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: June 14, 2017)

The field of device-independent quantum cryptography has seen enormous success in the past several years, including the achievement of universally composable security proofs for device-independent quantum key distribution (DI-QKD) and randomness expansion. 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 entirely self-contained.

PACS numbers:

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 random keys for herself, or to distribute random keys across distances with another party and then use these keys for secure information transmission. Quantum cryptography offers security against a computationally unlimited (and quantum-enabled) adversary.

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 exhibiting random behavior. The outputs of such devices cannot be fully predictable to an adversary, and therefore can be collected and processed by a classical user to obtain truly random bits, even when the devices themselves are not trusted. This idea has been used in multiple cryptographic contexts, including randomness expansion and amplification [1, 3], key distribution [2], 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 universal composability – i.e., proving security in the presence of quantum side information. 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].

Proofs of universal composability for device-independent random number generation have used tools specific to the quantum context, such as the reconstruction paradigm based on Trevisan's extractor [10], and inductive proofs based on quantum Renyi divergence [11–14]. Such proofs are long and mathematically complex. The most recent paper on the subject [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 multilayered and technically deep.

The goal of the current paper is provide a compact security proof for universal composability in the quantum context. 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 section II). The approach allows us to reduce security questions to more elementary questions about nonlocal games (where the advesary is included as a player). I have combined this idea with known techniques in the quantum information (mainly [16, 17]) to prove universal composability through elementary means.

The proof is self-contained, with results from other sources reproved rather than cited. The only assertions we take for granted are Azuma's inequality (see Theorem 7.2.1 in [18]) and Holder's inequality (see Corollary IV.2.6 in [19]).

Our main result is the informal theorem stated below (see Theorem IV.3 for a precise statement, and Figure 1 for the protocol). The result addresses private random number generation, where the goal is to use untrusted quantum devices and publically-known bits to produce secret bits. I am optimistic that the mirror adversary technique can be applied to other problems as well.

Theorem. (Informal) Suppose that two untrusted devices exhibit a Bell violation of $\delta > 0$ over N rounds. Then, $\Omega(N\delta^5)$ private randomness bits can be extracted from the outputs of the devices in polynomial time, using $O(N)$ bits of public randomness. The resulting private bits are secure against quantum side information.

* camiller@umd.edu

I. PRELIMINARIES.

Throughout the paper, a *register* D is a finite-dimensional Hilbert space, and a *state* ϕ of such a register is a density operator on V. If $D = D_1 \otimes D_2$, we will write ϕ^{D_1} for $\mathrm{Tr}_{D_2}\phi$. As a convenience, if X is an operator on D and Y is an operator on D_1, then the expression XY means $X(Y \otimes I_{D_2})$ and the expression YX means $(Y \otimes I_{D_2})X$.

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 POVMs 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 outputs $t_1, \ldots, t_N$ in sequence. In such a case, for any $u_1, \ldots, u_i$ and $t_1, \ldots, t_i$, 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) input alphabets $\mathcal{I}_1 \ldots, \mathcal{I}_r$ and output alphabets $\mathcal{O}_1, \ldots, \mathcal{O}_r$ (all finite sets), (2) a probability distribution p on $\mathcal{I} := \times_i \mathcal{I}_i$, and (3) a scoring function $L \colon \mathcal{I} \times \mathcal{O}_1 \times \ldots \times \mathcal{O}_n \to \mathbb{R}$. 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 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 all possible scores that can be achieved by quantum strategies.

Proposition I.1 *Let H be an n-player nonlocal game whose scoring function has range $[-C, C]$, 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*

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

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

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

Each variable $\overline{W}_i$ has range contained in $[-2C, 2C]$, and its expectation conditioned on $\overline{W}_1, \ldots, \overline{W}_n$ is zero. By Azuma's inequality, the probability that the event $\sum_{i=1}^N \overline{W}_i > \delta N$ occurs is no more than (4). The difference between $\sum_{i=1}^N \overline{W}_i$ and $\sum_{i=1}^N W_i$ is equal to the sum over $i \in 1, 2, \ldots, N$ of the expectations $E[W_i \mid W_{i-1} \cdots W_1]$, each of which cannot exceed $\omega(H)$, and thus 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).

II. THE MIRROR ADVERSARY.

If α is a quantum-classical state of a register QC, 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.

The mirror adversary technique begins with the observation that if the state QC was obtain by a C-valued measurement on a bipartite pure state QQ', then the pretty good measurement is essentially the adversary using precisely the same measurement in order to reconstruct C. This expressed by the following proposition.

Parameters:

- A 2-player Bell game G with alphabet size $n = 2^t$.
- A real number $\delta > 0$ (the degree of Bell violation).
- Positive integers N (the number of rounds), and K (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. The referee chooses a random affine automorphism[a] $\Psi : \mathbb{F}_{2^{Nt}} \to \mathbb{F}_{2^{Nt}}$ and computes
$$V := G \circ \Psi \circ F(\mathbf{s}), \tag{6}$$
where $F : (\mathbb{Z}/2^t\mathbb{Z})^N \to \mathbb{F}_{2^{Nt}}$ is a fixed bijection, and $G : \mathbb{F}_{2^{Nt}} \to \mathbb{F}_2^K$ is a fixed surjective $\mathbb{F}_2$-linear map (both chosen in advance).

[a] That is, a map $\mathbb{F}_{2^{Nt}} \to \mathbb{F}_{2^{Nt}}$ of the form $X \mapsto eX + f$, where $e \neq 0$.

FIG. 1. The random number generation protocol.

Proposition II.1 *Let Q, Q' be registers with a fixed isomorphism $Q \cong Q'$. Let ψ be a pure state of QQ' which symmetric under the interchange of Q and Q', and let α be the state of registers QC that arises from ψ by performing a measurement $\{R_c\}_{c \in C}$ on Q'. Then, the pretty good measurement induced by α on Q is isomorphic to $\{R_c\}$.*

Proof. Let $\rho = \psi^Q$. The state α is given by
$$\alpha = \sum_c |c\rangle\langle c| \otimes \sqrt{\rho} R_c \sqrt{\rho}. \tag{8}$$
And thus the pretty good measurement induced by α on Q is isomorphic to $\{\rho^{-1/2}\sqrt{\rho}R_c\sqrt{\rho}\rho^{-1/2}\} = \{R_c\}$. □

The pretty good measurement has the advantage that it is easy to compute, whereas finding the optimal measurement for guessing C from Q might be difficult. Moreover, as we will see further on in the proof, the pretty good measurement inherits the properties of the measurement was used to construct C, including the sequential measurement property discussed in the previous section.

The next proposition, which is a modification of a result from [16], is an expression of the fact that the pretty good measurement is almost optimal. It asserts that if the pretty good measurement is not much better than random at guessing C from Q, then C is nearly uniform with respect to Q. We state a version of the result that is more useful in the device-independent context, in that it includes an additional bit register which records whether a device-independent protocol has "aborted" or "succeeded."

Let Z denote a classical register with two basic states, *abort* and *succ*.

Proposition II.2 *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:*
$$R_{cz} = (\alpha^Q)^{-1/2} \alpha^Q_{cz} (\alpha^Q)^{1/2}, \tag{9}$$
$$R_z = (\alpha^Q)^{-1/2} \alpha^Q_z (\alpha^Q)^{1/2}. \tag{10}$$
Let $f = \mathrm{Tr}[\alpha^Q_{succ} R_{succ}]$ and
$$f' = \sum_c \mathrm{Tr}[\alpha^Q_{c,succ} R_{c,succ}]. \tag{11}$$
Then,
$$\left\| \alpha^{QC}_{succ} - \alpha^Q_{succ} \otimes U_C \right\|_1 \leq \sqrt{f' |C| - f}, \tag{12}$$
where U_C denotes the completely mixed state on C.

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 of the event that both $Z = succ$ and that an adversary who uses the pretty good measurement will guess $Z = succ$ and correctly guess the value of the register C. If $f' = f/|C|$ (that is, if the adversary's guess using the pretty good measurement is no better than random) then the term on the right side of (12) is equal to zero.

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

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

1. 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.

III. GUESSING GAMES.

The following is roughly the same as the "immunization" construction 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 $C > 0$. Then we define a new 3-player game G_C 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 $(-C)$ otherwise.

Proposition III.1 *For any Bell game G with alphabet size n,*

$$\omega(G_C) \leq 4\sqrt{n/C}. \tag{13}$$

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_C 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.

Note that 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

$$\delta_x := \sum_s \mathrm{Tr}(M_x^s \rho_x^s). \tag{14}$$

Note that if $\sum_x \delta_x > 1/C$, then (since a score of $-C$ 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 $\sum_x \delta_x \leq 1/C$.

By Proposition A.1, we have

$$\left\| \sum_s M_x^s \rho M_x^s - \rho \right\|_1 \leq \delta_x \tag{15}$$

for any x, y. Therefore if we let W_x denote the CPTP operator on A given by $X \mapsto \sum_s M_x^s \rho M_x^s$, we obtain the following distance inequalities for the states obtained by applying the maps W_x sequentially:

$$\|W_i W_{i-1} \cdots W_1(\rho) - \rho\|_1 \tag{16}$$

$$\leq \sum_{j=1}^{i} \|W_i W_{i-1} \cdots W_j(\rho) - W_{i-1} W_{i-2} \cdots W_{j+1}(\rho)\|_1$$

$$\leq \sum_{j=1}^{i} \|W_j(\rho) - \rho\|_1 \leq \sum_{j=1}^{i} 4\sqrt{\delta_j}. \tag{17}$$

(We have used the fact that $\|\cdot\|_1$ is non-increasing under CPTP maps in (17).)

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 (17), the state of the register AB is never more than trace distance $\sum_{j=1}^{i} 4\sqrt{\delta_j}$ 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

$$\omega(G, Y) \leq \sum_{j=1}^{n} 4\sqrt{\delta_j} \tag{18}$$

$$\tag{19}$$

which implies

$$\omega(G, Y) \leq 4\sqrt{n} \sqrt{\sum_{j=1}^{n} \delta_j}. \tag{20}$$

$$\tag{21}$$

Since we have assumed $\sum_x \delta_x \leq 1/C$, this yields the desired result. □

IV. SECURITY PROOF.

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

Proposition IV.1 *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,*

$$\mathbf{P}((\mathbf{S} = \mathbf{S}' \wedge succ \wedge succ') \leq e^{-\Omega(N\delta^5/n)}.$$

Proof. For any $C > 0$, if the three events on the left side of (23) all occur, then Alice and Bob have achieved an average score of at least δ at the game G_C^N using a sequential strategy. The probability of such a score is no more than

$$\exp(-N(\delta - 4\sqrt{n/C})^2/8C^2) \tag{22}$$

Setting $C = 64n/\delta^2$ yields the desired result.

Parameters:

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

1. Registers $ABA'B'$ are prepared in a symmetric pure state so that the state of AB is in 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 $\mathbb{F}_2^{Nt} \times (\mathbb{F}_2^{Nt} \setminus \{0\})$-valued registers Ψ, Ψ', so that for each register Z the corresponding primed register Z' is in a maximally entangled 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 computes a register V from S via Ψ (as in step 4 in Figure 1).
5. The adversary carries out step 3 herself, using the registers $A', B', \mathbf{X}', \mathbf{Y}'$ and the same 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 measures Ψ', and then computes V' from Ψ' and S' as in the previous step.

FIG. 3. The mirrored random number generation protocol.

Proposition IV.2 *The registers $\mathbf{V}, \mathbf{V}'$ at the conclusion of the process in Figure 3 satisfy*

$$\begin{aligned}&\mathbf{P}((\mathbf{V} = \mathbf{V}' \wedge succ \wedge succ')\\ &\leq e^{-\Omega(N\delta^5/n)} + 2^{-K}\mathbf{P}(succ \wedge succ').\end{aligned}$$

Proof. Note that for any distinct $\mathbf{r}_1, \mathbf{r}_2 \in (\mathbb{Z}/2^t\mathbb{Z})^N$, the probability that the random homomorphism in equation (6) from Figure 1 will map $\mathbf{r}_1, \mathbf{r}_2$ to the same element is exactly $1/\left|\mathbb{F}_2^K\right| = 2^{-K}$. Thus we have the following:

$$\begin{aligned}&\mathbf{P}((\Psi\mathbf{S} = \Psi\mathbf{S}') \wedge succ \wedge succ')\\ &= \mathbf{P}((\mathbf{S} = \mathbf{S}') \wedge succ \wedge succ')\\ &\quad + \mathbf{P}(\Psi\mathbf{S} = \Psi\mathbf{S}' \mid (\mathbf{S} \neq \mathbf{S}') \wedge succ \wedge succ'))\\ &\quad \cdot \mathbf{P}((\mathbf{S} \neq \mathbf{S}') \wedge succ \wedge succ')\\ &\leq e^{-\Omega(N\delta^5/n)} + 2^{-K} \cdot \mathbf{P}(succ \wedge succ'),\end{aligned}$$

as desired. □

By Proposition II.1, the register V' in Figure 3 is precisely the result of the adversary using a pretty good measurement in Figure 1 to recover in order to guess V. By applying Proposition II.2, we have the following.

Theorem IV.3 *Let ρ denote the state final state of the registers in Figure 1. Then,*

$$\left\|\rho_{succ}^{\mathbf{VXY\Psi E}} - U_{\mathbf{V}} \otimes \rho_{succ}^{\mathbf{XY\Psi E}}\right\|_1 \leq 2^{K-\Omega(N\delta^5/n)}. \quad \square$$

Note that if we fix δ, n and let $K = \lfloor cN \rfloor$ for some sufficiently small $c > 0$, the exponential on the right of (23) vanishes exponentially. Thus universally composable private random number generation (with a linear rate and negligible error term) is achieved.

Appendix A: Supplementary Proofs

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 A.1 *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

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

And, $\|P^z \alpha P^z - \sum_c P^c \alpha P^c\|_1 \leq \delta \leq \sqrt{\delta}$ 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 $\|\cdot\|_1$ is convex, and the square root function is concave. □

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

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

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

[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* (ACM, 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," 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).