Completely device-independent quantum key distribution

Edgar A. Aguilar,[1,2] Ravishankar Ramanathan,[2,3] Johannes Kofler,[4] and Marcin Pawłowski[2,3]
[1]*Institute of Mathematics, University of Gdansk, 80-952 Gdansk, Poland*
[2]*National Quantum Information Center of Gdansk, 81-824 Sopot, Poland*
[3]*Institute of Theoretical Physics and Astrophysics, University of Gdansk, 80-952 Gdansk, Poland*
[4]*Max-Planck-Institute of Quantum Optics, 85748 Garching, Germany*
(Received 6 November 2015; published 5 August 2016)

Quantum key distribution (QKD) is a provably secure way for two distant parties to establish a common secret key, which then can be used in a classical cryptographic scheme. Using quantum entanglement, one can reduce the necessary assumptions that the parties have to make about their devices, giving rise to device-independent QKD (DIQKD). However, in all existing protocols to date the parties need to have an initial (at least partially) random seed as a resource. In this work, we show that this requirement can be dropped. Using recent advances in the fields of randomness amplification and randomness expansion, we demonstrate that it is sufficient for the message the parties want to communicate to be (partially) unknown to the adversaries—an assumption without which any type of cryptography would be pointless to begin with. One party can use her secret message to locally generate a secret sequence of bits, which can then be openly used by herself and the other party in a DIQKD protocol. Hence our work reduces the requirements needed to perform secure DIQKD and establish safe communication.

DOI: 10.1103/PhysRevA.94.022305

I. INTRODUCTION

Within the advancing quantum information technologies, quantum key distribution (QKD) is arguably the technologically most advanced field and has already entered the market with working product solutions. In this quantum cryptographic protocol, two parties usually named Alice and Bob exploit the laws of quantum physics to produce a shared random key that remains unknown to the rest of the world and which can then be used as a one-time pad in a classical cryptographic scheme [1–4].

The security of entanglement-based QKD protocols relies on the violation of a Bell inequality [5] using pairs of quantum entangled particles shared by Alice and Bob. Remarkably, it has been shown that such entanglement-based protocols allow device-independent QKD (DIQKD) [6,7], in which the two parties need not make any assumptions about the inner workings of their devices, in particular the source that produces the systems which the parties measure as well as their own measurement devices. In principle, the measurement apparatuses can be bought from an untrusted party, the eavesdropper Eve, and the particle pair source can even be operated by her (as long as, for example, there are no hidden transmitters in the devices). Alice and Bob can still extract a secret key by sufficiently violating a Bell inequality. However, they are required to have access to a certain amount of randomness which they use for their setting choices [8,9]. This is related to the fact that no Bell inequality can be derived without the "freedom-of-choice assumption" [10].

For long messages, Alice and Bob need many settings to produce a key long enough, such that it becomes infeasible to invent their own random sequences bit by bit out of their heads. Hence their settings need to be produced by some sort of fast device. Such a random number generator and its corresponding randomness must be considered a resource in the protocol. However, it is impossible to verify that any given random number generator is not determined by some underlying mechanism which is simply unknown to the user but not to the eavesdropper. Clearly, Alice and Bob should not buy their randomness generators from Eve. Therefore, in some sense, the assumptions in DIQKD are contradictory. While one does not trust the measurement devices, one trusts the random number generators used for the setting choices. Recent developments (e.g., regarding the dual elliptic curve deterministic random bit generator) have shown that this trust can be problematic [11].

It is indeed possible to reduce the amount of required initial randomness via randomness amplification and expansion. These protocols exploit quantum correlations also in a device-independent way [12–17]. The former field studies how, given a source of imperfect randomness which is partially correlated to the external world, one can produce a short string which is completely uncorrelated and safe. The latter studies how, given a finite amount of perfect random bits one can produce a longer (potentially unbounded) random bit string. Both of these processes have been generalized recently to achieve unbounded random strings from finite min-entropy sources [15,16]. However, both protocols require an initial (at least partially) random seed, and there is no apparent way of getting around this assumption if one wants to stick to the device-independent scenario.

We define a completely DIQKD (CDIQKD) protocol to be one which is not only device-independent regarding the measurement apparatuses and the pair source but which also does not need to make any assumptions about the setting generators or initial random seeds. It seems that this is an impossible task. The QKD community has been working within the paradigm that if at least one of the parties does not have an initial (at least partially) random source, then sending safe messages is not feasible.

In this paper, however, we show that the obstacle is surmountable and that CDIQKD is indeed possible. The solution lies in the observation that Alice and Bob do not really need their settings to be random with respect to the whole universe. They only need randomness with respect to Eve. Therefore, having a string which is random to Eve and the devices used in the protocol is sufficient, even though the string is not random with respect to an honest party like Alice. And there is one thing, which is random to Eve due to the fundamental underlying assumption in cryptography: the message $\mathcal{X}$ which Alice wants to send to Bob. Without this trivial assumption—so basic that it usually is not even mentioned—there is no reasonable cryptographic task in the first place.

Our procedure seems counterintuitive and risky, but in this paper we give a proof of principle that it is secure. In the following, we will show that Alice can use her secret message to locally generate a secret sequence of bits, which can then be used by herself and Bob as the settings in an entanglement-based QKD protocol.

II. BACKGROUND AND ASSUMPTIONS

We will work with the standard QKD assumptions which, for the sake of clarity, are listed below.

Quantum key distribution assumptions

(1) *Shielding.* A no-signaling condition is imposed on the components of each device, as well as between devices in both parties' laboratories.

(2) *Authenticated classical communication channel between parties.* This is not assumed to be secure, i.e., any classical communication is accessible to Eve. Furthermore, we consider this authenticated channel to be available to the parties as a black box resource, that was for instance previously established using a secret key.

(3) *Restriction to quantum theory.* The adversary can only prepare devices following the laws of quantum mechanics. In particular, she does not possess arbitrary no-signaling devices.

(4) *Message with randomness.* Alice possesses a message $\mathcal{X}$ with k min-entropy with respect to Eve and the devices, and can estimate this value. k needs to be sufficiently large.

These are the fundamental assumptions, without any of which the protocol could not guarantee security. For example, without assumption (1), there could be a transmitter in the devices telling Eve everything that is going on in the laboratories (including the secret message), or Eve could manipulate the devices externally. Furthermore, the protocols work assuming a Bell inequality was violated for which the components of the physical devices must not communicate, which for example, could be enforced by a spacelike separation. Assumption (2) is needed to avoid the "man in the middle" attack, even though this classical channel is accessible to the adversary. In the present work we consider the channel as a black box resource; see the Discussion for an elaboration. Assumption (3) may seem restrictive at a mathematically fundamental level, but this is also a standard assumption for security proofs such as in [7,15,16,18], since superquantum correlations have not been observed experimentally. Finally, our main assumption is that Alice's message $\mathcal{X}$ has some conditional min-entropy with respect to Eve and the devices, and that Alice is able to estimate this value. We argue that this is a sound assumption (and indeed usually left implicit), since if the message was not at least partially random to Eve, then performing a QKD protocol would lose all its point to begin with, as was already suggested in the concluding remark of [19].

In this article, we think of *conditional min-entropy*$H_{\min}$ operationally. If we have the classical quantum state $\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x$, classical over X and quantum over E, then the probability that party E correctly guesses the value of the random variable X is

$$p_{\text{guess}}(X|E) = \sum_x P_X(x)\text{tr}\big[F_x \rho_E^x\big] = 2^{-H_{\min}(X|E)_\rho},$$

where $\{F_x\}$ is the optimal POVM on E [20]. In words, this means that the min-entropy quantifies how much of the string X is unknown to system E. This is the standard way of quantifying randomness, by which we mean how much of a variable is unpredictable to a third party. In that sense, the "most random variable" X corresponds to the uniform distribution U_X, which is completely independent from everything else. In that case the min-entropy is simply the number of random bits, $H_{\min}(X|E) = |X|$.

By *randomness extractors* $\text{Ext}(k,\varepsilon)$, we refer to deterministic algorithms, which take a source X with min-entropy k, together with a uniform random seed of length d, to produce an output of length m, which is an ε distance from the uniform distribution. We shall use Trevisan's extractor [21], which was proven to be secure against quantum adversaries in [18], following the works of [22,23]. See Appendix B for a rigorous treatment.

A powerful observation which we will also need is the *equivalence lemma* from [16]. The lemma states that the security of protocols using perfectly random strings depends on these strings being perfectly random to the devices, and requiring perfect randomness to both the devices and the adversaries is not necessary. This is formally stated in Appendix A as Lemma A.1. Since we are assuming that Eve doesn't signal to the devices, the important thing then is that the devices are not preprogrammed to receive certain inputs. If during the protocol Eve learns more about what random seeds Alice and Bob will use, then even if she adapts her eavesdropping strategy she cannot gain any advantage, so long as the devices were distributed beforehand.

Chung, Shi, and Wu devised a protocol which can amplify any finite source with min-entropy k, by using Trevisan's extractors $\text{Ext}(k,\varepsilon)$ [16]. They coined this procedure *physical randomness extraction*, because they rely on physical procedures which extract randomness in a secure manner through Bell tests. Their solution is to use $\text{Ext}(k,\varepsilon)$ on the min-entropy source with all 2^d possible seed strings of length d, and feeding each hashed output to different implementations of the physical extraction protocol (which here will be a randomness expansion protocol). By different implementations, we mean using new devices on each run of the physical protocol as to guarantee each input is really random with respect to the devices to be used (i.e., there aren't any memory correlations between implementations). See the first part of Fig. 1.

For expansion, we will use the recent protocol by Miller and Shi [15] (abbreviated as MS), which by itself gives cryptographic security in the output and is robust to noise. This protocol, together with the Equivalence Lemma can take a min-entropy source and produce unbounded expansion with

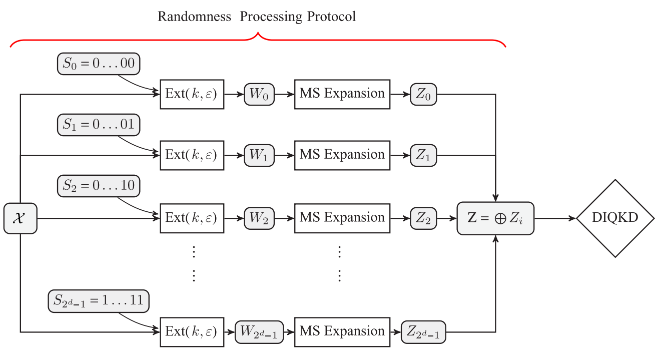

FIG. 1. Schematic representation of the protocol. An n-bit message $\mathcal{X}$ is fed into Trevisan's extractor with all possible seeds S of length d, which in turn is used to run the Miller-Shi protocol for expansion. Finally, these outputs are summed (modulus 2) to obtain the random seed $\mathcal{Z}$ used for the DIQKD scheme.

only two untrusted devices. Following [15,16] we treat a device D as a black box, with which the experimenter can interact classically. Each box D will consist of t spatially separated (no-signaling) components which will play an XOR nonlocal game. Hence the number t will depend on the nonlocal game to be played (e.g., for CHSH $t = 2$, and for GHZ $t = 3$). See [24] for an exposition on XOR games.

Currently, different DIQKD schemes exist that could work with our protocol. Choosing which one to implement is a matter of taste, since different Bell inequalities have different advantages. For example, the protocols [7,15] are robust against a constant fraction of noise, while [25] is even safe against no-signaling adversaries. What is common in these schemes though, is that at least one of the parties must have access to an additional source of randomness. Given that we would like our CDIQKD protocol to be noise tolerant, we propose to use one of [7,15]. To our knowledge, these are the only available protocols which are secure against quantum adversaries, possessing quantum side information.

The last concepts we need to introduce are the security parameters. The *completeness error* ε_c bounds the probability that we reject an honest implementation of the protocol, $\mathbb{P}[\text{Reject}] \leqslant \varepsilon_c$. The *soundness error* ε_s quantifies how random the output Z is if we choose to accept it. To see how, consider general output states which are decomposed as $\Phi \circ \Gamma_E[\rho] = |\text{Acc}\rangle\langle\text{Acc}| \otimes \sigma^{\text{Acc}}_{ZXDE} + |\text{Rej}\rangle\langle\text{Rej}| \otimes \sigma^{\text{Rej}}_{ZXDE}$, where Φ is the quantum channel of the protocol, and Γ_E is an arbitrary quantum channel on Eve's system. We require that there exists a state ξ such that $\xi^{\text{Acc}}_{ZXE} = U_Z \otimes \xi_{XE}$ and $\|\sigma^{\text{Acc}}_{ZXE} - \xi^{\text{Acc}}_{ZXE}\| \leqslant \varepsilon_s$. Here, $\sigma^{\text{Acc}}_{ZXE}$ is the subnormalized output after tracing out the devices D, and $U_Z = \frac{1}{|Z|}\mathbb{1}$ is the uniform distribution. Most of the time though, we will just talk about the *security parameter* $\delta = \max(\varepsilon_c,\varepsilon_s)$, which represents the worst error in both possible interpretations of the word error.

The *error tolerance parameter*, or noise level, η, parametrizes how an actual implementation of an untrusted device deviates from an honest one. That is, it is the maximum ratio of game rounds for which we observe an error (so that the observed correlations are not according to the optimal winning strategy).

III. KEY DISTRIBUTION PROTOCOL

For convenience, we divide our CDIQKD protocol into two parts: randomness processing and key distribution. The randomness processing part (which takes place entirely in Alice's laboratory) consists of taking Alice's message $\mathcal{X}$ as a seed to create a string of random numbers $\mathcal{Z}$ which will be used in the Key Distribution Scheme (e.g., to choose measurement bases, which bits to compare and test the Bell inequality on, or which hashing function to use).

Randomness processing protocol

(1) Alice lists all possible bit strings $(S_0,S_1,\dots,S_{2^d-1})$ of length d.

(2) Alice processes her message $\mathcal{X}$ with Trevisan's extractor, using all 2^d strings S_i as possible seeds. Call the outputs $W_i = \text{Ext}[\mathcal{X},S_i]$.

(3) Alice performs the MS unbounded randomness expansion protocol in parallel, on each W_i, and using different devices. The output of each expansion run is labeled Z_i.

(4) $\mathcal{Z} = \bigoplus_i Z_i$.

The actual size of $d = |S_i|$ and $m = |W_i|$ are specified in the next section.

The randomness processing protocol to be used is the composition of the protocols proposed by [16] and [15], as is depicted in Fig. 1. The ideal objective of the protocol is to obtain a random string $\mathcal{Z}$, independent from the input message $\mathcal{X}$, such that $|\mathcal{Z}| \gg |\mathcal{X}|$. In fact, the expansion protocol used allows us to make the output $\mathcal{Z}$ unbounded, so that Alice can be confident she will have enough random bits to feed the DIQKD protocol.

The MS-expansion protocol uses the concatenation of two devices to achieve unbounded randomness expansion [15]. As seen in Fig. 2, an input random string X_0 is fed into the first device and produces an output string X_1 which is longer and contains more min-entropy than the input. Then, string X_1 is fed into the second device, producing output X_2 which is also longer and contains more min-entropy than its corresponding input X_1. In this fashion, it is easily seen that

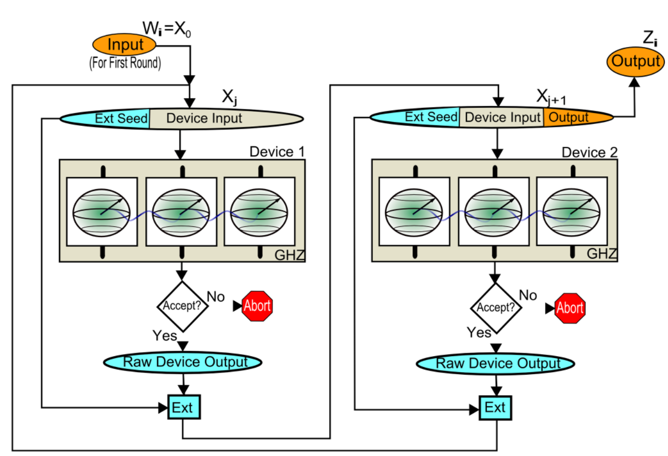

FIG. 2. Representation of the MS expansion protocol, used within the randomness processing protocol. By cross feeding the outputs of the devices to each other, Alice is able to obtain the unbounded random string Z.

alternating between the two devices, the random strings $\{X_j\}$ keep prolonging monotonically, and Alice is free to repeat this protocol as many times as possible to achieve unbounded expansion.

One may note however that in between device uses, the output must be processed through Trevisan's extractor, which provides security against quantum side information. Since the extractor requires two inputs, in reality not all of string X_j is fed into a device. Rather a part of it is kept to seed the extractor, which will operate on the raw expanded output of the device. Afterwards, Alice may choose to run the expansion on the whole string X_{j+1}, or directly use some of the bits as an output sequence (as depicted in Fig. 2).

The specific expansion protocol used to obtain the longer and more random output X_{j+1} from the shorter input X_j is given in Appendix C. For the moment, let's assume that Alice is running the protocol based on the GHZ nonlocal game, and that the size of her desired output is $N = |X_{j+1}|$. Then, Alice will feed N different inputs into the components of her device which are in charge of violating the GHZ-Bell inequality. The majority of the time Alice will use a predefined input for her device's components (say 111), and record the output of the first component (these are the so-called *generating rounds*). However, in order to be sure that the components are indeed outputting random strings, Alice needs to run statistical tests on her device. For this, she will select a random subset of the N inputs to actually "play" the GHZ game—i.e., the inputs to the device components are chosen at random from the set $\{111,100,010,001\}$. The GHZ game is won if $a_1 \oplus a_2 \oplus a_3 = x_1 \wedge x_2 \wedge x_3$, where the a_i are the output of the components, and the x_i the corresponding inputs. If during these *game rounds*, the device loses more often than allowed by the error tolerance parameter (optimized later), then Alice aborts. Otherwise, she now has a new random string X_{j+1} which has more min-entropy than what she started with.

Finally, Alice will have a fully secret string $\mathcal{Z}$ with respect to Eve. If the security of the string is high enough, this can be used to implement the now standard protocols of [7,26] or even the new QKD protocol of [15]. However, it is typically assumed that both Alice and Bob have access to RNG's or initial randomness. Now, only Alice has randomness available, and she must publicly broadcast to Bob what to measure. One way for this to be secure would be to require that Alice and Bob were already sharing all entangled pairs from the start. A way around this would be for Alice to wait until Bob has received his device (i.e., part of the entangled pair), and afterwards Alice would broadcast Bob's corresponding measurement setting (see Fig. 3). This eliminates the need of the vast quantum memory of the former approach. What is needed is that there exist quantum states and measurement settings such that each step in the protocol would be passed by honest parties, which both approaches possess.

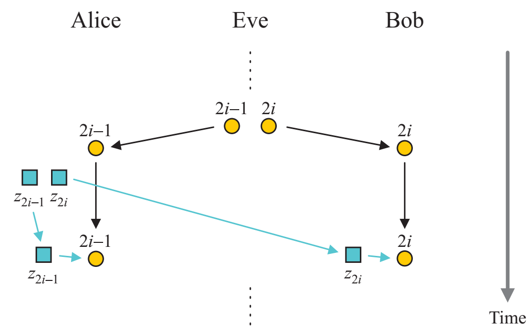

FIG. 3. Space-time scheme of a QKD protocol without initial randomness. From her secret message $\mathcal{X}$, Alice has already established a sequence $\mathcal{Z}$ of bits z_i unknown to Eve. Eve sequentially sends pairs of particles labeled with $2i-1$ and $2i$ ($i = 1,2,\ldots$) to Alice and Bob, respectively. Once Bob confirms he received particle $2i$, Alice sends the bit z_{2i} to Bob, which he uses as a setting. Alice uses z_{2i-1} for her own particle.

IV. SECURITY ANALYSIS

In this section we analyze the security of the protocol. Our starting point is that Alice holds a message of length n that she wants to communicate to Bob, and said message has min-entropy k (conditioned on Eve and the devices). For the protocol to work, it is part of the assumption that Alice can estimate (lower bound) the value k, which is also a commonly implied assumption in other protocols such as [12,15,16].

Of course all of the subprotocols we are utilizing here have been proven secure by their corresponding authors, but their composition is a nontrivial task. Also, the point of view we take here is that Alice has no further access to randomness, so there will be a lower bound for the security parameters (since these are functions of k, and it is finite). We also note that, since this is a proof of principle, the requirement of exponentially many different devices that arises from the scheme of Chung, Shi, and Wu is something we do not intend to improve, and we rest content with having a finite amount of devices.

The first part we analyze is Trevisan's Extractor, proven to be secure against quantum adversaries [18,21–23]. This will create an output of size $m < k$ an ε_T distance from uniform. The following Lemma gives a bound on the error and seed length needed. For an explicit and detailed proof, see Appendix B.

Lemma IV.1. Trevisan's extractor. For a message $\mathcal{X}$ with min-entropy k, $0 < m < k$, there exists an m-bit quantum proof extractor $\mathrm{Ext}(k,\varepsilon_T)$, using a seed of length ■

$$d = (7 + k - m + \log_2 |\mathcal{X}|)^2 \frac{\log_2(4m)}{\ln 2} \tag{4.1}$$

and with error

$$\varepsilon_T = 3\, m\, 2^{-\frac{1}{8}(k-m)+\frac{1}{4}}. \tag{4.2}$$

For analyzing the security of Miller and Shi's expansion protocol, we must choose a nonlocal game to be played. In what follows we shall use the GHZ game, with $t = 3$. Besides having a large quantum-classical gap and having an optimal strategy that wins with probability 1, both [15,27] have considered it for their analysis. Concretely, there exist carefully optimized parameters to implement the Miller-Shi unbounded protocol with a uniform seed, such that the security parameter decreases exponentially with the seed length m:

$$\varepsilon_{MS} = 2^{\frac{\alpha-m}{\beta}}, \tag{4.3}$$

with constants $\beta = 31328$, and $\alpha = 120{,}931$. See Appendix C for further details.

It is interesting to note that while the expansion error ε_{MS} decreases exponentially with the input length m, the error of the quantum proof extractor grows exponentially with the output size m. Hence there is a direct trade off, and Alice must choose m according to her error goals in an easy optimization problem. For simplicity though, Alice can take, e.g., $m = k/2$.

Finally, Chung, Shi, and Wu's main result gives the soundness and completeness errors one obtains after having performed extraction and expansion with each of the 2^d seeds and summing all of the outputs modulo 2. The answer is a function of both the extraction and expansion error, as well as the error tolerance η, which comes from the Miller-Shi expansion protocol. In particular, the security parameter δ of the whole randomness processing protocol will be given by $\delta = \max\left(\frac{\varepsilon_T+\varepsilon_{MS}}{\eta},\varepsilon_{MS} + 2\sqrt{\varepsilon_T} + 2\eta\right)$, using a total of 6×2^d device components [16]. This leads us to our first main result (proof in Appendix D).

Theorem IV.1. Security of randomness processing. If Alice performs the randomness processing protocol on her message $\mathcal{X}$ with min-entropy k, the output string $\mathcal{Z}$ is cryptographically secure. That is, the security parameter δ is exponentially small in k. ∎

It is worth noting that there is some threshold value for this protocol $k \gtrsim 200\,000$, under which it will not work at all. This is reminiscent of the 225 000 bits of min-entropy that are needed to have unbounded expansion with the MS protocol and a security parameter of $\epsilon = 10^{-1}$ [27]. That is, in order to achieve a fixed security parameter target for randomness expansion, the amount of input min-entropy must be above some threshold. In any case, we imagine k to be large enough so that the security parameter is sufficiently small.

Now that Alice has the random string $\mathcal{Z}$, she is ready to apply, together with Bob, the DIQKD protocol of either [7] or [15], which have their respective errors $\varepsilon_c,\varepsilon_s$. For a moment let us assume that $\mathcal{Z}$ is a perfectly random string; then the Equivalence Lemma of [16] would guarantee that the completeness and soundness errors of the DIQKD protocol would remain the same even if Eve learned most of $\mathcal{Z}$ later on (making this semantically secure). However, $\mathcal{Z}$ has security parameter δ, exponentially small in k, and this will add to the errors of the protocol (which could be understood as a consequence of the composability of the protocols [28]). Note that the string $\mathcal{Z}$ is indeed random to the devices in the DIQKD protocol, since the initial message had min-entropy $k = H_{\min}(\mathcal{X}|ED)$ conditioned on both the randomness processing devices D, and Eve (who is the one who potentially will create the DIQKD devices). We formalize this in our second main theorem, which is proven in Appendix E.

Theorem IV.2. Security of CDIQKD. Let there be a DIQKD protocol which requires a perfect random number generator and which has completeness and soundness errors $(\varepsilon_c,\varepsilon_s)$. Then, Alice can perform the randomness processing protocol on her secret message $\mathcal{X}$ with min-entropy k, to produce a secure random output $\mathcal{Z}$ and perform CDIQKD with errors $(\varepsilon_c + \delta,\varepsilon_s + \delta)$, where $\delta = 2^{-\Omega(k)}$. ∎

V. DISCUSSION

We have shown that even in the absence of randomness generators, Alice can securely perform DIQKD. This is indeed a remarkable fact, since it is commonly assumed that without initial randomness no security can be achieved. In this article, we have made a proof of principle based on the assumptions given. Note, however, that our protocol still required the use of a classical authenticated channel which traditionally is established using a shared secret key between the honest parties. At first sight this seems to call into question the result of this paper. However, recall that the authenticated channel does not have to be established each time the parties wish to send a message to each other. As stated in Assumption 2, we consider the authenticated channel to be a blackbox resource, that the parties could have established a long time in the past. A shared arbitrarily weak key suffices for this task, as shown in [29]. Traditional DIQKD relies on a further assumption, namely that the parties hold private secure random number generators, which they use to obtain inputs for the protocol. The security of the output randomness of these RNGs could be subject to question especially if these were prepared by an external adversary. The issue this paper addresses is therefore the removal of this crucial assumption in a fairly general framework for DIQKD. Finally, a secret key shared by the parties could replace the message in the presented protocol if it is of sufficiently high min-entropy.

We leave further generalizations and optimizations for future work. For example, we conjecture that our scheme can be simplified to use a significantly smaller number of devices and that it can be generalized to be secure against no-signaling adversaries also, leading one to drop the validity of quantum mechanics as an assumption.

ACKNOWLEDGMENTS

E.A. would like to thank R. Renner and K. Horodecki for helpful discussions, and M. Farkas for reviewing the manuscript. This work was supported by NCN Grant No. 2013/08/M/ST2/00626, the IDSMM program of the University of Gdansk, and the National Quantum Information Centre in Gdansk. J.K. acknowledges support from the European Union Integrated Project Simulators and Interfaces with Quantum Systems. R.R. acknowledges support from the ERC AdG grant QOLAPS, and the Foundation for Polish Science TEAM project cofinanced by the EU European Regional Development Fund.

APPENDIX A: DEFINITIONS AND NOTATION

In this section, we formalize some important definitions, which were just mentioned conceptually in the main text. Throughout this whole article, as is common in information science, $\log_2(x) = \log_2(x)$.

Definition A.1. Conditional min-entropy. Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$; the min-entropy of A conditioned on B is

$$H_{\min}(A|B)_{\rho_{AB}} = \max\{\lambda \in \mathbb{R} : \exists\, \sigma_B \in \mathcal{D}(\mathcal{H}_B) \text{ such that } \rho_{AB} \leqslant 2^{-\lambda}\mathbb{1}_A \otimes \sigma_B\}. \quad \text{(A1)}$$

Here, $\mathcal{D}(\mathcal{H})$ represents the set of density matrices in Hilbert space $\mathcal{H}$. For the completeness and soundness errors, we use the definitions given by [16], since our security parameter is based on the maximum of these quantities. Before that, we must specify what is meant by a physical system.

Definition A.2. Physical system [16]. A physical system $\mathcal{S}$ is defined on an arbitrarily large, but finite Hilbert space $X \otimes D \otimes E$, with a classical source $\mathcal{X}$ of length n with k min-entropy, t untrusted devices $D = (D_1, \ldots, D_t)$, and an adversary E. To each device D_i there corresponds a quantum interactive algorithm A_{D_i} that applies on D_i which outputs at most m bits.

Usually this is also called an (n,k,t,m)-physical source, where in our scenario the min-entropy k the message has is conditioned on both E and D. Hence a physical system $\mathcal{S}$ is specified by a state ρ_{XDE} and the algorithms the devices will follow $\{A_{D_i}\}$, but the latter are usually irrelevant for the security analysis.

Any randomness processing protocol (e.g., for amplification or expansion) can be viewed as a quantum channel $\Phi : \mathcal{D}(X \otimes D) \to \mathcal{D}(O \otimes Z \otimes X \otimes D)$, also called *physical randomness extractors* (since they act on physical systems). The new Hilbert spaces $O \otimes Z$ are for a decision bit o which will tell us to accept or reject the implementation of the protocol (if, e.g., the Bell test was not passed with confidence), and the new output random string $\mathcal{Z}$. If the physical randomness extractors require perfectly random inputs, i.e., they are designed to work on (n,n,t,m)-physical systems, they are called *seeded physical randomness extractors*.

Definition A.3. Completeness error [16]. There exist honest devices $D = (D_1, \ldots, D_s)$ with internal state σ_D and algorithms $\{A_{D_i}\}$, with each device outputting at most m bits such that for any (n,k,s,m)-physical system $\mathcal{S}$ satisfying $\mathrm{tr}_{XE}[\rho] = \rho_D = \sigma_D$, we have

$$\mathbb{P}[\mathrm{Acc}(\rho)] \geqslant 1 - \varepsilon_c, \tag{A2}$$

where $\mathrm{Acc}(\rho)$ denotes the event that the protocol accepts on the input state of the device and source supplied to the physical randomness extractor, when applied to $\mathcal{S}$ (i.e., $o = \mathrm{Acc}$).

In other words, this tells us that, if we are using honest devices, we will accept the protocol with high probability. The soundness error, in turn tells us how close we are to a truly random output (i.e., a uniform distribution), conditioned on accepting the protocol.

Definition A.4. Soundness error [16]. Suppose the physical system $\mathcal{S}$ is equipped with a decision bit O; then the projection of the output $\Phi[\rho]$ to the acceptance subspace is at most an ε_s distance away from a state of the form $U_Z \otimes \xi_{XE}$ conditioned on accepting, where ξ_{XE} is some classical quantum state. General output states are decomposed as $\Phi \circ \Gamma_E[\rho] = |\mathrm{Acc}\rangle\langle\mathrm{Acc}| \otimes \sigma^{\mathrm{Acc}}_{ZXDE} + |\mathrm{Rej}\rangle\langle\mathrm{Rej}| \otimes \sigma^{\mathrm{Rej}}_{ZXDE}$, where Γ_E is an arbitrary quantum channel on Eve's system. We require that there exists a state ξ such that $\xi^{\mathrm{Acc}}_{ZXE} = U_Z \otimes \xi_{XE}$ and

$$\left\|\sigma^{\mathrm{Acc}}_{ZXE} - \xi^{\mathrm{Acc}}_{ZXE}\right\| \leqslant \varepsilon_s, \tag{A3}$$

where $\sigma^{\mathrm{Acc}}_{ZXE}$ is the subnormalized output after tracing out device D, and $U_Z = \frac{1}{|Z|}\mathbb{1}$ is the uniform distribution.

An important result which we will need for our analysis, which has to do with physical randomness extractors, is the following lemma.

Lemma A.1. Equivalence lemma [16]. Let Φ be a seeded physical randomness extractor, with seeds X which are perfectly random to both Eve and the devices [i.e., $H_{\min}(X|DE) = n$], have parameters $(\varepsilon_s,\varepsilon_c,\eta)$. Then the same physical randomness extractor Φ, when applied to an input which is perfectly random to just the devices [i.e., $H_{\min}(X|D) = n$] will have the same parameters $(\varepsilon_s,\varepsilon_c,\eta)$.

The moral being that the crucial thing is that the input is random to the devices used.

APPENDIX B: QUANTUM STRONG EXTRACTORS

In this section, we analyze the security of Trevisan's extractor from Ref. [18], to prove Lemma 4.1. We begin with a formal definition of a quantum-strong extractor.

Definition B.1. Quantum proof strong extractor. $\mathrm{Ext}:\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, is an m-bit quantum proof (k,ε)-strong extractor, if for all states ρ_{XE} classical on X with $H_{\min} \geqslant k$, and a uniform seed Y of length d, we have

$$\tfrac{1}{2}\|\rho_{\mathrm{Ext}(X,Y)YE} - U_m \otimes \rho_y \otimes \rho_E\| \leqslant \varepsilon, \tag{B1}$$

with $\|\cdot\|$ the trace-norm, and U_m the totally mixed state in $\mathbb{C}^{2^m}$.

The classical version of this definition ignores the quantum state E and uses the variational distance in Eq. (B1). Explicitly, a *(k,ε)-strong extractor* satisfies $\frac{1}{2}\|Ext(X,Y) \circ Y - U_m \circ Y\| \leqslant \varepsilon$. The main theorem of [18] relates the security of 1 bit (k,ε)-strong extractors to m-bit extractors which are quantum proof. This is done via means of *weak (t,r) designs*, which are just families of partioning sets—otherwise irrelevant here.

Theorem B.1. Trevisan's extractor is quantum proof (Theorem 4.6 of [18]). Let $C : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}$ be a (k,ε)-strong extractor with uniform seed and $S_1, \ldots, S_m \subset [d]$, a weak (t,r) design. Then $\exists$ an extractor $\mathrm{Ext}_C : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, which is a $[k + rm + \log_2(1/\varepsilon), 3m\sqrt{\varepsilon}]$-quantum proof strong extractor.

The existence of such weak designs is given by [22].

Lemma B.1. Existence of weak $(t,1)$- designs (Lemma 17 of [22]). $\forall t,m \in \mathbb{N}, \exists$ weak $(t,1)$ design $S_1, \ldots, S_m \subset [d]$ such that $d = t\lceil\frac{t}{\ln 2}\rceil\lceil\log_2(4m)\rceil$. Furthermore, such a weak- design can be found in $\mathrm{Poly}(m,d)$ time and $\mathrm{Poly}(m)$ space.

For the 1-bit extractor C, we will use *list-decodable codes*—again, for our purposes all we require is their existence and that they can be found efficiently. This was implicitly proven by [21,22], and explicitly stated in [18] Theorem C.3.

Lemma B.2. List decodable vodes are 1-bit extractors (Theorem C.3 of [18]). Let $C : \{0,1\}^n \to \{0,1\}^{\bar{n}}$ be an (ε,L)-list decodable code. Then $\exists \mathrm{Ext}_C : \{0,1\}^n \times [\bar{n}] \to \{0,1\}$, which is a $(\log_2 L + \log_2(\frac{1}{2\varepsilon}), 2\varepsilon)$-strong extractor, created from code C.

Finally, we need an existence theorem for list decodable codes.

Lemma B.3. Existence of list decodable codes (Lemma C.2 of [18], Theorem 24 of [30]). $\forall n \in \mathbb{N}$, and $\varepsilon > 0$, $\exists$ a code $C_{n,\varepsilon} : \{0,1\}^n \to \{0,1\}^{\bar{n}}$ which is $(\varepsilon, 1/\varepsilon^2)$ list decodable. Furthermore, $\bar{n}$ can be assumed to be a power of 2, and satisfies the bound $\bar{n} \leqslant 32n/\varepsilon^4$. The code $C_{n,\varepsilon}$ can be evaluated in $\mathrm{Poly}(n,1/\varepsilon)$ time.

With all of this in mind, we are ready to prove Lemma 4.1. This is an analogous result to Corollary 5.3 of [18], and [27] has also made a similar analysis.

Lemma B.4. (Lemma 4.1 from main text). For a message $\mathcal{X}$ with k min-entropy, $m < k$, there exists an m-bit quantum

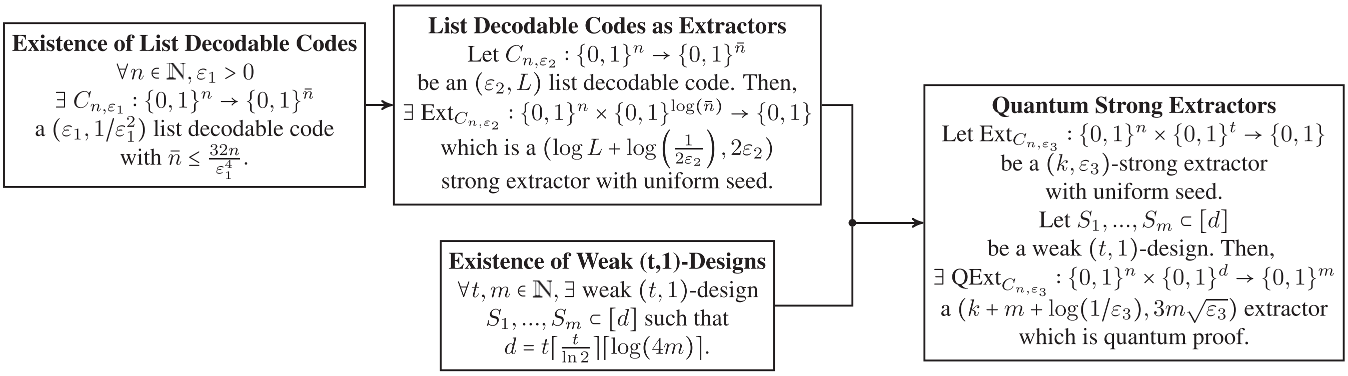

FIG. 4. Schematic diagram for the proof of Lemma 4.1.

proof extractor $\mathrm{Ext}(k, \varepsilon_T)$, using a seed of length

$$d = (7 + k - m + \log_2 |\mathcal{X}|)^2 \frac{\log_2(4m)}{\ln 2} \tag{B2}$$

and with error

$$\varepsilon_T = 3\, m\, 2^{-\frac{1}{8}(k-m)+\frac{1}{4}}. \tag{B3}$$

Proof. Lemma 4.1. To facilitate the proof of this lemma, which involves many different concepts and parameters, we refer to Fig 4. Notice that the notation is slightly different from the statement of the lemmas, to make it more consistent throughout the proof.

We take $\bar{n}$ to be a power of 2, $\bar{n} = 2^t$. Next, we create a $(\delta, 1/\delta^2)$ list-decodable code from Lemma B.3, so that we are guaranteed the existence of a 1-bit $[3\,\log_2(\frac{1}{2\delta}) + 2, 2\delta]$-strong extractor $C : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}$, with the help of Lemma B.2. We consider the worst case (saturated) bound on $\bar{n}$:

$$\bar{n} = \frac{32n}{\delta^4} \to t = \log_2\left(\frac{2^5 n}{\delta^4}\right). \tag{B4}$$

Equipped with this 1-bit extractor, we shall now use Theorem B.1 to create an m-bit extractor which is quantum proof. Direct application of the Theorem yields a $(4\log_2(\frac{1}{2\delta}) + m + 2$, $3m\sqrt{2\delta})$-quantum proof extractor. We want the final error of the extractor to be ε; hence we take $\delta = \varepsilon^2/(2 \times 9m^2)$ to get a quantum proof $[8\,\log_2(\frac{m}{\varepsilon}) + m + 2 + 8\,\log_2 3, \varepsilon]$-strong extractor. Now, in order for this extractor to work, we need the min-entropy of the input message to satisfy $k \geqslant 8\,\log_2(\frac{m}{\varepsilon}) + m + 2 + 8\,\log_2 3$. Manipulating this inequality gives us the minimal error the output of the extractor can have:

$$\varepsilon \geqslant 3\, m\, 2^{\frac{2+m-k}{8}}. \tag{B5}$$

Finally, the t from Eq. (B2) is the same appearing in Lemma B.1, related to the $(t,1)$ designs. Since we are bounding the number of devices (and hence seed length), we will ignore the ceiling operators from Lemma B.1, which in the limit of large t and m will be negligible. Hence the seed length for Trevisan's extractor will be $d = \log_2^2(2^9 3^8 \frac{nm^8}{\varepsilon^8}) \frac{\log_2(4m)}{\ln 2}$ (having substituted in the value for δ). If now we take the lowest bound from Eq. (B5) for the error ε we obtain

$$d = (7 + k - m + \log_2 n)^2 \frac{\log_2(4m)}{\ln 2}. \tag{B6}$$

It is interesting to note that the error ε only depends on m and k, having a direct tradeoff between the available min-entropy and how large of an output we desire. Meanwhile, d depends on all parameters but the term $k - m$ has opposite sign, showing qualitatively that the error and seed length are inversely related.

APPENDIX C: RANDOMNESS EXPANSION

In this section, we explicitly analyze the protocol that we are using for expansion, namely the one given by Miller and Shi [15]. In particular, we choose this protocol since it provides cryptographic security, i.e., the error parameters are exponentially small and are negligible in the running time of the protocol. It also tolerates a constant level of noise, where, e.g., it was shown that any device which wins the GHZ game with probability at least 0.985 will achieve exponential randomness expansion with probability approaching unity. Finally, and very important for us, with the Equivalence Lemma (as given by [16]) this is able to produce unbounded expansion using only two devices—by realizing that the expansion protocol is indeed a physical randomness extractor.

In what follows, for simplicity, we will restrict the protocol to playing the GHZ game where the optimum quantum strategy wins with probability 1, and will refer the readers to [15,27] for the generic version.

The unbounded protocol is just a concatenation of their one-shot protocol, so we provide the latter here. For that, we need to define the variables needed: $N \in \mathbb{N}$ is the *output length*, $\eta \in (0, \frac{1}{2})$ the *error tolerance*, denoting how much of a statistical error the components are allowed to make relative to the optimal winning strategy's expectation, and $q \in (0,1)$ the *test probability* which denotes the chance a given round will be a game (Bell) round. The protocol is then as follows.

(1) A bit g is chosen according to the distribution $(1 - q, q)$.

(2) If $g = 1$ ("game round"), then an input string from $\{111, 001, 010, 100\}$ is chosen at random to play the GHZ game. If the GHZ game is won then output 0, else output 1 and record "Failure" F.

(3) If $g = 0$ ("generating round"), the string 111 is used as input on the device $D = (D_1, D_2, D_3)$. Record the output of the first component D_1.

(4) Repeat steps (1)–(3), $(N - 1)$ more times.

(5) If the total number of failures F exceeds $\eta q N$, the protocol *Aborts*. Otherwise, the protocol *Succeeds*, and the output N-bit sequence is recorded.

In general, the one-shot protocol as given above can (for the right choice of parameters η,q,N) provide an output which is ε close to having $(1-\delta)N$ min-entropy for any choice of δ, and ε exponentially small as a function of N. Gross and Aaronson have optimized over the parameters (η,q,N) and given a bound on the initial seed length needed to get unbounded expansion [27]. In particular, they display a linear dependence on $\log_2(1/\varepsilon)$, giving the actual slope to be $\beta = 31328$. Then, they state that the upper bound on seed length needed to get security of $\varepsilon = 10^{-1}$ is 225 000. From this, simple substitution gives $\alpha \leqslant 120931$, and hence Lemma 4.2. We note that they also give a bound of 715 000 bits needed to achieve $\varepsilon = 10^{-6}$, but this gives a lower value of α (= 90 584), so we conservatively kept the upper bound. For asymptotic statements, these constants are irrelevant so long as they remain positive.

APPENDIX D: SECURITY OF RANDOMNESS PROCESSING

In this section, we follow the analysis of [16], to prove the security of our randomness processing protocol, as given in Sec. III of the main text.

Hence, for our analysis, the following theorem is crucial.

Theorem D.1. Chung-Shi-Wu theorem [16]. Let $0<\eta<1$ be the error tolerance parameter. Let X be an n-bit string with k min-entropy. Let $\mathrm{Ext}(k,\varepsilon_T):\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m$, be an m-bit quantum proof extractor, with seed length d. Let there be a protocol Φ (also called physical randomness extractor), which takes a perfectly random seed of length m to produce an output random string z, together with a decision bit $\wr$, with completeness error ε_c and soundness error ε_s. If, for every $S_i\in\{0,1\}^d$, we perform $\Phi[Ext[X,S_i]]=Z_i$, ($Ext[X,S_i]$ being Trevisan's extractor applied on string X using seed S_i), then the protocol producing the output string $\mathcal{Z}=\bigoplus Z_i$ has completeness error $\frac{\varepsilon_c+\varepsilon_T}{\eta}$ soundness error $\varepsilon_s+2\sqrt{\varepsilon_T}+2\eta$, provided less than an η-fraction of protocol Φ applications were rejected.

This is the exact form of the randomness processing protocol that we have given in the main text (Fig. 1), where Φ will be Miller and Shi's unbounded expansion protocol. We will take the MS-expansion security parameter $\varepsilon_s=\varepsilon_c=\varepsilon_{MS}$ given by [27]. Here, we are still left with our errors as functions of m, k, and now (from the previous theorem) η. To have a bound on the security parameter, we will find explicit functions for m and η, depending only on Alice's min-entropy k. We thus have all the ingredients to prove Theorem 4.1. We note however that since this article focuses on a proof of principle, the following proof is done such that it is clear to follow at the expense of not choosing the most optimum coefficient for the exponential decay in the security parameter.

Theorem D.2. Security of randomness processing (Theorem 4.1). If Alice performs the randomness processing protocol on her message $\mathcal{X}$ with min-entropy k, the output string $\mathcal{Z}$ is cryptographically secure. That is, $\exists$ a constant $\gamma>0$ such that the security parameter is $\delta=O(2^{-\gamma k})$.

Proof. Theorem 4.1. We begin by writing the error parameters that arise from the Trevisan extractor as $\varepsilon_T = c_1 m\, 2^{-c_2(k-m)}$, and the one from the Miller and Shi expansion protocol as $\varepsilon_{MS}=c_3\,2^{-c_4 m}$, for some constants c_1,c_2,c_3,c_4, where k is the min-entropy of the message $\mathcal{X}$, and m is both the output length of Trevisan's extractor, and the input size of the expansion protocol. For simplicity, we shall take $m=k/2$, which yields as errors:

$$\varepsilon_T=\frac{c_1}{2}k\,2^{-\frac{c_2}{2}k},$$
$$\varepsilon_{MS}=c_3\,2^{-\frac{c_4}{2}k}.$$

From the Chung-Shi-Wu theorem D.1, we have that the security parameter $\delta=\max\left(\frac{\varepsilon_{MS}+\varepsilon_T}{\eta},\varepsilon_{MS}+2\sqrt{\varepsilon_T}+2\eta\right)$. So we will take $\eta=2^{-\alpha k}$, with a suitably chosen α. To make the security parameter as small as possible, we must choose α large enough so it does not dominate the soundness error but we see that this will bring a tradeoff with the completeness error. In fact, from the completeness error, we have

$$\frac{\varepsilon_{MS}+\varepsilon_T}{\eta}=\frac{c_1}{2}k\,2^{-(\frac{c_2}{2}-\alpha)k}+c_3\,2^{-(\frac{c_4}{2}-\alpha)k}.$$

This requires that $2\alpha<\min(c_2,c_4)$. From the soundness error we have

$$\varepsilon_{MS}+2\sqrt{\varepsilon_T}+2\eta=c_3\,2^{-\frac{c_4}{2}k}+\sqrt{2c_1k}\,2^{-\frac{c_2}{4}k}+2\times2^{-\alpha k}.$$

From here, for the asymptotic statement, we see that we need a choice of α such that the expression $\min\left(\frac{c_2}{2}-\alpha,\ \frac{c_4}{2}-\alpha,\ \frac{c_2}{4},\ \frac{c_4}{2},\ \alpha\right)$ is as big as possible, since those are the coefficients of the exponential decay. Using our actual values for the constants $c_2=1/8$ (from Lemma 4.1), and $c_4=1/31328$ from [27], we see that the best is to take $\alpha=c_4/4=1/125312$. This completes the proof of the theorem, with the security parameter as $\delta=O(2^{-\gamma k})$ with $\gamma\geqslant1/125312$ (since our choice of $m<k$ was the simplest).

In fact, using the same values for the constants c_2,c_4, if we instead take $m=\frac{3916}{3917}k$, and $\eta=2^{-k/62672}$, we can get a better $\tilde{\gamma}=1/62672$, which is almost a factor 2 better than the exponent given in the theorem. Note further that for asymptotic statements, for any $\varepsilon,\alpha>0$, we have $\mathrm{poly}(x)e^{-\alpha x}=O(e^{-(\alpha-\varepsilon)x})$, so that we essentially ignore the prefactors k and $\sqrt{k}$ which appear in the proof.

APPENDIX E: SECURITY OF CDIQKD

In this last section, we prove Theorem 4.2.

Theorem E.1. Security of CDIQKD (Theorem 4.2). Let there be a DIQKD protocol which requires a perfect random number generator, and has completeness and soundness errors (ε_c, ε_s). Then, Alice can perform the randomness processing protocol on her secret message $\mathcal{X}$ with min-entropy k, to produce a secure random output $\mathcal{Z}$ and perform CDIQKD with errors ($\varepsilon_c+\delta$, $\varepsilon_s+\delta$), where $\delta=2^{-\Omega(k)}$.

Proof. Theorem 4.2. We need to check the security of the DIQKD protocol, given that $\mathcal{Z}$ is not perfectly random, but rather has an exponentially small error, $\delta=2^{-\gamma k}$, for constant $\gamma>0$. Let ρ_{ZXDE} be the output state of the randomness processing protocol (conditioned on accepting), then the soundness error just means that $\|\rho_{ZXDE}-U_Z\otimes\rho_{XDE}\|\leqslant\delta$, where D refers to the devices of the DIQKD protocol.

Completeness. The DIQKD completeness error ε_c is calculated expecting perfect randomness in the protocol. Hence

$\mathbb{P}[\mathrm{Rej}(U_Z \otimes \rho_{XDE})] \leqslant \varepsilon_c$. Here $\mathrm{Rej}[\rho]$ denotes the event that the protocol rejects upon input ρ. This immediately implies that $\mathbb{P}[\mathrm{Rej}(\rho_{ZXDE})] \leqslant \varepsilon_c + \delta$, since the trace norm operationally corresponds to the distinguishability of states.

Soundness. Let Λ be the quantum channel of the DIQKD protocol which produces the shared key $\mathcal{Y}$ between Alice and Bob; we write Λ^{Acc} to denote the action of the quantum channel upon acceptance. Let $\Lambda^{\mathrm{Acc}}[U_Z \otimes \rho_{XDE}] = \sigma^{\mathrm{Acc}}_{YZXDE}$; then the soundness error is given by $\|\sigma^{\mathrm{Acc}}_{YZXE} - U_Y \otimes \sigma^{\mathrm{Acc}}_{ZXE}\| \leqslant \varepsilon_s$. From the contractivity of the trace norm under quantum channels, we have $\|\Lambda^{\mathrm{Acc}}[\rho_{ZXDE}] - \Lambda^{\mathrm{Acc}}[U_Z \otimes \rho_{XDE}]\| \leqslant \|\rho_{ZXDE} - U_Z \otimes \rho_{XDE}\| \leqslant \delta$. And by the triangle inequality, we have the new soundness error $\|\psi^{\mathrm{Acc}}_{YZXE} - U_Y \otimes \sigma^{\mathrm{Acc}}_{ZXE}\| \leqslant \varepsilon_s + \delta$, with $\Lambda^{\mathrm{Acc}}[\rho_{ZXDE}] = \psi^{\mathrm{Acc}}_{YZXDE}$.

[1] C. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), Vol. 175.

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

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[4] 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).

[5] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Physics **1**, 195 (1964).

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

[7] U. Vazirani and T. Vidick, Fully Device-independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[8] J. Kofler, T. Paterek, and C. Brukner, Experimenter's freedom in Bell's theorem and quantum cryptography, Phys. Rev. A **73**, 022104 (2006).

[9] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, Weak randomness seriously limits the security of quantum key distribution, Phys. Rev. A **86**, 062308 (2012).

[10] J. Bell, J. Clauser, M. Horne, and A. Shimony, An exchange on local beables, Dialectica **39**, 85 (1985).

[11] J. Menn, Exclusive: Secret contract tied NSA and security industry pioneer, http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220.

[12] R. Colbeck and R. Renner, Free randomness can be amplified, Nat. Phys. **8**, 450 (2012).

[13] 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, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[14] R. Gallego, L. Masanes, G. D. L. Torre, C. Dhara, L. Aolita, and A. Acín, Full randomness from arbitrarily deterministic events, Nat. Commun. **4**, 2654 (2013).

[15] C. A. Miller and Y. Shi, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing, STOC'14* (ACM New York, 2014), pp. 417–426.

[16] K.-M. Chung, Y. Shi, and X. Wu, Physical randomness extractors: Generating random numbers with minimal assumptions, arXiv:1402.4797v3 [quant-ph].

[17] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka, Realistic noise-tolerant randomness amplification using finite number of devices, Nature Commun. **7**, 11345 (2016).

[18] A. De, C. Portmann, T. Vidick, and R. Renner, Trevisan's extractor in the presence of quantum side information, SIAM J. Comput. **41**, 915 (2012).

[19] A. Ekert and R. Renner, The ultimate physical limits of privacy, Nature **507**, 443 (2014).

[20] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[21] L. Trevisan, Extractors and pseudorandom generators, J. ACM **48**, 860 (2001).

[22] R. Raz, O. Reingold, and S. Vadhan, Extracting all the randomness and reducing the error in trevisan's extractors, J. Comput. Syst. Sci. **65**, 97 (2002).

[23] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[24] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, Consequences and limits of nonlocal strategies, in *19th IEEE Annual Conference on Computational Complexity, 2004* (IEEE, New York, 2004), pp. 236–249.

[25] J. Barrett, R. Colbeck, and A. Kent, Unconditionally secure device-independent quantum key distribution with only two devices, Phys. Rev. A **86**, 062326 (2012).

[26] J. Barrett, R. Colbeck, and A. Kent, Memory Attacks on Device-independent Quantum Cryptography, Phys. Rev. Lett. **110**, 010503 (2013).

[27] R. Gross and S. Aaronson, Bounding the seed length of Miller and Shi's unbounded randomness expansion protocol, arXiv:1410.8019v1 [quant-ph].

[28] J. Müller-Quade and R. Renner, Composability in quantum cryptography, New J. Phys. **11**, 085006 (2009).

[29] R. Renner and S. Wolf, Unconditional authenticity and privacy from an arbitrarily weak secret, in *Proceedings of CRYPTO'03* (Springer-Verlag, Berlin, 2003), pp. 78–95.

[30] V. Guruswami, J. Hastad, M. Sudan, and D. Zuckerman, Combinatorial bounds for list decoding, IEEE Trans. Inf. Theory **48**, 1021 (2002).