Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model

S. Pironio,[1] Ll. Masanes,[2,3] A. Leverrier,[4,5] and A. Acín[2,6]

[1]*Laboratoire d'Information Quantique, Université Libre de Bruxelles (ULB), 1050 Bruxelles, Belgium*
[2]*ICFO-Institut de Ciencies Fotoniques, 08860 Castelldefels, Barcelona, Spain*
[3]*H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom*
[4]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[5]*INRIA Rocquencourt, Domaine de Voluceau, Boîte Postale 105, 78153 Le Chesnay Cedex, France*
[6]*ICREA-Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain*

(Received 9 November 2012; revised manuscript received 12 June 2013; published 9 August 2013; corrected 22 January 2014)

Device-independent quantum key distribution (DIQKD) is a formalism that supersedes traditional quantum key distribution, as its security does not rely on any detailed modeling of the internal working of the devices. This strong form of security is only possible using devices producing correlations that violate a Bell inequality. Full security proofs of DIQKD have recently been reported, but they tolerate zero or small amounts of noise and are restricted to protocols based on specific Bell inequalities. Here, we provide a security proof of DIQKD that is both more efficient and noise resistant, and also more general, as it applies to protocols based on arbitrary Bell inequalities and can be adapted to cover supraquantum eavesdroppers limited by the no-signaling principle only. It is formulated, however, in the bounded-quantum-storage model, where an upper bound on the adversary's quantum memory is *a priori* known. This condition is not a limitation at present, since the best existing quantum memories have very short coherence times.

DOI: 10.1103/PhysRevX.3.031007 Subject Areas: Quantum Physics, Quantum Information

I. INTRODUCTION

Quantum key distribution is the art of distilling a secret key between two distant parties, Alice and Bob, who have access to an untrusted quantum channel [1]. In this scenario, one typically assumes that the equipment in Alice and Bob's labs can be trusted and, moreover, that its behavior is accurately described by a given theoretical model. Unfortunately, this assumption is so strong that it is often not justified in practice [2]. In particular, many loopholes can be exploited by an eavesdropper to get around the usual security proofs: For instance, the state preparation might be imperfect [3] or the eavesdropper might perform a blinding attack to take control of the detectors at a distance [4].

One way around such problems consists of exhaustively listing all the potential mismatches between the theoretical model and the real implementation and taking care of each one of them individually. However, this approach is dubious as it is impossible to be sure that all loopholes have really been addressed. Another, more promising approach is inspired by the recent framework of device-independent quantum information processing [5,6]. Here, the idea is that if Alice and Bob are able to experimentally violate a Bell inequality [7], it means that their data exhibit intrinsic randomness as well as secrecy [8,9], independently of the internal operation of the devices [5]. In recent years, this framework has been used to prove the security of device-independent key distribution [10–17]; to certify randomness expansion [18–22] and the self-testing of quantum computers [23] and states [24,25]; and to guarantee the presence of entanglement [26].

In the present work, we focus on the cryptographic task of key distribution, which has been the subject of many very recent developments. Until recently, security proofs were restricted to scenarios where Alice and Bob have access to a pair of memoryless devices or n independent pairs of devices, thus ensuring that the measurements inside their own labs were causally disconnected [10] or commuting [12,13]. This restriction is reminiscent of the notion of collective attacks in standard quantum key distribution, where some independence assumption is required. Ideally, one would like a protocol where only one device is required per party and for which no assumption is needed for the device. Achieving this improvement is indeed the motivation for doing device-independent cryptography in the first place.

Recent results have been able to address this issue. In Ref. [14], the authors introduced a protocol based on the chained Bell inequality [27] and established its security against arbitrary adversaries. The protocol, however, only produces a single secret bit and does not tolerate any noise. In Refs. [15,16], the authors proved a strong converse of Tsirelson's optimality result for the Clauser-Horne-Shimony-Holt (CHSH) game, based on the CHSH inequality [28]: The only way to use quantum resources to win the game as predicted by Tsirelson's bound is to use a strategy close to the optimal one for independent and identically distributed states, that is, to apply the optimal measurements on copies of a two-qubit maximally entangled state. This theorem provides a security proof for device-independent quantum key distribution (DIQKD) based on the CHSH inequality. Unfortunately, the security proof also does not seem resistant to any constant amount of noise. While this work was completed, Vazirani and Vidick gave a universally composable security proof of DIQKD against arbitrary attacks [17]. Their protocol, based again on the CHSH inequality, is both reasonably efficient (the key length scales linearly with the number of measurements) and tolerant to a constant fraction of noise. A drawback, however, is that the maximum amount of noise tolerated is of the order of 1%, significantly lower than the bounds obtained for protocols using n pairs of devices.

In the present paper, we present a security proof that (i) works for only two devices, that is, does not require commuting measurements or memoryless devices, (ii) can be applied to generic DIQKD protocols based on arbitrary Bell inequalities, and (iii) has the same efficiency and tolerance to noise as previous proofs using memoryless devices.

All these nice properties, however, come at the price of working in the so-called bounded-quantum-storage (BQS) model, where one assumes that an upper bound is known for the quantum memory of the adversary [29,30]. While this assumption might appear as a strong limitation, we point out that an even stronger requirement, corresponding to the situation where the bound on the quantum memory is zero, can actually be easily enforced in any realistic implementation by delaying the reconciliation process, since the best existing quantum memories have very short coherence times [31]. Another advantage of our general framework is that it can also provide security beyond quantum theory, that is, against eavesdroppers that are only limited by the no-signaling principle.

The outline of the paper is the following. We first give a brief reminder of the relation between nonlocality, that is, violation of a Bell inequality, and randomness, as well as a short description of the BQS model. We then describe the protocol of quantum key distribution and present its secret key rate. We prove the security of the protocol in the BQS model. We conclude by briefly comparing our results with the existing security proofs and discussing some rather natural follow-up questions.

II. NONLOCALITY AND RANDOMNESS

In the following, we consider a bipartite scenario where Alice and Bob input random variables X and Y in their respective devices and obtain classical outputs A and B, respectively. We denote λ_A, λ_B, λ_X, and λ_Y the sizes of the alphabets of A, B, X, and Y, respectively. Moreover, we denote by $P(a, b|x, y)$ the probability of getting the specific results $A = a$ and $B = b$ when the inputs are $X = x$ and $Y = y$, and by $P(A, B|X, Y)$ the vector with components $P(a, b|x, y)$.

A Bell inequality can be written as

$$I[P(A,B|X,Y)] := \sum_{a,b,x,y} \beta(a,b,x,y) P(a,b|x,y) \leq I_{\text{cl}}, \quad (1)$$

where I_{cl} is the classical upper bound. To any such Bell inequality, one can associate a bound on the randomness of the output A, given the input $X = x$ through a function τ_x such that

$$P(a|x) \leq \tau_x(I[P(A,B|X,Y)]) \quad \text{for all } a \in \lambda_A. \quad (2)$$

Such a function can be computed using the techniques given in Ref. [32], as explained in Ref. [19]. Without loss of generality, this function can be assumed to be monotonically nonincreasing and such that $-\log[\tau_x(\cdot)]$ is convex. (Throughout this article, all log functions are in base 2.)

For simplicity, we consider the case where there exists an input-independent bound, i.e., a function τ such that $\tau(I) = \tau_x(I)$ for all $x \in \lambda_X$. Examples of Bell inequalities satisfying this property are the CHSH inequality [28], the chained inequality [27], and the Collins-Gisin-Linden-Massar-Popescu inequality [33]. Our results, however, can easily be generalized to cover the case of input-dependent bounds.

III. BOUNDED-QUANTUM-STORAGE MODEL

The bounded-storage model was first introduced in the classical setting by Maurer [34], who considered a key expansion scenario where the key is obtained from a short secret key initially shared by the legitimate parties and a large amount of randomness, which is public but only available for a short time. The adversary, who does not know the initial key, needs to store all the public randomness in order to learn the final key, a task impossible to perform when her memory is bounded.

Such a model can be translated in the quantum regime, where restrictions on the size of a quantum memory appear quite reasonable, given present-day technology. In addition to their limited size, quantum memories also suffer from a relatively short coherence time, after which they essentially become classical memories. Depending on which aspect one focuses on, two different models can be considered: In the bounded-quantum-storage model [29,30], one assumes that after a certain waiting time T, an upper bound on the size (expressed in qubits) of the quantum memory Q of the adversary applies. We denote this bound by $H_0(Q) := \log_2 \text{rank}(\rho_Q)$, the max-entropy of the quantum system Q held by the adversary. In the more realistic noisy-storage model [35,36], one assumes that after the waiting time T, the quantum memory Q of the adversary is degraded by the noise, which is represented by a certain quantum channel. Apart from these restrictions on the quantum memory Q, the adversary can store an unlimited amount of classical information E in both models.

In this work, we study the BQS model. The main advantage of postulating a bound of the size of the quantum memory of the adversary is that it allows us to treat her side information as classical and simply take into account her quantum features through $H_0(Q)$. Indeed, consider the scenario where an adversary tries to guess a key K from classical information denoted by E and her quantum memory Q, possibly correlated to E. This correlation scenario is described by a classical-classical-quantum state $\rho_{KEQ} = \sum_{k,e} P(k,e)|k\rangle\langle k| \otimes |e\rangle\langle e| \otimes \rho_Q^{ke}$. Then, the chain rule for min-entropy [37], together with the operational interpretation of the guessing probability P_{guess} established in Ref. [38], implies that

$$P_{\text{guess}}(K|EQ) \leq P_{\text{guess}}(K|E) \cdot 2^{H_0(Q)}, \tag{3}$$

where $P_{\text{guess}}(K|E) := \sum_e \max_k P(k,e)$ and $P_{\text{guess}}(K|EQ) := \max_{M_k} \sum_{k \in K} P(k) \operatorname{tr}(M_k \rho_{EQ})$, where $\{M_k\}_{k\in K}$ defines a measurement on EQ. This identity allows us to bound the guessing probability, given the classical-quantum side information EQ, by simply bounding a purely classical guessing probability.

IV. DESCRIPTION OF THE PROTOCOL

The DIQKD protocol that we consider in this paper is very general in the sense that it is compatible with arbitrary Bell inequalities, in particular, with the various examples of Bell inequalities mentioned above. Our protocol consists of four steps: measurements, estimation of the Bell violation, error correction, and privacy amplification. We denote by n the number of times each device is used during the protocol.

(1) *Measurements.*—Alice and Bob, respectively, generate the random variables $U_j, V_j \in \{0,1\}$ with distribution $\Pr\{U_j = 1\} = \Pr\{V_j = 1\} = q = n^{-1/8}$ for $j = 1, \ldots, n$. If $U_j = 0$, then Alice measures round j with input 0, obtaining outcome A_j. If $U_j = 1$, then Alice generates X_j with uniform distribution $P(x_j) = 1/\lambda_X$ and measures round j with input X_j, obtaining outcome A_j. Bob does the analog with V_j, input Y_j, and outcome B_j. In other words, events where $U_j = V_j = 0$ are used to establish a raw key, while events where $U_j = V_j = 1$ are used to test the Bell inequality and guarantee that a secret key can indeed be extracted from the raw key.

(2) *Estimation.*—Alice and Bob publish (u_j, v_j) for all j and discard the data corresponding to the rounds with $u_j \neq v_j$. The data corresponding to the m postselected rounds $(u_j, a_j, b_j, x_j, y_j)$ with $v_j = u_j$ are relabeled with the index $i = 1, \ldots, m$, keeping the time order. The data corresponding to the rounds of the set $\mathcal{E} := \{i | U_i = V_i = 1\}$ are also published and used to estimate the Bell-inequality violation. More specifically, Alice and Bob can use the public data to compute the following quantity:

$$I_{\text{est}} := \frac{\lambda_X \lambda_Y}{|\mathcal{E}|} \sum_{i \in \mathcal{E}} \beta(a_i, b_i, x_i, y_i). \tag{4}$$

The data of the rounds not in $\mathcal{E}$ constitute the raw keys of Alice $R = (A_i)_{i \notin \mathcal{E}}$ and Bob $S = (B_i)_{i \notin \mathcal{E}}$.

(3) *Error correction.*—Alice and Bob publish n_C bits in order to correct Bob's errors $S \rightarrow S'$. In the following, we consider the worst case, where all the messages published within the error-correction step are a function θ of Alice's raw key R. This public communication is denoted $C := \theta(R)$. For sufficiently large n_C, all errors are corrected as $S' = R$ with high probability. Note that some of the published bits are used to estimate how many more bits need to be published for a successful error correction. For large n, publishing $n_C \approx nH(A|B)$ bits is enough. For more details about the functioning of error correction, we refer to Ref. [37].

(4) *Privacy amplification.*—Alice generates and publishes a two-universal [39] random function F that maps R onto an n_K-bit string $K = F(R)$. The number n_K depends on the published information and on the bound on the quantum memory size $H_0(Q)$ as

$$n_K := \max\Big\{0, \Big\lfloor -m \log_2 \tau\Big(\frac{|\mathcal{E}|}{m}(n^{1/8} - 1)^2 I_{\text{est}} - n^{-1/8}\Big) - n_C - H_0(Q) - 2|\mathcal{E}| \log_2(\lambda_A \lambda_B) - \sqrt{n}\Big\rfloor\Big\}, \tag{5}$$

where $\lfloor \gamma \rfloor$ is the largest integer not bigger than γ. Alice and Bob then compute $[F(R), F(S')]$, obtaining two copies of the secret key.

As we already pointed out, our security proof assumes a bound $H_0(Q)$ on the quantum memory of the adversary after a certain waiting time T. The honest parties should therefore implement the protocol in two steps: (i) They receive the quantum systems from the source and perform the measurements, and (ii) a time T later, they perform the rest of the protocol involving the public communication for the estimation, error correction, and privacy amplification. In particular, according to current and near-future technology, by taking T of the order of a few minutes [31], the state stored in the memory has completely decohered, and we can enforce a situation where $H_0(Q) = 0$, which corresponds to the case of an eavesdropper possessing only classical-side information. In that case, the max-entropy $H_0(Q)$ can be taken equal to zero in Eq. (5).

More generally, from the discussion in Sec. III, in order to deal with an adversary whose quantum memory is bounded by $H_0(Q)$, it is sufficient to consider the case of purely classical-side information and to subtract the quantity $H_0(Q)$ from the final key size. In the remainder of this paper, we will therefore consider for simplicity the case when $H_0(Q) = 0$ in Eq. (5).

V. SECURITY AND EFFICIENCY

To prove security, we will not make any assumption on the behavior of the devices of Alice and Bob, except that they do not broadcast information about the inputs and outputs toward the adversary (a condition without which there is no hope of ever establishing any secret). Modulo this requirement, we can even assume for simplicity that the devices have been built by the adversary. The eavesdropper could, in particular, hold quantum systems that are entangled with the systems in the users' devices. However, our proof of security will hold under the condition that the eavesdropper cannot store this quantum information past the measurement step of the protocol. After this step, she should thus perform a measurement M on her quantum system, which would give her some classical information E about the behavior of Alice and Bob's devices. But, since until this point no public communication has been exchanged between Alice and Bob, we can also assume that the eavesdropper has performed her measurement before the users received their devices from the source. The fact that our proof of security holds independently of the behavior of the devices then implies that it holds independently of the prior classical information E that Eve holds on the devices, and we can thus forget E in the following.

At the end of the protocol, Alice holds the secret key K and Eve holds the information published in the estimation step $W = [(U_1, \ldots, U_m), (A_i, B_i, X_i, Y_i)_{i\in\mathcal{E}}]$, in the error-correction step $C = \theta(R)$, and in the privacy-amplification step F. Let $P(k, f, w, c)$ be the probability distribution for these random variables.

We say that K is an ideal secret key if it is uniformly distributed and uncorrelated with all the rest:

$$P(k, f, w, c) = 2^{-n_K(w)} P(f, w, c) \quad \text{for all } k, f, w, c. \tag{6}$$

Note that since $\mathcal{E}$ and I_{est} are functions of w, so is n_K. It is unrealistic to expect that a protocol can generate an ideal secret key. Instead, what we demand is that the distribution generated by the above protocol be indistinguishable from an ideal secret key. It is known that the optimal success probability when discriminating between the two distributions is [37]

$$p_{\text{succ}} = \frac{1}{2} + \frac{1}{4} \sum_{k,f,w,c} |P(k, f, w, c) - 2^{n_K(w)} P(f, w, c)|. \tag{7}$$

The main result of this work (see the theorem below) is to show that

$$p_{\text{succ}} \le \tfrac{1}{2} + \gamma \mathbf{e}^{-\beta_0^2 n^{1/8}}, \tag{8}$$

where $\beta_0 = \sqrt{8}\lambda_X \lambda_Y \max_{a,b,x,y}|\beta(a, b, x, y)|$ and γ is a constant. For large n, the success probability (8) tends to $1/2$, which makes the optimal discriminating strategy no better than a random guess.

Let us now discuss the efficiency of the protocol in the asymptotic limit, where n tends to infinity. For large n, one expects

$$m \approx n \Pr\{U = V\} \approx n - 2n^{7/8},$$
$$|\mathcal{E}| \approx n \Pr\{U = V = 1\} \approx n^{3/4},$$

with high probability. These scalings give an asymptotic secret key rate R_K of

$$R_K := \lim_{n\to\infty} \frac{n_K}{n} = \log \frac{1}{\tau(I_{\text{est}})} - H(A|B). \tag{9}$$

This rate is the same as the one given in Ref. [12] for memoryless devices but with security against full quantum adversaries. Note that as soon as the bound $\tau(I[P(A, B|X, Y)])$ is nontrivial, that is, strictly less than 1, there exists a regime for the noise where the secret key rate is positive asymptotically.

In the case of the CHSH inequality $\beta(a,b,x,y) = (-1)^{a\oplus b\oplus x\cdot y}$, we define τ_{QM} and τ_{NS} such that $p(a|x) \le \tau_{\text{QM}}(I[P(A, B|X, Y)])$ holds against an adversary limited by quantum theory and $p(a|x) \le \tau_{\text{NS}}(I[P(A, B|X, Y)])$ holds against an adversary limited by the no-signaling principle. The specific values of these functions were derived in Refs. [12,19]:

$$\tau_{\text{QM}}(I) = \frac{1}{2}\left(1 + \sqrt{2 - \frac{I^2}{4}}\right), \tag{10}$$

$$\tau_{\text{NS}}(I) = \frac{1}{4} - \frac{I}{4}. \tag{11}$$

In Fig. 1, we plot the asymptotic secret key rate R_K as a function of the visibility of the Werner state $\rho_\nu = \nu|\phi\rangle\langle\phi| + (1 - \nu)\mathbb{1}/4$ shared by Alice and Bob. For this state, the asymptotic value of I_{est} is $2\sqrt{2}\nu$ and the quantum-bit error rate is $q := \frac{1-\nu}{2}$, meaning that the conditional entropy $H(A|B)$ is given by the binary entropy of q, namely, $h(q) := -q \log q - (1 - q) \log(1 - q)$.

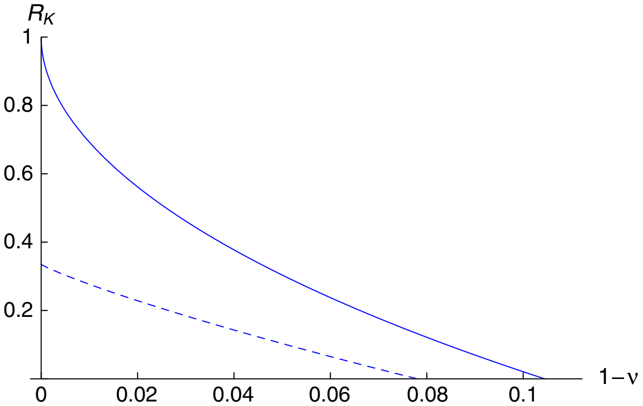

FIG. 1. Asymptotic secret key rate R_K vs noise $1 - \nu$ for the CHSH protocol and a state $\rho_\nu = \nu|\phi\rangle\langle\phi| + (1 - \nu)\mathbb{1}/4$, where $|\phi\rangle$ is maximally entangled. The upper curve corresponds to a quantum adversary, while the lower one considers an adversary only limited by the no-signaling principle.

VI. PROOF

We now proceed with a detailed security proof for the protocol described above. Before we present and prove our main result, which is an explicit bound on p_{succ}, we need three technical lemmas.

Let us introduce a more compact notation:

$$t_i := \begin{cases} a_i & \text{if } i \notin \mathcal{E} \\ (a_i, b_i) & \text{if } i \in \mathcal{E}, \end{cases} \tag{12}$$

$$z_i := \begin{cases} u_i & \text{if } i \notin \mathcal{E} \\ (u_i, x_i, y_i) & \text{if } i \in \mathcal{E} \end{cases} \tag{13}$$

for $i = 1, \ldots, m$. Variables with superindex i represent the chain of variables associated with time steps equal to or earlier than i, that is, $t^i = (t_1, t_2, \ldots, t_i)$. Recall that the information made public in the estimation step is $w = [u^m, (a_i, b_i, x_i, y_i)_{i\in\mathcal{E}}]$ and that the raw key is $r = (a_i)_{i\notin\mathcal{E}}$. Let $g = (a_i, b_i)_{i\in\mathcal{E}}$ and note that $t^m = (r, g)$ and $w = (z^m, g)$.

Lemma 1.—The no-signaling constraints imposed by the causal structure of the protocol imply

$$P(t^m|z^m) \leq \tau^m(\bar{I}[t^m, z^m]) \tag{14}$$

for all (t^m, z^m), where τ^m refers to the mth power of τ and

$$\bar{I}[t^m, z^m] := \frac{1}{m}\sum_{i=1}^{m} I[P(A_i, B_i|X_i, Y_i, t^{i-1}, z^{i-1})]. \tag{15}$$

Note that above, in $P(A_i, B_i|X_i, Y_i, t^{i-1}, z^{i-1})$, the symbols A_i, B_i, X_i, and Y_i are uppercase, while t^{i-1} and z^{i-1} are lowercase, meaning that $P(A_i, B_i|X_i, Y_i, t^{i-1}, z^{i-1})$ is the vector with components $P(a_i, b_i|x_i, y_i, t^{i-1}, z^{i-1})$ for all values of a_i, b_i, x_i, and y_i but fixed t^{i-1} and z^{i-1}.

Proof: This proof is based on an argument introduced in Ref. [19]. A useful observation is that bound (2) implies

$$P(a, b|x, y) \leq \tau(I[P(A, B|X, Y)]) \quad \text{for all } a, b, x, y. \tag{16}$$

The following chain of equalities and inequalities follows from the Bayes rule, no signaling to the past, bounds (2) and (16), and the concavity of the function $\log[\tau(\cdot)]$:

$$\begin{aligned} P(t^m|z^m) &= P(t_1|z^m)P(t_2, t_3, \ldots|z^m, t_1) \\ &= P(t_1|z^1)P(t_2, t_3, \ldots|z^m, t_1) \\ &= \prod_{i=1}^{m} P(t_i|z^i, t^{i-1}) \\ &\leq \prod_{i=1}^{m} \tau(I[P(A_i, B_i|X_i, Y_i, z^{i-1}, t^{i-1})]) \\ &\leq \tau^m(\bar{I}[t^m, z^m]). \end{aligned} \tag{17}$$

□

Lemma 2.—The numbers $|\mathcal{E}|$, I_{est}, and $\bar{I}$ are functions of the random variable (T^m, Z^m) and satisfy

$$\Pr\left\{\bar{I} \leq \frac{|\mathcal{E}| I_{\text{est}}}{m \Pr\{U=1|U=V\}} - n^{-1/8}\right\} \leq \exp(-m n^{-3/4} \beta_0^{-2}), \tag{18}$$

where $\beta_0 = \sqrt{8}\lambda_X\lambda_Y \max_{a,b,x,y}|\beta(a, b, x, y)|$.

[Here, a comment is in order. Actually, $\bar{I}$ is not only a function of (T^m, Z^m) but also depends on the global probability distribution $P(T^m, Z^m)$. But, we think of this distribution as given, fixed, and unknown. This dependence prevents the straight generalization of the results in this paper to a quantum adversary.]

Proof: The function

$$\eta(t, z) := \begin{cases} 0 & \text{if } u = 0 \\ \frac{\beta(a,b,x,y)}{P(x,y)\Pr\{U=1|U=V\}} & \text{if } u = 1 \end{cases}$$

satisfies

$$\sum_{i=1}^{m} \eta[t_i, z_i] = \frac{I_{\text{est}}[t^m, z^m]|\mathcal{E}|}{\Pr\{U = 1|U = V\}} \tag{19}$$

and

$$\mathbb{E}[\eta(T_i, Z_i)|t^{i-1}, z^{i-1}] = I[P(A_i, B_i|X_i, Y_i, t^{i-1}, z^{i-1})] \tag{20}$$

for all i. Consider the sequence of functions of (t^m, z^m) defined by

$$\alpha_l(t^l, z^l) = \sum_{i=1}^{l} \eta(t_i, z_i) - \mathbb{E}[\eta(T_i, Z_i)|t^{i-1}, z^{i-1}] \tag{21}$$

for $l = 1, \ldots, m$. The fact that

$$\mathbb{E}[\alpha_l(T^l, Z^l)|t^{l-1}, z^{l-1}] = \alpha_{l-1}(t^{l-1}, z^{l-1}) \tag{22}$$

implies that the sequence of random variables $\alpha_l(T^l, Z^l)$ is a martingale [40] with respect to the sequence (T_l, Z_l). Also, using the fact that $P(x, y) = (\lambda_X\lambda_Y)^{-1}$ and $\Pr\{U=1|U=V\} = q^2/[q^2 + (1-q)^2] \geq q^2$, the differences

$$\begin{aligned} &|\alpha_l(t^l, z^l) - \alpha_{l-1}(t^{l-1}, z^{l-1})| \\ &\quad \leq 2\max_{t,z}|\eta(t, z)| \leq \frac{2\max_{a,b,x,y}|\beta(a, b, x, y)|}{(\lambda_X\lambda_Y)^{-1}q^2} =: \nu \end{aligned} \tag{23}$$

are bounded for all values of (t^m, z^m). Constraints (22) and (23) constitute the premises for Azuma's inequality [40]

$$\Pr\{\alpha_l(T^l, Z^l) \geq l\mu\} \leq \exp\left(\frac{-(l\mu)^2}{2l\nu^2}\right) \tag{24}$$

for any $\mu > 0$. Using Eqs. (19)–(21), we obtain

$$\begin{aligned}\bar{I}[t^m, z^m] &= \frac{1}{m}\sum_{i=1}^{m} I[P(A_i, B_i|X_i, Y_i, z^{i-1}, t^{i-1})]\\ &= \frac{1}{m}\left(\sum_{i=1}^{m}\eta[t_i, z_i] - \alpha_m(t^m, z^m)\right)\\ &= \frac{1}{m}\left(\frac{|\mathcal{E}|I_{\mathrm{est}}}{\Pr\{U = 1|U = V\}} - \alpha_m(t^m, z^m)\right),\end{aligned}$$

and setting $\mu = q = n^{-1/8}$ gives Eq. (18). □

Lemma 3.—There is a good event $\mathcal{G}$ with probability

$$P(\mathcal{G}) \geq 1 - 3\exp(-mn^{-3/4}\beta_0^{-2}) - (\lambda_A\lambda_B)^{-|\mathcal{E}|}, \tag{25}$$

such that

$$P(r|w, \mathcal{G}) \leq 2(\lambda_A\lambda_B)^{2|\mathcal{E}|}\tau^m\left(\frac{|\mathcal{E}|I_{\mathrm{est}}(w)}{m\Pr\{U = 1|U = V\}} - n^{-1/8}\right) \tag{26}$$

for all w such that $P(w|\mathcal{G}) > 0$.

Proof: This proof uses a trick introduced in Ref. [21]. The values of (t^m, z^m) in the set

$$\mathcal{G}_1 := \left\{(t^m, z^m)|\bar{I} \geq \frac{|\mathcal{E}|I_{\mathrm{est}}}{m\Pr\{U = 1|U = V\}} - n^{-1/8}\right\} \tag{27}$$

are the good ones, since Alice and Bob correctly lower bound $\bar{I}$ (and hence n_K) from the values $|\mathcal{E}|$ and I_{est} determined in the estimation step. In the condition defining $\mathcal{G}_1$ above, every symbol is a constant except for $\bar{I}$, $|\mathcal{E}|$, and I_{est}, which are functions of (t^m, z^m). Note that $\bar{I}$ also depends on the global distribution $P(t^m, z^m)$, which prevents the generalization of these results to the case of quantum adversary. Fortunately, according to Lemma 2, the probability of $\mathcal{G}_1$ is large:

$$P(\text{not } \mathcal{G}_1) < \exp(-mn^{-3/4}\beta_0^{-2}). \tag{28}$$

Note the abuse of notation $P(\mathcal{G}_1) = \Pr\{(T^m, Z^m) \in \mathcal{G}_1\}$. Define the set

$$\mathcal{G}_2 := \{w|P(\mathcal{G}_1|w) \geq 1/2\}, \tag{29}$$

and note that $P(\text{not } \mathcal{G}_1|\text{not } \mathcal{G}_2) > 1/2$. Using this bound and $P(\text{not}\,\mathcal{G}_1) \geq P(\text{not}\,\mathcal{G}_1|\text{not}\,\mathcal{G}_2)P(\text{not}\,\mathcal{G}_2)$, we obtain $P(\text{not}\,\mathcal{G}_2) < 2P(\text{not}\,\mathcal{G}_1)$.

Recall $G = (A_i, B_i)_{i\in\mathcal{E}}$ and note that $T^m = (R, G)$ and $W = (Z^m, G)$. Define the set

$$\mathcal{G}_3 := \{(g, z^m)|P(g|z^m) \geq (\lambda_A\lambda_B)^{-2|\mathcal{E}|}\}, \tag{30}$$

and note that

$$P(\text{not } \mathcal{G}_3) = \sum_{(g,z^m)\notin\mathcal{G}_3} P(z^m)P(g|z^m) < \sum_{g,z^m} P(z^m)(\lambda_A\lambda_B)^{-2|\mathcal{E}|} \tag{31}$$

where we have used $\sum_g 1 = (\lambda_A\lambda_B)^{|\mathcal{E}|}$. The good event mentioned in the statement of this lemma is $\mathcal{G} = (\mathcal{G}_1 \text{ and } \mathcal{G}_2 \text{ and } \mathcal{G}_3)$ and has probability $P(\mathcal{G}) \geq 1 - P(\text{not}\,\mathcal{G}_1) - P(\text{not}\,\mathcal{G}_2) - P(\text{not}\,\mathcal{G}_3)$, as in Eq. (25).

We assume $(g, z^m) \in \mathcal{G}_2 \cap \mathcal{G}_3$, since it is a premise of the lemma. If $(r, g, z^m) \notin \mathcal{G}_1$, then $P(r|g, z^m, \mathcal{G}_1) = 0$. Hence, the nontrivial case happens for $(r, g, z^m) \in \mathcal{G}_1$, which we assume in what follows. Using the Bayes rule, the definitions of $\mathcal{G}_2$ and $\mathcal{G}_3$, Lemma 1, and Eq. (27), we obtain

$$\begin{aligned}&P(r|g, z^m, \mathcal{G}_1)\\ &\quad\leq \frac{P(r|g, z^m)}{P(\mathcal{G}_1|g, z^m)} \leq \frac{P(r, g|z^m)}{P(\mathcal{G}_1|g, z^m)P(g|z^m)}\\ &\quad\leq 2(\lambda_A\lambda_B)^{2|\mathcal{E}|}\tau^m(\bar{I}[r, g, z^m])\\ &\quad\leq 2(\lambda_A\lambda_B)^{2|\mathcal{E}|}\tau^m\left(\frac{|\mathcal{E}|I_{\mathrm{est}}(g, z^m)}{m\Pr\{U = 1|U = V\}} - n^{-1/8}\right),\end{aligned} \tag{32}$$

which shows the lemma. □

Theorem.—The distance between the secret key generated by the protocol and an ideal key is

$$\begin{aligned}&\sum_{k,f,w,c} |P(k, f, w, c) - 2^{-n_K(w)}P(f, w, c)|\\ &\quad\leq 2^{(1-n^{1/2})/2} + 6\mathbf{e}^{-mn^{-3/4}\beta_0^{-2}} + 2(\lambda_A\lambda_B)^{-|\mathcal{E}|}.\end{aligned}$$

Proof: Using definitions (5) and (A2), Lemma 3, and $\sum_c 1 = 2^{n_C}$, we obtain

$$\begin{aligned}&P_{\mathrm{guess}}(R|C; w, \mathcal{G})\\ &\quad= \sum_c \max_r P(r, c|w, \mathcal{G}) = \sum_c \max_{\substack{r\\ \theta(r)=c}} P(r|w, \mathcal{G})\\ &\quad\leq \sum_c 2(\lambda_A\lambda_B)^{2|\mathcal{E}|}\tau^m\left(\frac{|\mathcal{E}|I_{\mathrm{est}}(g)}{m\Pr\{U = 1|U = V\}} - n^{-1/8}\right),\\ &\quad= 2^{1-n_K(g)-\sqrt{n}}.\end{aligned}$$

The symbol $P_{\mathrm{guess}}(R|C; w, \mathcal{G})$ denotes the knowledge of R with respect to C (see the Appendix) when the statistics is conditioned on the events $W = w$ and $\mathcal{G}$. Next, we use the identity

$$P(t^m, z^m) = P(\mathcal{G})P(t^m, z^m|\mathcal{G}) + P(\text{not } \mathcal{G})P(t^m, z^m|\text{not } \mathcal{G}) \tag{33}$$

with the event $\mathcal{G}$ introduced in Lemma 3. Noticing that (K, F, W, C) is a function of (T^m, Z^m, F), using Eq. (33), the triangular inequality, and Lemma 4, we see that

$$\begin{aligned}\sum_{k,f,w,c}|P(k,f,w,c)-2^{-n_K(w)}P(f,w,c)| &\leq \sum_{k,f,w,c}|P(k,f,w,c|\mathcal{G})-2^{-n_K(w)}P(f,w,c|\mathcal{G})|+2P(\text{not }\mathcal{G})\\ &\leq \sum_{k,f,w,c}P(w|\mathcal{G})|P(k,f,c|w,\mathcal{G})-2^{-n_K(w)}P(f,c|w,\mathcal{G})|+2P(\text{not }\mathcal{G})\\ &\leq \sum_{w}P(w|\mathcal{G})\sqrt{2^{n_K(w)}P_{\text{guess}}(R|C;w,\mathcal{G})}+2P(\text{not }\mathcal{G})\\ &\leq \sum_{w}P(w|\mathcal{G})2^{(1-n^{1/2})/2}+2P(\text{not }\mathcal{G})\\ &= 2^{(1-n^{1/2})/2}+6\exp(-mn^{-3/4}\beta_0^{-2})+2(\lambda_A\lambda_B)^{-|\mathcal{E}|},\end{aligned}$$

which concludes the proof. □

VII. CONCLUSIONS

In this work, we provide a novel security proof for DIQKD. Contrary to most of the existing proofs, it applies to the situation in which Alice and Bob generate the raw key using two devices. In particular, it does not need to assume that the devices are memoryless or, equivalently, that each raw-key symbol is generated using a different device. While there exist other recent proofs that also work without this assumption, they tolerate zero [14–16] or rather small amounts of noise [17]. Another important feature of our proof is that it can also be applied to no-signaling supraquantum eavesdroppers. All these advantages come at the price of working in the bounded-storage model, where a bound on the size of Eve's quantum memory is assumed to be available. This model is actually a relaxation of a scenario where Eve does not have access to a long-term quantum memory, and, therefore, effectively she cannot store quantum information. While these features may at first be considered a strong assumption, it is a very realistic assumption, taking into account current technology. An interesting follow-up question would be to see whether our technique could be adapted to the noisy-storage model [35,36].

Another natural open question is to understand how assumptions on the memory can be completely removed within the framework presented here, or alternatively how the other existing proofs [14–17] could be improved to tolerate realistic noise rates. In the case of no-signaling eavesdroppers, there is some evidence suggesting that the fact that Eve can store information and delay her measurement prevents any form of privacy amplification between the honest parties [41]. However, the recent results of Ref. [17] imply that privacy amplification is indeed possible against quantum eavesdroppers. A good understanding of privacy amplification in the device-independent quantum scenario is probably the missing ingredient to get robust and practical fully device-independent security proofs.

ACKNOWLEDGMENTS

We acknowledge useful discussions with Serge Massar. This work is supported by the ERC SG PERCENT and NLST, by the EU Projects Q-Essence and QCS, by the CHIST-ERA DIQIP Project, by the Spanish FIS2010-14830 Projects, by the SNF through the National Centre of Competence in Research "Quantum Science and Technology," by the CNRS through the PEPS ICQ2013 CCQD, by CatalunyaCaixa, by the Interuniversity Attraction Poles Photonics@be Programme (Belgian Science Policy), by the Brussels-Capital Region through a BB2B Grant, and from the FRS-FNRS under Project DIQIP. Financial support was also provided by EU ERC Advanced Grant No. NLST (PHYS RQ8784), the EU Qessence project, and the Templeton Foundation.

APPENDIX

A random function $F:\mathcal{R}\rightarrow\{0,1\}^n$ is two-universal [39] if

$$\Pr\{F(r)=F(r')\}\leq 2^{-n}$$

for all $r, r'\in\mathcal{R}$, with $r\neq r'$. The following is a simple extension of the main result in Ref. [39].

Lemma 4.—Let R and E be two (possibly correlated) random variables, where R takes values in the set $\mathcal{R}$, and let F: $\mathcal{R}\rightarrow\{0,1\}^n$ be a two-universal random function [39]. The random variable $K=F(R)$ satisfies

$$\sum_{k,f,e}|P(k,f,e)-2^{-n}P(f,e)|\leq\sqrt{2^n P_{\text{guess}}(R|E)}, \qquad \text{(A1)}$$

where

$$P_{\text{guess}}(R|E)=\sum_e \max_r P(r,e). \qquad \text{(A2)}$$

Proof: Using the convexity of the square function, the fact that F is independent of R and E, and two-universality, we obtain

$$
\begin{aligned}
\Big(\sum_{k,f,e}|P(k,f,e)-2^{-n}P(f,e)|\Big)^2 &\le \sum_{k,f,e}P(f,e)2^{-n}\Big(2^n\sum_r P(r|e)\delta^k_{f(r)}-1\Big)^2\\
&=\sum_{f,e}P(f,e)2^{-n}\Big(2^{2n}\sum_{r,r'}P(r|e)P(r'|e)\delta^{f(r')}_{f(r)}+2^n-2^{1+n}\Big)\\
&=-1+2^n\sum_{f,e}P(f,e)\Big(\sum_{r\neq r'}P(r|e)P(r'|e)\delta^{f(r')}_{f(r)}+\sum_r P(r|e)^2\Big)\\
&\le 2^n\sum_e P(e)\sum_r P(r|e)^2\\
&\le 2^n P_{\mathrm{guess}}(R|E).
\end{aligned}
$$

□

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The Security of Practical Quantum Key Distribution*, Rev. Mod. Phys. **81**, 1301 (2009).

[2] V. Scarani and C. Kurtsiefer, *The Black Paper of Quantum Cryptography: Real Implementation Problems*, arXiv:0906.4547.

[3] F. Xu, B. Qi, and H.-K. Lo, *Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution System*, New J. Phys. **12**, 113026 (2010).

[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination*, Nat. Photonics **4**, 686 (2010).

[5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-Independent Security of Quantum Cryptography against Collective Attacks*, Phys. Rev. Lett. **98**, 230501 (2007).

[6] D. Mayers and A. Yao, *Self Testing Quantum Apparatus*, Quantum Inf. Comput. **4**, 273 (2004).

[7] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, England, 1987).

[8] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[9] J. Barrett, L. Hardy, and A. Kent, *No Signaling and Quantum Key Distribution*, Phys. Rev. Lett. **95**, 010503 (2005).

[10] L. Masanes, *Universally Composable Privacy Amplification from Causality Constraints*, Phys. Rev. Lett. **102**, 140501 (2009).

[11] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, *Unconditional Security of Key Distribution from Causality Constraints*, arXiv:quant-ph/0606049.

[12] L. Masanes, S. Pironio, and A. Acín, *Secure Device-Independent Quantum Key Distribution with Causally Independent Measurement Devices*, Nat. Commun. **2**, 238 (2011).

[13] E. Hänggi and R. Renner, *Device-Independent Quantum Key Distribution with Commuting Measurements*, arXiv:1009.1833.

[14] J. Barrett, R. Colbeck, and A. Kent, *Unconditionally Secure Device-Independent Quantum Key Distribution with Only Two Devices*, Phys. Rev. A **86**, 062326 (2012).

[15] B. W. Reichardt, F. Unger, and U. Vazirani, *A Classical Leash for a Quantum System: Command of Quantum Systems via Rigidity of CHSH Games*, arXiv:1209.0448.

[16] B. W. Reichardt, F. Unger, and U. Vazirani, *Classical Command of Quantum Systems via Rigidity of CHSH Games*, arXiv:1209.0449.

[17] U. Vazirani and T. Vidick, *Fully Device Independent Quantum Key Distribution*, arXiv:1210.1810.

[18] R. Colbeck, Ph.D. thesis, University of Cambridge, 2006.

[19] 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 (London) **464**, 1021 (2010).

[20] S. Pironio and S. Massar, *Security of Practical Private Randomness Generation*, Phys. Rev. A **87**, 012336 (2013).

[21] S. Fehr, R. Gelles, and C. Schaffner, *Security and Composability of Randomness Expansion from Bell Inequalities*, Phys. Rev. A **87**, 012335 (2013).

[22] U. V. Vazirani and T. Vidick, *Certifiable Quantum Dice—Or, Testable Exponential Randomness Expansion*, arXiv:1111.6054.

[23] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, in *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming*, Lecture Notes in Computer Science Vol. 4051 (Springer, New York, 2006), p. 72.

[24] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, *Device-Independent State Estimation Based on Bell's Inequalities*, Phys. Rev. A **80**, 062327 (2009).

[25] M. McKague, T. H. Yang, and V. Scarani, *Robust Self-Testing of the Singlet*, J. Phys. A **45**, 455304 (2012).

[26] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, *Device-Independent Witnesses of Genuine Multipartite Entanglement*, Phys. Rev. Lett. **106**, 250404 (2011).

[27] S. L. Braunstein and C. M. Caves, *Wringing Out Better Bell Inequalities*, Ann. Phys. (N.Y.) **202**, 22 (1990).

[28] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett. **23**, 880 (1969).

[29] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, *Cryptography in the Bounded-Quantum-Storage Model*, SIAM J. Comput. **37**, 1865 (2008).

[30] R. T. König and B. M. Terhal. *The Bounded-Storage Model in the Presence of a Quantum Adversary*, IEEE Trans. Inf. Theory **54**, 749 (2008).

[31] The two main approaches for quantum memories are based on an ensemble of atoms or on crystals. To our knowledge, the best existing quantum memories with an ensemble of atoms have coherence times of the order of 100 ms; see A. G. Radnaev, Y. O. Dudin, R. Zhao, H. H. Jen, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, *A Quantum Memory with Telecom-Wavelength Conversion*, Nat. Phys. **6**, 894 (2010); moving to crystals, coherence times of the order of a few seconds have been reported for classical light—see J. J. Longdell, E. Fraval, M. J. Sellars, and N. B. Manson, *Stopped Light with Storage Times Greater than One Second Using Electromagnetically Induced Transparency in a Solid*, Phys. Rev. Lett. **95**, 063601 (2005). While, in principle, the method should be scalable to light at the quantum level, this application has not been demonstrated yet. Of course, improvements on these coherence times may be expected in the foreseeable future; however, there is no evidence that these improvements will be significant.

[32] M. Navascués, S. Pironio, and A. Acín, *Bounding the Set of Quantum Correlations*, Phys. Rev. Lett. **98**, 010401 (2007); S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *Device-Independent Quantum Key Distribution Secure against Collective Attacks*, New J. Phys. **11**, 045021 (2009).

[33] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, *Bell Inequalities for Arbitrarily High-Dimensional Systems*, Phys. Rev. Lett. **88**, 040404 (2002).

[34] U. Maurer, *Conditionally-Perfect Secrecy and a Provably-Secure Randomized Cipher*, J. Cryptol. **5**, 53 (1992).

[35] S. Wehner, C. Schaffner, and B. M. Terhal, *Cryptography from Noisy Storage*, Phys. Rev. Lett. **100**, 220502 (2008).

[36] R. König, S. Wehner, and J. Wullschleger, *Unconditional Security from Noisy Quantum Storage*, IEEE Trans. Inf. Theory **58**, 1962 (2012).

[37] R. Renner, Ph.D. thesis, ETH Zurich, 2006, arXiv:quant-ph/0512258.

[38] R. König, R. Renner, and C. Schaffner, *The Operational Meaning of Min- and Max-Entropy*, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[39] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, *Generalized Privacy Amplification*, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[40] K. Azuma, *Weighted Sums of Certain Dependent Random Variables*, Tohoku Math. J. **19**, 357 (1967).

[41] R. Arnon-Friedman, E. Hänggi, and A. Ta-Shma, *Towards the Impossibility of Non-signalling Privacy Amplification from Time-like Ordering Constraints*, arXiv:1205.3736; R. Arnon-Friedman and A. Ta-Shma, *Limits of Privacy Amplification against Nonsignaling Memory Attacks*, Phys. Rev. A **86**, 062333 (2012).