.
3. Alice returns the register S_x. Bob measures B with $\{N_y^t\}_t$ and reports the result.

FIG. 2. A process in which Alice is forced to behave classically.

Our proof is similar to [17]. We will use the process described in Figure 2.

Proof. Let $Y = (\Gamma, \mathbf{M}, \mathbf{N}, \mathbf{P})$ be a quantum strategy for G_K on a space $A \otimes B \otimes E$. Let $\rho = \Gamma^{AB}$, and for any $x \in \mathcal{X}, s \in \mathcal{S}$, let ρ_x^s denote the subnormalized state of AB induced by the measurement P_{xy}^s on E.

For any x, y, the probability that Alice's and Eve's outputs will disagree when the input is $(x, y, (x, y))$ is given by the quantity $(1 - \sum_s \mathrm{Tr}(M_x^s \rho_x^s))$, which we denote by δ_x. Note that if the average failure probability $\sum_x \delta_x / n$ exceeds $1/K$, then (since a score of $-K$ is awarded when Eve fails to guess Alice's output) the score achieved by Y obviously cannot exceed 0. So, we will assume for the remainder of the proof that $\sum_x \delta_x/n \leq 1/K$.

By Proposition 8 in the appendix, we have

$$\left\| \sum_s M_x^s \rho M_x^s - \rho \right\|_1 \leq 4\sqrt{\delta_x} \tag{12}$$

for any x, y. Therefore if we let W_x denote the completely positive trace-preserving map on A given by $X \mapsto \sum_s M_x^s X M_x^s$, we obtain the following distance inequalities for the states obtained by applying the maps W_x sequentially:

$$\|W_i W_{i-1} \cdots W_1(\rho) - \rho\|_1 \tag{13}$$
$$\leq \sum_{j=1}^{i} \|W_i W_{i-1} \cdots W_j(\rho) - W_{i-1} W_{i-2} \cdots W_{j+1}(\rho)\|_1$$
$$\leq \sum_{j=1}^{i} \|W_j(\rho) - \rho\|_1 \leq \sum_{j=1}^{i} 4\sqrt{\delta_j}. \tag{14}$$

(Here we have used the fact that $\|\cdot\|_1$ is non-increasing under quantum processes.)

Observe that in the process in Figure 2, the state that Alice and Bob measure at step 3 is separable, and so their expected score cannot exceed 0. On the other hand, by (14), the state of the register AB is never more than trace distance $\sum_{j=1}^{n} 4\sqrt{\delta_j}$ from the original state ρ, and so the expected score achieved in Figure 2 also cannot be less than $\omega(G, Y) - \sum_{j=1}^{n} 4\sqrt{\delta_j}$. Thus we have

$$\omega(G, Y) \leq \sum_{j=1}^{n} 4\sqrt{\delta_j} \tag{15}$$

which implies $\omega(G, Y) \leq 4\sqrt{n}\sqrt{\sum_{j=1}^{n} \delta_j}$. Since we have assumed $\sum_x \delta_x \leq n/K$, this yields the desired result. □

Security proof. We will now prove the security of the protocol in Figure 1 by considering the "mirrored" version of the protocol as shown in Figure 3.

Proposition 6 *For the process in Figure 3, let succ and succ′ denote the events that the referee and the adversary consider the protocol to have succeeded (respectively). Then,*

$$\mathbf{P}((\mathbf{S} = \mathbf{S}') \wedge succ \wedge succ') \leq e^{-\Omega(N\delta^6/n^4)}. \tag{16}$$

Proof. For any $K \geq 1$, if the three events on the left side of (16) all occur, then Alice and Bob and the adversary have achieved an average score of at least δ at the repeated game $(G_K)^N$ using a sequential tripartite strategy. By Propositions 2 and 5, the probability of such a score is no more than

$$\exp(-N(\delta - 4n/\sqrt{K})^2/8K^2) \tag{17}$$

Parameters:

- A 2-player Bell game G with alphabet size n.
- A real constant $\delta > 0$ and positive integers N, J.
- A bipartite state Σ of registers AB.

1. Registers $ABA'B'$ are prepared in the canonical purification of the state Σ.
2. The referee prepares n-valued registers $X_1, \ldots, X_N, X_1', \ldots, X_N' Y_1, \ldots, Y_N, Y_1', \ldots, Y_N'$, and D-valued registers F, F' (where D denotes the hash family from step 4 in Figure 1) so that for each register Z the corresponding primed register Z' is in a Bell state with Z. The referee gives all primed registers to the adversary.
3. The referee measures the registers $\mathbf{X}, \mathbf{Y}$ in the standard bases to obtain $x_1, \ldots, x_N$ and $y_1, \ldots, y_N$, which are given sequentially to Alice and Bob who return outputs $s_1, \ldots, s_N, t_1, \ldots, t_N$.
4. The referee checks whether the average score exceeds δ. If not, the referee considers the protocol aborted. If so, the referee measures F, and then computes $\mathbf{V} := F(\mathbf{S})$.
5. The adversary carries out step 3 above herself, using the registers $A', B', \mathbf{X}', \mathbf{Y}'$ and the conjugates of the measurements used by Alice and Bob, to obtain outputs $\mathbf{S}', \mathbf{T}'$. If the average score at G is less than δ, the adversary considers the protocol aborted. If not, she computes $\mathbf{V}' := F'(\mathbf{S}')$.

FIG. 3. The mirrored random number generation protocol.

Setting $K = (8n/\delta)^2$ yields the desired result. □

Note that the event $((\mathbf{V} = \mathbf{V}') \wedge succ \wedge succ')$ can occur only if either $((\mathbf{S} = \mathbf{S}') \wedge succ \wedge succ')$ occurs, or if $((\mathbf{S} \neq \mathbf{S}') \wedge succ \wedge succ')$ occurs but nonetheless $F(\mathbf{S}) = F(\mathbf{S}')$. Since F is chosen from a 2-universal hash family, we have

$$\mathbf{P}((\mathbf{V} = \mathbf{V}' \wedge succ \wedge succ')$$
$$\leq e^{-\Omega(N\delta^6/n^4)} + 2^{-J}\mathbf{P}(succ \wedge succ').$$

By Proposition 3, the register $\mathbf{V}'$ in Figure 3 is precisely the result of the adversary using a pretty good measurement in Figure 1 in order to guess $\mathbf{V}$. Thus by Proposition 4 (with $C = \mathbf{V}$ and $Q = \mathbf{XY}FE$), we obtain the following.

Theorem 7 *Let ρ denote the final state of the registers in Figure 1. Then,*

$$\left\|\rho_{succ}^{\mathbf{VXY}FE} - U_{\mathbf{V}} \otimes \rho_{succ}^{\mathbf{XY}FE}\right\|_1 \leq 2^{J/2 - \Omega(N\delta^6/n^4)}. \quad \square$$

Note that if we fix δ, n and let $J = \lfloor cN \rfloor$ for some sufficiently small $c > 0$, the expression on the right of the inequality above vanishes exponentially. Thus random number generation with a linear rate and negligible error term is achieved.

Appendix A: Supplementary Proofs

1. The proof of Proposition 4

We follow the proof of Lemma 4 in [16]. Let $X = \alpha^Q$ and $Y = \alpha^{QC}_{succ}$. Note that $\mathrm{Tr}(X) = 1$, and therefore $\left\| X^{1/d} \right\|_d = 1$ for any d. By Holder's inequality, we have the following.

$$\begin{aligned}
&\left\| Y - Y^Q \otimes U_C \right\|_1 \\
&\leq \left\| X^{1/4} \otimes I_C \right\|_4 \left\| X^{-1/4}(Y - Y^Q \otimes U_C)X^{-1/4} \right\|_2 \\
&\quad \cdot \left\| X^{1/4} \otimes I_C \right\|_4 \\
&= |C|^{1/4} \cdot \mathrm{Tr}\left[\left(X^{-1/4}(Y - Y^Q \otimes U_C)X^{-1/4} \right)^2 \right]^{1/2} |C|^{1/4} \\
&= |C|^{1/2} \left\{ \mathrm{Tr}\left[\left(X^{-1/4} Y X^{-1/4} \right)^2 \right] \right. \\
&\quad -2\mathrm{Tr}\left[X^{-1/2} Y X^{-1/2} (Y^Q \otimes U_C) X^{-1/4} \right] \\
&\quad \left. +\mathrm{Tr}\left[\left(X^{-1/4}(Y^Q \otimes U_C)X^{-1/4} \right)^2 \right] \right\}^{1/2} \\
&= |C|^{1/2} \left\{ \mathrm{Tr}\left[\left(X^{-1/4} Y X^{-1/4} \right)^2 \right] \right. \\
&\quad \left. -\frac{1}{|C|} \mathrm{Tr}\left[\left(X^{-1/4}(Y^Q)X^{-1/4} \right)^2 \right] \right\}^{1/2},
\end{aligned}$$

where we have used the fact that $\mathrm{Tr}[(Y^Q \otimes U_C)Z] = \frac{1}{|C|}\mathrm{Tr}[Y^Q Z^Q]$ for any Hermitian operator Z on QC. By substitution we obtain the desired result.

2. Predictable measurements

We reprove an additional result used by other authors [17, 20]. The following proposition asserts that if a quantum-classical state of a register QC is such that C can be accurately guessed from a measurement on Q, then that same measurement does not disturb the state by much.

Proposition 8 *Let QC be a classical quantum register in state α, and let $\{P^c\}_c$ be a projective measurement on Q whose outcome agrees with C with probability $1-\delta$. Then,*

$$\left\| \sum_{c \in C} P^c \alpha P^c - \alpha \right\|_1 \leq 4\sqrt{\delta}. \tag{A1}$$

Proof. Our proof is similar to that of [20], Lemma I.4. First suppose that α is concentrated on a single basic state of C, i.e., $P_\alpha(C = z) = 1$ for some z. Then,

$$\mathrm{Tr}((P^z)\alpha) = 1 - \delta,$$

and therefore

$$\begin{aligned}
&\left\| P^z \alpha P^z - \alpha \right\|_1 \\
&= \left\| (P^z)^\perp \alpha P^z + (P^z)\alpha(P^z)^\perp + (P^z)\alpha(P^z)^\perp \right\|_1 \\
&\leq \left\| (P^z)^\perp \alpha P^z \right\|_1 + \left\| (P^z)\alpha(P^z)^\perp \right\|_1 + \left\| (P^z)^\perp \alpha (P^z)^\perp \right\|_1 \\
&= 2\left\| (P^z)^\perp \alpha P^z \right\|_1 + \delta \\
&\leq 2\left\| (P^z)^\perp \sqrt{\alpha} \right\|_2 \left\| \sqrt{\alpha} P^z \right\|_2 + \delta \\
&\leq 2\sqrt{\left\| (P^z)^\perp \alpha (P^z)^\perp \right\|_1} \sqrt{\left\| P^z \alpha P^z \right\|_1} + \delta \\
&= 2\sqrt{(1-\delta)\delta} + \delta \\
&\leq 3\sqrt{\delta}.
\end{aligned}$$

And, $\left\| P^z \alpha P^z - \sum_c P^c \alpha P^c \right\|_1 \leq \delta \leq \sqrt{\delta}$ which yields the desired result.

To general case now follows, since any state of CQ is is a convex combination of states that are concentrated on a single value of C, the function $\left\| \cdot \right\|_1$ is convex, and the square root function is concave. □

3. Two-universal hash families

We make use of some standard ideas (see, e.g., section 4.6.1 in [21]). Let P, R be finite sets with $|R| \leq |P|$. Then, a set of functions D from P to R is 2-*universal* if for any distinct $p, p' \in P$, the probability that a function F chosen uniformly at random from D will satisfy $F(p) = F(p')$ is less than or equal to $1/|R|$.

Proposition 9 *Let P be a finite set and let u be a positive integer with $2^u \leq |P|$. Then there exists a 2-universal set of functions from P to $\mathbb{F}_2^u$ of size $\leq 4|P|^2$.*

Proof. Let v be such that $2^{v-1} < |P| \leq 2^v$. Without loss of generality, we may assume that $P \subseteq \mathbb{F}_{2^v}$. Let D' be the set of all affine endomorphisms $(X \mapsto aX + b)$ of $\mathbb{F}_{2^v}$. Fix a function $T \colon \mathbb{F}_{2^v} \to \mathbb{F}_2^u$ such that each element of R has exactly 2^{u-v} pre-images, and let $D = T \circ D'$. Note that $|D| \leq |D'| = (2^v)^2 \leq 4|P|^2$.

For any $p \neq p'$ and q, q' in $\mathbb{F}_{2^v}$, there is exactly one function in D' which maps (p, p') to (q, q'). Thus the distribution of $(F(p), F(p'))$ on $P \times P$ is uniform when F is chosen at random from D', and likewise $(T \circ F(p), T \circ F(p'))$ is uniform on $R \times R$. The desired result follows.

[1] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation," Ph.D. thesis, University of York, arXiv:0911.3814 (2007).

[2] R. Colbeck and R. Renner, Nature Physics **8**, 450 (2012).

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, Phys. Rev. Lett. **106**, 220501 (2011).

[5] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday,

D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, *et al.*, Nature **464**, 1021 (2010).

[6] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm, "Experimentally generated random numbers certified by the impossibility of superluminal signaling," (2017), arXiv:1702.05178.

[7] S. Fehr, R. Gelles, and C. Schaffner, Physical Review A **87**, 012335 (2013).

[8] S. Pironio and S. Massar, Physical Review A **87**, 012336 (2013).

[9] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).

[10] U. Vazirani and T. Vidick, in *Proceedings of the forty-fourth annual ACM Symposium on Theory of Computing (STOC)* (2012) pp. 61–76.

[11] C. A. Miller and Y. Shi, J. ACM **63**, 33:1 (2016).

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

[13] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation," (2016), arXiv:1607.01796.

[14] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs," (2016), arXiv:1607.01797.

[15] R. Jain, C. A. Miller, and Y. Shi, "Parallel device-independent quantum key distribution," (2017), arXiv:1703.05426.

[16] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Transactions on Information Theory **57**, 5524 (2011).

[17] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick, SIAM Journal on Computing **40**, 848 (2011).

[18] N. Alon and J. H. Spencer, *The probabilistic method* (John Wiley & Sons, 2004).

[19] R. Bhatia, *Matrix Analysis* (Springer-Verlag, 1997).

[20] A. Winter, *Coding Theorems of Quantum Information Theory*, Ph.D. thesis, Universitat Bielfeld (1999).

[21] J. Katz and Y. Lindell, *Introduction to Modern Cryptography* (CRC Press, 2015).