Simple and Tight Device-Independent Security Proofs

SIAM J. COMPUT.
Vol. 48, No. 1, pp. 181–225

SIMPLE AND TIGHT DEVICE-INDEPENDENT SECURITY PROOFS[*]

ROTEM ARNON-FRIEDMAN[†], RENATO RENNER[†], AND THOMAS VIDICK[‡]

Abstract. Device-independent security is the gold standard for quantum cryptography: not only is security based entirely on the laws of quantum mechanics, but it holds irrespective of any a priori assumptions on the quantum devices used in a protocol, making it particularly applicable in a quantum-wary environment. While the existence of device-independent protocols for tasks such as randomness expansion and quantum key distribution has recently been established, the underlying proofs of security remain very challenging, yield rather poor key rates, and demand very high quality quantum devices, thus making them all but impossible to implement in practice. We introduce a technique for the analysis of device-independent cryptographic protocols. We provide a flexible protocol and give a security proof that provides quantitative bounds that are asymptotically tight, even in the presence of general quantum adversaries. At a high level our approach amounts to establishing a reduction to the scenario in which the untrusted device operates in an identical and independent way in each round of the protocol. This is achieved by leveraging the sequential nature of the protocol and makes use of a newly developed tool, the "entropy accumulation theorem" of Dupuis, Fawzi, and Renner [*Entropy Accumulation*, preprint, 2016]. As concrete applications we give simple and modular security proofs for device-independent quantum key distribution and randomness expansion protocols based on the CHSH inequality. For both tasks, we establish essentially optimal asymptotic key rates and noise tolerance. In view of recent experimental progress, which has culminated in loophole-free Bell tests, it is likely that these protocols can be practically implemented in the near future.

Key words. quantum cryptography, device independence, key distribution, security proofs, randomness

AMS subject classifications. 81P94, 81P45, 81P40, 94A60

DOI. 10.1137/18M1174726

1. Introduction.

Classical cryptography relies on computational assumptions, such as the hardness of factoring, to deliver a wide range of functionalities, from secure communication to secure distributed computation and program obfuscation. The advent of quantum information in the 1980s brought forward a completely different possibility: security based only on the fundamental laws of physics. The quantum protocols for key distribution by Bennett and Brassard [14] and Ekert [31] allow mutually trustful users connected only by an authenticated classical channel, and an arbitrary quantum channel, to establish a private key whose security is guaranteed by the laws of quantum mechanics. With their private key, the users can then communicate with perfect security using, e.g., a one-time pad.

Quantum information is a double-edged sword. A typical protocol for quantum

[*] Received by the editors March 9, 2018; accepted for publication (in revised form) December 19, 2018; published electronically February 26, 2019.

http://www.siam.org/journals/sicomp/48-1/M117472.html

Funding: The research of the first and second authors was supported by the Stellenbosch Institute for Advanced Study (STIAS), by the European Commission via the project "RAQUEL," by the Swiss National Science Foundation via the National Center for Competence in Research, QSIT, and by the Air Force Office of Scientific Research (AFOSR) via grant FA9550-16-1-0245. The third author's research was partially supported by NSF CAREER grant CCF-1553477, an AFOSR YIP award, the IQIM, and the NSF Physics Frontiers Center (NFS grant PHY-1125565) with support from the Gordon and Betty Moore Foundation (GBMF-12500028).

[†] Institute for Theoretical Physics, ETH-Zürich, CH-8093, Zürich, Switzerland (rotemaf@berkeley.edu, renner@phys.ethz.ch).

[‡] Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA 91125 (vidick@cms.caltech.edu).

key distribution (QKD) requires the users, Alice and Bob, to manipulate quantum states: for example, in Ekert's protocol, Alice has to prepare multiple entangled pairs of photons and send one photon from each pair to Bob; both users then perform specific measurements on their respective photons in order to generate the classical key. The first proofs of security for QKD crucially relied on the fact that each user's internal operations were implemented in a specific way: the state preparation implemented by Alice and the measurements performed by Bob all had to follow the low-level prescription given in the protocol. Initial implementations of QKD revealed how delicate these assumptions are. This is not only a question of the quality of the devices used. A wide range of side-channel attacks [33, 48, 79, 35] were able to successfully exploit the very phenomena of quantum mechanics on which the security of QKD relies, such as the no-cloning or uncertainty principles, to provide attacks that did not respect some of the assumptions made by the security proofs, which were difficult, if not impossible, to verify in practice (such as the assumption that Alice prepares a single pair of photons at a time, and not a more complex system with additional, undetected degrees of freedom that could leak information to an eavesdropper).

The paradigm of device independence offers an uncompromising solution to this conundrum. A cryptographic protocol is termed device-independent (DI) if its security guarantees hold irrespective of the quality, or trustworthiness, of the physical devices used to implement the protocol [52, 10] (see [30] for a perspective article). Security in such protocols should be based only on the statistics observed by the honest parties executing the protocol. In other words, any execution of the protocol should contain a "proof" that the generated key is secure, a proof that remains valid as long as very mild assumptions on the physical devices used are satisfied (informally, that no information is exchanged between the users' and eavesdroppers' laboratories, arguably an unavoidable requirement).

Although the formulation of the DI paradigm appeared only much later in work of Mayers and Yao, the possibility for device independence was arguably already present in Ekert's protocol. Ekert's intuition was to tie the privacy of the users' keys to the nonlocal effects that led to the generation of the key (measurement of a Bell pair). Ekert observed that quantum entanglement allows distant parties to generate bits that are correlated in such a strong way that it (seemingly) precludes any correlation with a third party—a phenomenon now known as the monogamy of correlations.

The framework for the study of nonlocality was put in place by Bell in the 1960s [12]. Motivated by questions in the foundations of quantum mechanics (including a proposal for an experiment that could in principle test the EPR "paradox" [29]), Bell introduced the notion of what is now known as a Bell inequality (see [66, 17] for excellent reviews on the topic). In the context of device independence, we interpret a Bell inequality [12] as the specification of a small game[1] that can be played by the honest parties using their respective quantum devices. What makes the game interesting is that it is designed in a way such that any classical strategy for the devices (i.e., any model for their actions that can be implemented as a convex combination of deterministic strategies) leads to a success probability ω_c in the game such that $\omega_c < 1$. In contrast, there exists a quantum strategy (i.e., one in which the devices determine outcomes in the game by performing local measurements on a shared entangled state) that achieves a greater success probability, $\omega_q > \omega_c$. The use of such a game has the following major immediate consequence: if the honest parties observe that their devices are able to attain a success probability that is strictly larger than

[1] For an explicit example of a game, see section 2.3.

ω_c, they can conclude that their devices must be nonclassical—the devices must share entanglement. This provides a first step in the implementation of the DI program: a statistical test that can be performed with the devices and that guarantees some element of quantumness. Early results in device independence went further by establishing a quantitative relationship between the devices' success probability and the amount of secret randomness produced during the game [58, 4], leading to a "statistical test for information-theoretically secure randomness" [22], a task that is provably impossible to achieve using classical systems alone.

In the past decade, an extended line of works has explored the application of the device-independence paradigm to multiple cryptographic tasks. A partial list includes QKD [10, 57, 78], randomness expansion [58, 77, 24, 53] and amplification [23, 34, 19, 15, 45], verified quantum computation [36, 38, 21], bit commitment [5], and weak string erasure [44]. For virtually all these tasks, a proof of security ultimately amounts to bounding the knowledge that an adversary (a malicious party, or an eavesdropper) can gain about the output of the protocol. This knowledge, or uncertainty, is modeled using a notion of entropy called the smooth conditional min-entropy [62]. In the case of QKD, for example, the output is the raw key K, and proving security is essentially equivalent[2] to establishing a lower bound on the smooth conditional min-entropy $H_{\min}^{\varepsilon}(K|E)$, where E is the quantum system held by Eve, which can be initially correlated to the device producing K (for formal definitions, see section 2).

Evaluating the smooth min-entropy $H_{\min}^{\varepsilon}(K|E)$ of a large system is often difficult, especially in the DI setting where not much is known about the way K is produced. One assumption commonly used to simplify this task is that the bits of $K = K_1, \ldots, K_n$ are created in an independent and identical way and hence K itself is an independent and identically distributed (i.i.d.) random variable. That is, it is assumed that the device held by Alice and Bob makes the same measurements on the same quantum states in every round of the protocol. This means that the device is initialized with some (unknown) state which has a tensor product structure $\rho_{AB}^{\otimes n}$ and that the measurements have a tensor product structure as well. In that case, the total entropy in K can be easily related to the sum of the entropies in each round separately.[3] A bound on the entropy accumulated in one round can usually be derived using the expected winning probability in the game played in that round, which in turn can be easily estimated during the protocol in the i.i.d. case using standard Chernoff-type bounds since the same game is just being played repeatedly with the same strategy.

Unfortunately, even though quite convenient (and, in many cases, seemingly necessary) for the analysis, the i.i.d. assumption is a very strong one in the DI scenario. In particular, under such an assumption the device cannot use any internal memory (i.e., its actions in one round cannot depend on the previous rounds) or even display time-dependent behavior (due to inevitable imperfections, for example).

Without this assumption about the device, however, not much is a priori known about the structure of K, the expected winning probability in one round of the protocol, or the way the total entropy of K is accumulated one round after the other (as the device might correlate the different rounds in an almost arbitrary way). Therefore, security proofs that estimated $H_{\min}^{\varepsilon}(K|E)$ directly for the most general case had to

[2] From that point onward, standard classical postprocessing steps, e.g., error correction and privacy amplification, suffice to prove the security of the protocol; see section 5 for the details.

[3] Formally, the bound can be calculated using the quantum asymptotic equipartition property [74], for example.

use far more complicated techniques and statistical analysis compared to the i.i.d. case.[4]

1.1. Results and contributions. We introduce a general framework, consisting of a flexible protocol and analysis, for obtaining DI proofs of security for a broad range of cryptographic tasks. Our technique takes advantage of the sequential nature of the protocol, as well as the specific way in which classical statistics are collected by users of the protocol, to establish a reduction to the i.i.d. setting. A major advantage of our approach is that the reduction is virtually lossless in terms of parameters. Hence, our result establishes the a priori surprising fact that general quantum adversaries are no stronger than an adversary restricted to i.i.d. attacks. As a consequence, we are able to extend tight results known for, e.g., DIQKD, under the i.i.d. assumption, to the most general setting. This yields the best rates known for any protocol for a DI cryptographic task.

To further discuss our results, we state an informal version of our main theorem, which describes the entropy generation guarantees of our protocol (see Lemma 3.2 for a formal statement and Theorem 4.1 for the specialization of the protocol to the CHSH inequality).

Theorem 1.1 (main theorem, informal). *Fix a choice of parameters, including an underlying nonlocal game, for Protocol* 3.1. *Then there exist constants* $c_1, c_2 > 0$ *such that the following holds: Let* D *be any device and* $\rho_{|\Omega}$ *be the state generated using Protocol* 3.1, *conditioned on the protocol not aborting. Then, for any* $\varepsilon_1, \varepsilon_2 \in (0,1)$, *either the protocol aborts with probability greater than* $1-\varepsilon_1$ *or*

$$H_{\min}^{\varepsilon_2}\left(\mathbf{AB}|\mathbf{XYTF}E\right)_{\rho_{|\Omega}} > c_1 n - c_2\sqrt{n\log(1/\varepsilon_1\varepsilon_2)}\ . \tag{1.1}$$

We remark that there are multiple implementations of devices that when used in an execution of Protocol 3.1 lead to a negligible probability of the protocol aborting (this is formalized in our completeness statement; see section 3.2). Importantly, devices that are within reach of current state-of-the-art technology also belong to this set of devices. Thus, Theorem 1.1 gives a nontrivial bound on the entropy produced by such devices. This was not achieved by previous works, as discussed in section 1.2.

Let us explain (1.1). The registers **AB** contain the classical outputs generated by the device during the protocol. The registers **XYTF** contain the classical inputs selected by the users, as well as auxiliary classical information exchanged during the protocol, that may be leaked to the adversary. E is a quantum register that describes the adversary's quantum system, which may be correlated with the initial state of the devices. Thus, (1.1) gives a very precise bound on the amount of the smooth min-entropy present in the users' outputs at the end of the protocol, conditioned on all information available to the adversary. (As we discuss later, this formulation is flexible enough that it can be applied to obtain guarantees not only for the task of randomness generation but also for quantum key distribution and other cryptographic tasks.)

We give explicit formulas for computing the constants c_1 and c_2 that appear in (1.1) as a function of the parameters of the protocol (such as the fraction of rounds used for testing and the threshold value based on which the decision to accept or reject is made). Importantly, the constant c_1 that governs the leading-order term equals the optimal constant, i.e., the same leading constant that would be obtained under the

[4] This led to nonoptimal proofs, both readability- and parameter-wise (e.g., key rates or amount of tolerable noise). See section 1.2 for a discussion of related works.

i.i.d. assumption, which by the asymptotic equipartition property is the Shannon entropy accumulated in one round of the protocol. Thus our result implies that general quantum adversaries do not force weaker rates compared to those achieved in less general scenarios. That is, it is possible to achieve rate vs. noise tradeoffs which are as good as those achieved in much more restricted settings, such as under the i.i.d. assumption.

To determine the constant c_1, the user of our result must perform only one further crucial optimization: identify a so-called "min-tradeoff function," a convex, differentiable function that lower bounds the conditional Shannon entropy generated in a single round of the protocol, as a function of the game value. Informally, the requirement that the min-tradeoff function is differentiable and convex allows one to account for lower-order fluctuations in the entropy generated that arise from finite statistics. In section 4, we give a min-tradeoff function that can be used when the game that underlies the protocol is the CHSH game of Clauser et al. [20]. Other use cases may require other min-tradeoff functions; indeed, in section 1.2 below we survey recent works that applied our results to a variety of scenarios by computing an appropriate min-tradeoff function.

As already mentioned, beyond the first-order term in (1.1) our result also provides control over the constant c_2 in front of the second-order term. Such control is a necessary condition for any application where finite values of n need to be considered, such as in cryptography, and even more so quantum cryptography, where values of n that can be achieved in practice remain relatively small. (See, e.g., Figure 6, where one can see that finite-size effects can play an important role up to even moderately large values of $n \approx 10^{10}$.) As loophole-free Bell tests (a necessity for DI cryptography) are finally being realized [43, 70, 37], the ability to derive essentially optimal values for c_1 and c_2 considerably decreases the gap between theory and experiments, thereby marking an important step towards practical DI protocols and their implementations.

We provide two concrete applications for Theorem 1.1. To begin with, we consider a DIQKD protocol based on the CHSH game and prove its security. The achieved key rates and noise tolerance are significantly higher than in previous works. For large enough number of rounds n, the key rate as a function of the noise tolerance essentially coincides with the optimal result of [57], derived for the restricted i.i.d. and asymptotic case. In particular, as in [57], we show that the protocol can tolerate up to the optimal error rate of 7.1% while still producing a positive key rate. (For comparison,[5] in [78] the maximal noise tolerance was 1.6%.) Moreover, the achieved key rates are comparable to those achieved in device-*dependent* QKD protocols [68, 69] already starting from $n = 10^6$. (For further details and plots, see section 5.5.2.) As a second application we consider a randomness expansion protocol based on the CHSH inequality. Here as well, we obtain an expansion rate which is essentially the same as the optimal rate achieved in [58] in the case of *classical* adversaries only, while our result holds against *quantum* adversaries. This is much better than the rates obtained in previous works [77, 53, 54].

Main ideas of the proof. As expressed earlier, the main difficulty in the analysis is to overcome the lack of any a priori independence assumptions on the quantum state shared by the users' devices, as well as a potential eavesdropper. Towards this we first leverage the sequential nature of the protocol. Our approach is to show that the random variables that model events observed by the users (such as the classical

[5] The noise models of the two works are a bit different; the value of 1.6% is the relevant one after equating the models.

input/output behavior of their device in successive rounds) obey a natural Markov property. Using that property, we are able to apply a newly developed tool, the "entropy accumulation theorem" (EAT) [28], to act as a replacement for the chain rule for the conditional smooth min-entropy. The EAT allows us to quantify how entropy "accumulates" across many random variables generated through a certain iterative quantum processes as long as it fulfils a number of conditions that are tied to the Markov property (see section 2.6 for the exact statement). As a result, we obtain a modular protocol that can be used as a "skeleton" for many DI cryptographic tasks; the protocol comes with fine-tuned guarantees on the entropy that is generated throughout as a function of quantities that can be estimated based on the analysis of a single round of the protocol. Next, we provide a concrete instantiation of the protocol based on the CHSH inequality. By combining the results of [57], derived for the i.i.d. case, with our analysis of the general protocol, we obtain a lower bound on the generated entropy rate when using the CHSH inequality as a basis for the protocol. Finally, we apply our results to prove the security of a DIQKD protocol that we propose, with essentially optimal key rate and noise tolerance.

1.2. Related and subsequent work. The idea of basing the security of cryptographic protocols (QKD especially) on the violation of Bell inequalities originates in the celebrated work of Ekert [31]. Later, Mayers and Yao [52] recognized that devices maximally violating a Bell inequality (they considered a variant of the CHSH inequality) could be fully characterized, up to local degrees of freedom, and thus need not be trusted a priori. Barrett, Hardy, and Kent [10] were the first to combine both ideas together and derive a proof of security for QKD in the DI scenario. Their security proof holds even in the presence of a superquantum adversary, limited only by the nonsignalling principle. The protocol of [10], however, could not tolerate any amount of noise and produced just one secret bit when using the device many times (i.e., the key rate is zero).

Following these initial works, a long line of research [2, 3, 67, 1, 49, 57, 40, 39, 50, 51] led to protocols, and proof techniques, that establish nonvanishing key rates with a positive noise tolerance in the i.i.d. setting against quantum or superquantum adversaries (the former typically leading to better rates and noise tolerance). Most relevant for our work are the results of [57], where the security of a DIQKD protocol was proven in the asymptotic limit, i.e., when the device is used $n \to \infty$ times, and under the i.i.d. assumption described above. Their protocol is based on the CHSH inequality [20], and their analysis shows that it achieves the best possible rates under these assumptions.

For the more challenging scenario presented by the non-i.i.d. setting, security was first established in [78]; see also [61], where the authors give a secure protocol but with vanishing rate and no noise tolerance. A more recent proof of security by Miller and Shi [53] is closest to our results in that it bounds the amount of entropy generated in the protocol in a round-by-round fashion, similar in spirit to (but technically very different from) our use of the EAT (see section 2.6 for a description). The security proofs of the existing works are quite complex and achieve relatively low key rates and noise tolerance (if any).

Although it was introduced only much more recently than QKD, the first task to have received a complete proof of security in the DI setting is the task of randomness expansion. This task, first considered in [22], is the problem of expanding a short initial amount of seed randomness into a longer string that is information-theoretically random; aside from its practical relevance, the task received attention because it is one of the simplest problems that is classically impossible, yet for which quantum computing provides an information-theoretically secure solution. In the non-i.i.d. setting, it was shown in [58] that a quadratic expansion was possible, but the analysis in that paper was limited to the case of classical adversaries. Security against quantum adversaries was established in [77], where it was shown that exponential expansion is possible. The analysis of [77], however, does not tolerate noise in the devices; subsequent work [53] provided a different analysis that is able to tolerate a positive noise rate.

The maximum amount of randomness that can be generated from one system violating a specific Bell inequality by a given amount has been well studied. In [58], tight bounds for the CHSH game are obtained; see, e.g., [26, 46] for recent works exploring different aspects of the question. However, when using the device repeatedly, in the non-i.i.d. setting, few works give explicit rates; to the best of our knowledge, the only quantitative results available are from [54] (see also [59, 32] for an analysis in the non-i.i.d. case but under the assumption that the adversary holds only classical side information) and remain relatively weak in comparison to the best one may expect from the known results under the i.i.d. assumption.

Since the initial announcement of our work in [6],[6] our framework has already been applied to a variety of additional tasks, including conference key agreement [65], randomness expansion and privatization [45], and randomness generation with sublinear quantum resources [8]. Our results have been applied to the analysis of the first experimental implementations of a protocol for randomness generation in the fully DI framework [47, 71]. In all these cases, the difficulty consists in establishing a good min-tradeoff function by analyzing in detail a single round of the protocol used; our results then almost automatically imply the appropriate rate for the n-round protocol. More recently, the second-order terms in the EAT have been improved in [27].

Structure of the paper. The paper is organized as follows. We start with some preliminaries in section 2. In section 3, we show how the EAT can be used in DI protocols for a general Bell inequality. Then, in section 4, we explicitly calculate and plot the entropy rates for the case of the CHSH inequality. We continue in sections 5 and 6 with our DIQKD and randomness expansion protocols, respectively. We end in section 7 with some open questions.

2. Preliminaries.

2.1. General notation.

All logarithms are in base 2. Random variables (RVs) are denoted by capital letters, while specific values are denoted by small letters. We denote vectors in bold face; for example, $\mathbf{X} = X_1, \dots, X_n$ is a vector of RVs. Sets are denoted with calligraphic fonts.

The set $\{1, 2, \dots, n\}$ is denoted by $[n]$.

Given a value $\mathbf{c} = c_1, \dots, c_n \in \mathcal{C}^n$, where $\mathcal{C}$ is a finite alphabet, we denote by $\mathrm{freq}_{\mathbf{c}}$ the probability distribution over $\mathcal{C}$ defined by $\mathrm{freq}_{\mathbf{c}}(\tilde{c}) = \frac{|\{i|c_i=\tilde{c}\}|}{n}$ for $\tilde{c} \in \mathcal{C}$.

We assume familiarity with the standard notation for quantum states and measurements; see [56] for a comprehensive introduction. We generally index pure quantum states or density matrices by the registers on which they are supported; e.g., ρ_{AB} is a density matrix supported on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. If $\rho_{\mathbf{C}E}$ is a state classical on $\mathbf{C}$, we write $\Pr[\mathbf{c}]_\rho$ to denote the probability that ρ assigns to $\mathbf{c}$. For

[6] The publication [6] is an extended abstract that presents the main results reported in this submission, but has a much more limited discussion of applications, and only contains informal proof sketches.

$m \in \mathbb{N}_+$, ρ_{U_m} denotes the completely mixed state on m qubits and $\mathbb{I}$ is the identity operator.

Let $f : \mathcal{S} \to \mathbb{R}$ be a function over some set $\mathcal{S} \subset \mathbb{R}^m$. Then the infinity norm of the gradient of f is defined as

$$\|\nabla f\|_\infty = \sup \left\{ \left| \frac{\partial}{\partial x_i} f(\mathbf{x}) \right| : \mathbf{x} \in \mathcal{S},\, i \in \{1, \ldots, m\} \right\} .$$

For convenience, all important parameters, constants, and RVs used in the paper are listed in the tables in Appendix A.

2.2. Entropies and Markov chains.

Entropies and conditional entropies. h is used for the binary entropy function $h(p) = -p \log(p) - (1-p)\log(1-p)$. The von Neumann entropy $H(\rho)$ of a quantum state ρ is given by $H(\rho) = -\mathrm{Tr}(\rho \log \rho)$. Given a bipartite state $\rho_{AE} \in \mathcal{H}_A \otimes \mathcal{H}_E$, the conditional von Neumann entropy is defined as $H(A|E)_{\rho_{AE}} = H(\rho_{AE}) - H(\rho_E)$. When the state on which the entropy is evaluated is clear from the context, we drop the subscript and write $H(A|E)$.

Min-entropy. Given a state classical on A, $\rho_{AE} = \sum_a p_a \, |a\rangle\langle a| \otimes \rho_E^a$, the conditional min-entropy is

$$H_{\min}(A|E) = -\log p_{\mathrm{guess}}(A|E) \ ,$$

where $p_{\mathrm{guess}}(A|E)$ is the maximum probability of guessing A given the quantum system E:

$$p_{\mathrm{guess}}(A|E) = \max_{\{M_E^a\}_a} \sum_a p_a \mathrm{Tr}(M_E^a \rho_E^a) \ ,$$

and the maximum is taken over all positive-operator valued measures $\{M_E^a\}_a$ on E. For any quantum state ρ_{AE}, $H(A|E) \geq H_{\min}(A|E)$.

The smooth conditional min-entropy with smoothness parameter ε of a state ρ_{AE} is defined to be $H_{\min}^{\varepsilon}(A|E)_{\rho_{AE}} = \max_{\sigma_{AE} \in \mathcal{B}^{\varepsilon}(\rho_{AE})} H_{\min}(A|E)_{\sigma_{AE}}$, for $\mathcal{B}^{\varepsilon}(\rho_{AE})$ the set of subnormalized states σ_{AE} with $P(\rho_{AE}, \sigma_{AE}) \leq \varepsilon$, where P is the purified distance [75].

Max-entropy. The quantum smooth max-entropy of a state ρ_{AE} is given by

$$H_{\max}^{\varepsilon}(A|E)_{\rho_{AE}} = \log \inf_{\sigma_{AE} \in \mathcal{B}^{\varepsilon}(\rho_{AE})} \sup_{\tau_E} \|\sigma_{AE}^{\frac{1}{2}} \tau_E^{-\frac{1}{2}}\|_1^2 \ .$$

We will also use the closely related H_0^{ε} entropy. For classical $\mathbf{X}$ and $\mathbf{Y}$ distributed according to $\mathrm{P}_{\mathbf{XY}}$, $H_0(\mathbf{X}|\mathbf{Y}) = \max_{\mathbf{y}} \log \left|\mathrm{Supp}\left(\mathrm{P}_{\mathbf{X}|\mathbf{Y}=\mathbf{y}}\right)\right|$, where $\mathrm{Supp}\left(\mathrm{P}_{\mathbf{X}|\mathbf{Y}=\mathbf{y}}\right) = \{\mathbf{x} | \mathrm{P}_{\mathbf{X}|\mathbf{Y}=\mathbf{y}}(\mathbf{x}) > 0\}$. Its smooth version is given by

$$H_0^{\varepsilon}(\mathbf{X}|\mathbf{Y}) = \min_{\Omega} \max_{\mathbf{y}} \log \left|\mathrm{Supp}\left(\mathrm{P}_{\mathbf{X}|\Omega, \mathbf{Y}=\mathbf{y}}\right)\right| \ ,$$

where the minimum ranges over all events Ω with probability at least $1 - \varepsilon$.

Markov chains. A tripartite quantum state ρ_{ABC} is said to fulfil the Markov chain condition $A \leftrightarrow B \leftrightarrow C$ if $I(A : C|B) = 0$, where $I(A : C|B) = H(AB) + H(BC) - H(B) - H(ABC)$ is the conditional mutual information. $I(A : C|B) = 0$ if and only if given B, A and C are independent.[7]

[7] There are also other equivalent ways of defining Markov chains for quantum states [42], but for our purposes this definition suffices.

2.3. Nonlocal games. We consider general two-player nonlocal games G. In a game G, the two players, Alice and Bob, share a bipartite quantum state. Given a question for Alice and a question for Bob, they can choose how to measure their parts of the state and then use the measurement outcomes to supply an answer each. They win if their answers fulfil a predefined requirement, called the winning criterion.

More formally, a game G is defined via sets of questions and answers for Alice and Bob, $\mathcal{X}, \mathcal{Y}$ and $\mathcal{A}, \mathcal{B}$, a distribution π over $\mathcal{X} \times \mathcal{Y}$ (we will generally assume this is a product distribution), and a winning criterion $w : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$.[8]

A strategy for the players in a game G is specified by, first, a bipartite state $\rho_{Q_A Q_B}$, where Alice holds register Q_A and Bob register Q_B, and, second, local measurements that each player performs on his or her register in order to determine the answer to the given question. We use $\omega \in [0, 1]$ to denote the winning probability of a strategy in the game G.

We sometimes use the equivalent language of Bell inequalities. The Bell functional associated to a nonlocal game is the linear function from $\mathbb{R}^{\mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B}}$ to $\mathbb{R}$ that maps a tuple p to $\sum_{x,y,a,b} \pi(x, y)w(x, y, a, b)p(x, y, a, b)$. In this language, the quantum value of the game is also called the largest violation of the Bell inequality, i.e., the largest value attained by the Bell functional when evaluated on tuples p that correspond to conditional distributions that can be realized by performing local measurements on an entangled state.

The CHSH game. We use a variant of the CHSH game previously used in [57, 78] in the context of DIQKD. In this game, Alice has two possible inputs $\mathcal{X} = \{0, 1\}$ and Bob three possible inputs $\mathcal{Y} = \{0, 1, 2\}$. The output sets are $\mathcal{A} = \mathcal{B} = \{0, 1\}$. The input distribution π_{CHSH} is uniform on $\mathcal{X} \times \mathcal{Y}$. The winning condition is the following:[9]

$$w_{\mathrm{CHSH}} = \begin{cases} 1, & x, y \in \{0, 1\} \text{ and } a \oplus b = x \cdot y, \\ 1, & (x, y) = (0, 2) \text{ and } a = b, \\ 0 & \text{otherwise.} \end{cases}$$

The optimal quantum strategy for this game is the same as in the standard CHSH game [20], except that if Bob's input is a 2, he applies the same measurement as Alice's measurement on input 0. Since the underlying state is maximally entangled, this ensures that their outputs will always match when $(x, y) = (0, 2)$.

Conditioned on Bob's input not being 2, the game played is the CHSH game. The optimal quantum strategy in the CHSH game achieves winning probability $\omega = \frac{2+\sqrt{2}}{4} \approx 0.85$, while the optimal classical strategy achieves a winning probability of 0.75.

Instead of describing the quantum advantage in the CHSH game in terms of the winning probability, one can also work with the correlation coefficients defined by $E_{xy} = \Pr[a = b|x, y] - \Pr[a \neq b|xy]$ for any pair of inputs (x, y). The CHSH value is then given by $\beta = E_{00} + E_{01} + E_{10} - E_{11}$. The relation between the winning probability in the CHSH game and the CHSH value is given by $\omega = 1/2 + \beta/8$. The largest values that these quantities can take in the classical case are $\beta = 2$ and $\omega = \frac{3}{4}$, and the optimal quanta are $\beta = 2\sqrt{2}$ and $\omega = \frac{2+\sqrt{2}}{4}$.

2.4. Untrusted device. In a DI protocol, the honest parties interact with an *untrusted device*. We now explain what is meant by this term and what the assump-

[8] A general Bell inequality would allow for an $\mathbb{R}$-valued w; we will not need this here.

[9] The value of w_{CHSH} for the inputs $(x, y) = (1, 2)$ is left undefined, as it is never used.

tions regarding such a device are. For simplicity, we consider the case of two honest parties, Alice and Bob, but this can be extended to more parties in the obvious way.

A device D is modeled by a tripartite apparatus (including both state and measurement devices), distributed between Alice, Bob, and the adversary Eve. We think of the device as being prepared by Eve, and hence we call it untrusted. This allows Eve, in particular, to keep a purification of Alice and Bob's quantum state in a quantum register in her possession.[10] Although the device is untrusted, we always assume that the following requirements hold (some of these requirements can be verified).

The device can be used to run the considered protocol. That is, Alice and Bob can interact with D according to the relevant protocol (for an example of a protocol, see Protocol 3.1 below). Alice and Bob's components of D implement the protocol by making sequential measurements on quantum states. In each round of the protocol, we say that the device is implementing some strategy for the game G being played. The device may have memory, and thus apply a different strategy each time the game is played, depending on the previous rounds. Therefore, the measurement operators may change in each round, and the state on which the measurements are performed may be the postmeasurement state from the previous round, a new state, or any combination of these two.

We sometimes use the terminology *honest device* or *honest implementation.* A device is said to be honest if it implements the protocol by using a certain prespecified strategy. In that case, the actions of the device are known and fixed (noise can still be present).

Communication (signaling) between the components of the device. The communication between Alice, Bob, and Eve's components is restricted in the following way:

1. Alice and Bob's components of D cannot signal to Eve's component.
2. Alice and Bob can decide when to allow communication (if any) between their components. This ensures that the underlying quantum state of Alice and Bob's components of the device is (at least) bipartite and that the measurements made in the two components, in each round, are in tensor product with one another.
3. Alice and Bob can decide when to receive communication (if any) from Eve's component.

The requirement given in Item 1 is necessary for DI cryptography; without it, the device could directly send to Eve all the raw data it generated.

Item 2 implies that Alice and Bob's component must be (at least) bipartite. This is necessary to assure that the violation of the considered Bell inequality is meaningful and implies security.

Items 2 and 3 give Alice, Bob, and Eve's components the possibility to communicate in certain stages of the protocol. This is neither a restrictive nor a necessary assumption. This possibility to communicate is added since it is advantageous to actual implementations of certain protocols. To be specific, we consider the following scenario: *In between* different rounds of the protocol, Alice and Bob's components of the device are allowed to communicate freely. During the execution of a single round, however, no communication is allowed. In particular, when the game is being played, there is no communication between the components once the honest parties'

[10] We emphasise that Eve is not required to measure her quantum state at any particular point. During the run of the considered protocol, Eve can eavesdrop on all the classical communication between the honest parties and can later choose to measure her quantum register depending on this information.

inputs are chosen and until the outputs are supplied by the device.[11] Furthermore, in between rounds Eve may send information to the device but not receive any from it. In actual implementations, this implies that entanglement can be distributed "on the fly" for each round of the protocol, instead of maintaining large quantum memories.

Other assumptions. Apart from the above description of the untrusted device, we assume the following other standard assumptions used in DI cryptography:

1. The honest parties' physical locations are secure (unwanted information cannot leak outside to Eve or between their devices).
2. The honest parties have a trusted random number generator.
3. The honest parties have trusted classical postprocessing units to make the necessary (classical) calculations during the protocol.
4. There is an authenticated, but public, classical channel connecting the honest parties (if necessary).
5. Quantum physics is correct.

2.5. Security definitions.

DIQKD. A DIQKD protocol (see section 5 for a description of an explicit protocol) consists of an interaction between two trusted parties, Alice and Bob, and an untrusted device as defined in section 2.4. At the end of the protocol, each party outputs a key, $\tilde{K}_A$ for Alice and $\tilde{K}_B$ for Bob. The goal of the adversary, Eve, is to gain as much information as possible about Alice and Bob's keys without being detected (i.e., in the case where the protocol is not being aborted).

Correctness, secrecy, and overall security of a protocol are defined as follows (see also [60, 11]).

Definition 2.1 (correctness). *A DIQKD protocol is said to be ε_{corr}-correct, when implemented using a device D, if Alice and Bob's keys, $\tilde{K}_A$ and $\tilde{K}_B$, respectively, are identical with probability at least $1-\varepsilon_{corr}$. That is,* $\Pr(\tilde{K}_A \neq \tilde{K}_B) \leq \varepsilon_{corr}$.

Definition 2.2 (secrecy). *A DIQKD protocol is said to be ε_{sec}-secret, when implemented using a device D, if for a key of length l, $(1-\Pr[abort])\,\|\rho_{\tilde{K}_A E} - \rho_{U_l} \otimes \rho_E\|_1 \leq \varepsilon_{sec}$, where E is a quantum register that may initially be correlated with D.*

ε_{sec} in the above definition can be understood as the probability that some nontrivial information leaks to the adversary [60].

If a protocol is ε_{corr}-correct and ε_{sec}-secret (for a given D), then it is $\varepsilon^s_{\mathrm{QKD}}$-correct-and-secret for any $\varepsilon^s_{\mathrm{QKD}} \geq \varepsilon_{corr} + \varepsilon_{sec}$.

Definition 2.3 (security). *A DIQKD protocol is said to be $(\varepsilon^s_{\mathrm{QKD}}, \varepsilon^c_{\mathrm{QKD}}, l)$-secure if the following hold:*

1. *(Soundness) For* any *implementation of the device D, it is $\varepsilon^s_{\mathrm{QKD}}$-correct-and-secret.*
2. *(Completeness) There exists an honest implementation of the device D such that the protocol aborts with probability at most $\varepsilon^c_{\mathrm{QKD}}$.*

The protocols that we consider below take into account possible noise in the honest implementation. That is, even when there is no adversary at all, the actual implementation of the devices might not be perfect. Thus, the *completeness* of the protocol implies its *robustness* to the desired amount of noise.

Last, a remark regarding the composability of this security definition is in order.

[11] To be more precise and concrete, in Protocol 3.1, for example, communication is allowed in every round i right after step 4 is done, and until the beginning of round $i+1$, i.e., before T_{i+1} is chosen.

A security definition is said to be composable [18, 13, 60] if it implies that the protocol can be used arbitrarily and composed with other protocols (proven secure by themselves), without compromising security. Obviously, if Alice and Bob wish to use the keys they produced in the DIQKD protocol in some other cryptographic protocol (i.e., they compose the two protocols), it is necessary for them to use protocols which were proven to have composable security.

For the case of (device-*dependent*) QKD, Definition 2.3 was rigorously proven to be composable [60]. This suggests that the same security definition should also be the relevant one in the DI context, and, indeed, as far as we are aware, it is the definition that has been used in all prior works on DI cryptography. Nevertheless, the claim that Definition 2.3 is composable for DI protocols as well has never been rigorously proven, and the result of [9] suggests that this is not the case when the same devices are reused in the composition. We still use this definition, as it seems like the most promising security definition to date. This implies that, as in all other works, *after the end of the protocol* the device cannot be used again in general [9].

Randomness expansion. In the task of randomness expansion, there is a single user interacting sequentially with an untrusted device. At the start of the interaction, the user is presented with a source $R \in \{0,1\}^r$ of uniformly random bits. The user then interacts sequentially with the device in a deterministic way (the only sources of randomness being the initial string R and any randomness which may be present in the devices' outputs). At the end of the protocol, the user returns a string $Z \in \{0,1\}^m$ of m bits that is statistically close to uniform, conditioned on R as well as any side information of the adversary. (See section 6 for a concrete example of a randomness expansion protocol.) More formally, we require the following.

DEFINITION 2.4 (security of randomness expansion). *A protocol is said to be called an $(\varepsilon^c_{RE}, \varepsilon^s_{RE})$-secure $r \to m$ randomness expansion protocol*[12] *if, provided as input r uniformly random bits, the following hold:*

1. *(Soundness) For any implementation of the device D, the protocol either aborts or returns a classical string $Z \in \{0,1\}^m$ and we have*

$$(1 - \Pr[abort])\, \|\rho_{ZRE} - \rho_{U_m} \otimes \rho_{RE}\|_1 \leq \varepsilon^s_{RE}\ ,$$

   where E is a quantum register that may initially be correlated with D.
2. *(Completeness) There exists an honest implementation of the device such that the protocol aborts with probability at most ε^c_{RE}.*

As in the case of DIQKD, this security definition was not proven to be composable in general.

2.6. The entropy accumulation theorem.

2.6. The entropy accumulation theorem. The main tool used in this work is the EAT [28, Theorem 4.4]. Below we give the necessary details in a notation appropriate for our work (although less general than the original EAT).

We work with channels with the following properties.

DEFINITION 2.5 (EAT channels). *EAT channels $\mathcal{N}_i : R_{i-1} \to R_i A_i B_i I_i C_i$, for $i \in [n]$, are completely positive and trace-preserving (CPTP) maps such that for all $i \in [n]$, the following hold:*

[12] All parameters ε^c_{RE}, ε^s_{RE}, r, and m will in general be functions of a parameter n that also parameterizes the protocol and the number of rounds of interactions between the user and the device.

1. *A_i, B_i, I_i, and C_i are finite-dimensional classical systems (RVs). A_i and B_i are of dimensions d_{A_i} and d_{B_i}, respectively. R_i are arbitrary quantum registers.*
2. *For any input state $\sigma_{R_{i-1}R'}$, where R' is a register isomorphic to R_{i-1}, the output state $\sigma_{R_iA_iB_iI_iC_iR'} = (\mathcal{N}_i \otimes \mathbb{I}_{R'})\left(\sigma_{R_{i-1}R'}\right)$ has the property that the classical value C_i can be measured from the marginal $\sigma_{A_iB_iI_i}$ without changing the state.*
3. *For any initial state $\rho^0_{R_0E}$, the final state $\rho_{\mathbf{ABIC}E} = (\mathrm{Tr}_{R_n} \circ \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1) \otimes \mathbb{I}_E\ \rho^0_{R_0E}$ fulfils the Markov chain condition $A_{1\dots i-1}B_{1\dots i-1} \leftrightarrow I_{1\dots i-1}E \leftrightarrow I_i$ for each $i \in [n]$.*

Definition 2.6 (tradeoff functions). *Let $\mathcal{N}_1, \dots, \mathcal{N}_N$ be a family of EAT channels. Let $\mathcal{C}$ denote the common alphabet of $C_1, \dots, C_n$. A differentiable and convex function $f_{\min}$ from the set of probability distributions p over $\mathcal{C}$ to the real numbers is called a* min-tradeoff function *for $\{\mathcal{N}_i\}$ if it satisfies*[13]

$$f_{\min}(p) \leq \inf_{\sigma_{R_{i-1}R'}:\mathcal{N}_i(\sigma)_{C_i}=p} H\left(A_iB_i|I_iR'\right)_{\mathcal{N}_i(\sigma)}$$

for all $i \in [n]$, where the infimum is taken over all input states of $\mathcal{N}_i$ for which the marginal on C_i of the output state is the probability distribution p.

Similarly, a differentiable and concave function $f_{\max}$ from the set of probability distributions p over $\mathcal{C}$ to the real numbers is called a max-tradeoff function *for $\{\mathcal{N}_i\}$ if it satisfies*

$$f_{\max}(p) \geq \sup_{\sigma_{R_{i-1}R'}:\mathcal{N}_i(\sigma)_{C_i}=p} H\left(A_iB_i|I_iR'\right)_{\mathcal{N}_i(\sigma)}$$

for all $i \in [n]$, where the supremum is taken over all input states of $\mathcal{N}_i$ for which the marginal on C_i of the output state is the probability distribution p.

Theorem 2.7 (EAT [28]). *Let $\mathcal{N}_i : R_{i-1} \to R_iA_iB_iI_iC_i$ for $i \in [n]$ be EAT channels as in Definition 2.5, $\rho_{\mathbf{ABIC}E} = (\mathrm{Tr}_{R_n} \circ \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1) \otimes \mathbb{I}_E\ \rho_{R_0E}$ the final state, Ω an event defined over $\mathcal{C}^n$, p_Ω the probability of Ω in ρ, and $\rho_{|\Omega}$ the final state conditioned on Ω. Let $\varepsilon_s \in (0,1)$.*

For $f_{\min}$ a min-tradeoff function for $\{\mathcal{N}_i\}$ as in Definition 2.6 and any $t \in \mathbb{R}$ such that $f_{\min}(\mathrm{freq}_{\mathbf{c}}) \geq t$ for any $\mathbf{c} \in \mathcal{C}^n$ for which $\Pr[\mathbf{c}]_{\rho_{|\Omega}} > 0$,

$$H^{\varepsilon_s}_{\min}\left(\mathbf{AB}|\mathbf{I}E\right)_{\rho_{|\Omega}} > nt - v\sqrt{n}\ ,$$

where $v = 2\left(\log(1+2d_{A_iB_i}) + \lceil\|\nabla f_{\min}\|_\infty\rceil\right)\sqrt{1-2\log(\varepsilon_s\cdot p_\Omega)}$ and $d_{A_iB_i}$ denotes the dimension of A_iB_i.

Similarly, for $f_{\max}$ a max-tradeoff function for $\{\mathcal{N}_i\}$ as in Definition 2.6 and any $t \in \mathbb{R}$ such that $f_{\max}(\mathrm{freq}_{\mathbf{c}}) \leq t$ for any $\mathbf{c} \in \mathcal{C}^n$ for which $\Pr[\mathbf{c}]_{\rho_{|\Omega}} > 0$,

$$H^{\varepsilon_s}_{\max}\left(\mathbf{AB}|\mathbf{I}E\right)_{\rho_{|\Omega}} < nt + v\sqrt{n}\ ,$$

where $v = 2\left(\log(1+2d_{A_iB_i}) + \lceil\|\nabla f_{\max}\|_\infty\rceil\right)\sqrt{1-2\log(\varepsilon_s\cdot p_\Omega)}$.

To gain a bit of intuition on how Theorem 2.7 is going to be used, note the following. The event Ω will usually be the event of the considered protocol not aborting (or

[13] The infimum and supremum over the empty set are defined as plus and minus infinity, respectively.

a closely related event). The relevant state for which the smooth min- or max-entropy is going to be evaluated is $\rho_{|\Omega}$. To use the theorem, it should be possible to define *some* EAT channels $\{\mathcal{N}_i\}$ that produce the final state ρ from the initial state ρ_{R_0} by applying the channels sequentially; these channels are not necessarily the channels used in the actual protocol to produce ρ. The tradeoff functions can be seen as a bound on the entropy accumulated in *one* round i, and, if such a bound t exists, then Theorem 2.7 asserts that the total amount of entropy, accumulated in all rounds $i=1$ to n together, is roughly n times t. It is in this sense that the theorem essentially allows us to perform a reduction to the i.i.d. setting.

3. DI entropy accumulation protocol.

The main task in proving the security of DIQKD and other protocols is to prove a bound on the (smooth) min-entropy of the raw data held by Alice and Bob, conditioned on all the information available to the adversary Eve. The goal of this section is to show how the EAT (Theorem 2.7) can be used in a general DI setting to achieve such a bound.

For this, we consider the entropy accumulation protocol, described as Protocol 3.1 below. Although we call it a "protocol," one should see it more as a mathematical tool which allows us to use the EAT rather than an actual protocol to be implemented.[14] To be more specific, the EAT channels (as in Definition 2.5) will be defined via the steps made in the entropy accumulation protocol. The relevance of the protocol stems from the fact that the final state at the end of the protocol, on which a smooth min-entropy bound can be proven using the EAT, is the same state as (or can easily be related to) the final state in the actual protocol to be executed (depending on the specific application).

3.1. The protocol.

Protocol 3.1 is used to generate raw data for Alice and Bob by using an untrusted device D. It is based on an arbitrary nonlocal game G as defined in section 2.3, together with a definition of test and generation inputs for Alice and Bob. The test inputs, $\mathcal{X}_t \subset \mathcal{X}$ and $\mathcal{Y}_t \subset \mathcal{Y}$, are used by the parties during the test rounds ($T_i = 1$ below) from which the Bell violation is estimated, while the generation inputs, $\mathcal{X}_g \subset \mathcal{X}$ and $\mathcal{Y}_g \subset \mathcal{Y}$, are used in the other rounds (the sets are not necessarily disjoint). We also assume that $\mathcal{X}_g \subset \mathcal{X}_t$, as it is important that, given a value in $\mathcal{X}_g$, the device is not able to infer the value of T_i. Ideally, one should use a game G for which Alice and Bob's outputs are perfectly correlated (or anticorrelated) with sufficiently high probability when the parties use the generation inputs.[15]

We now define the EAT channels using the rounds of the protocol (where one round includes steps 2–6 in Protocol 3.1). For this, the following notation is used. For every $i \in \{0\} \cup [n]$, the (unknown) quantum state of the device D shared by Alice and Bob after round i of the protocol is denoted by $\rho^i_{Q_A Q_B}$. We denote the register holding this state by R_i. In particular, $R_0 \equiv Q_A Q_B$ at the start of the protocol. At step 4 in Protocol 3.1, the quantum state of the devices is changed from $\rho^{i-1}_{Q_A Q_B}$ in R_{i-1} to $\rho^i_{Q_A Q_B}$ in R_i by the use of the device.[16] Our EAT channels are then

[14] In particular, in a setting with two distinct parties, Alice and Bob, communication is required to actually implement it. We ignore this here, as it is not relevant for the analysis.

[15] In a DIQKD protocol (or other tasks with two separated honest parties), this requirement is used to ensure a good key rate, as the output bits in the generation rounds will be the main contributors to the final key. For tasks such as randomness expansion, where there is only one honest party, it is not necessary to generate matching outputs.

[16] To be a bit more precise, the quantum state is changed in two steps. First, the relevant measurement of step 4 is done (where it is assumed that the measurements of the different components are in tensor product). Then, after A_i and B_i are recorded, the different components of the device are allowed to communicate. Thus, some further changes can be made to the postmeasurement state even based on the memory of all components together.

Protocol 3.1 Entropy accumulation protocol.

```
Arguments:
    $G$ – two-player nonlocal game
    $\mathcal{X}_g \subset \mathcal{X}_t \subset \mathcal{X}$ – generation and test inputs for Alice
    $\mathcal{Y}_g, \mathcal{Y}_t \subset \mathcal{Y}$ – generation and test inputs for Bob
    $D$ – untrusted device of (at least) two components that can play $G$ repeatedly
    $n \in \mathbb{N}_+$ – number of rounds
    $\gamma \in (0,1]$ – expected fraction of test rounds
    $\omega_{\text{exp}}$ – expected winning probability in $G$ for an honest (perhaps noisy) implementation
    $\delta_{\text{est}} \in (0,1)$ – width of the statistical confidence interval for the estimation test

1: For every round $i \in [n]$ do steps 2–6:
2:     Alice chooses $T_i \in \{0,1\}$ at random such that $\Pr(T_i = 1) = \gamma$ and sends her choice of $T_i$ to Bob over a public authenticated classical channel.
3:     If $T_i = 0$, Alice and Bob choose inputs $X_i \in \mathcal{X}_g$ and $Y_i \in \mathcal{Y}_g$, respectively. If $T_i = 1$, they choose inputs $X_i \in \mathcal{X}_t$ and $Y_i \in \mathcal{Y}_t$.
4:     Alice and Bob use $D$ with $X_i, Y_i$ and record their outputs as $A_i$ and $B_i$, respectively.
5:     (Optional symmetrization step): Alice and Bob choose together a (random) value $F_i$ and respectively update their outputs $A_i, B_i$ depending on $F_i$.
6:     If $T_i = 0$, then Bob updates $B_i$ to $B_i = \perp$, and they set $C_i = \perp$. If $T_i = 1$, they set $C_i = w(A_i, B_i, X_i, Y_i)$.
7: Alice and Bob abort if $\sum_i C_i < (\omega_{\text{exp}}\gamma - \delta_{\text{est}}) \cdot n$ .
```

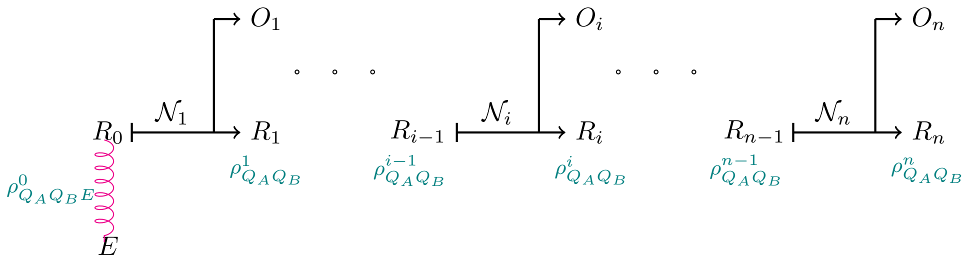

FIG. 1. *The EAT channels $\mathcal{N}_i : R_{i-1} \to R_i A_i B_i X_i Y_i T_i C_i$. In the figure, $O_i = A_i B_i X_i Y_i T_i C_i$. The initial quantum state shared by Alice, Bob, and Eve is $\rho^0_{Q_AQ_BE}$, and the sequence of maps $\mathcal{N}_i$ creates the state $\rho^n_{Q_AQ_BE\mathbf{O}}$.*

$\mathcal{N}_i : R_{i-1} \to R_i A_i B_i X_i Y_i T_i C_i$ defined by the CPTP map describing the ith round of Protocol 3.1, as implemented by the untrusted device D (see Figure 1). We prove in Lemma 3.2 below that they indeed satisfy the conditions given in Definition 2.5.

In the following, we are interested in the state of Alice, Bob, and Eve after the nth round of the protocol, both before and after Alice and Bob decide whether or not to abort in step 7. The state *before* step 7 is denoted by

$$\rho_{\mathbf{ABXYTC}E} = (\mathrm{Tr}_{R_n} \circ \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1) \otimes \mathbb{I}_E \, \rho^0_{Q_AQ_BE} \, . \tag{3.1}$$

In step 7, Alice and Bob decide whether or not they should abort the protocol according to the estimated Bell violation in the test rounds. Let Ω denote the event that they do not abort,[17] i.e.,

$$\Omega = \left\{ \sum_j C_j \geq (\omega_{\mathrm{exp}}\gamma - \delta_{\mathrm{est}}) \cdot n \right\} . \tag{3.2}$$

The final state, *conditioned on not aborting*, is denoted by $\rho_{\mathbf{ABXYTC}E|\Omega}$ or just $\rho_{|\Omega}$ to ease notation. Below we bound the entropy which is accumulated in this state during the rounds of the protocol.

3.2. Completeness. Suppose that Alice and Bob execute Protocol 3.1 with a device D which performs i.i.d. measurements on a tensor product state $\rho_{Q_AQ_B}^{\otimes n}$ such that the winning probability achieved in game G by the device D executed on a single state $\rho_{Q_AQ_B}$ is ω_{exp}. We call any such implementation an *honest implementation*. The following lemma bounds the probability of Protocol 3.1 aborting in an honest implementation.

LEMMA 3.1. *Protocol* 3.1 *is complete with completeness error* $\varepsilon_{EA}^{c} \leq \exp(-2n\delta_{\mathrm{est}}^2)$. *That is, the probability that the protocol aborts for an honest implementation of the devices* D *is at most* ε_{EA}^{c}.

Proof. Alice and Bob abort in step 7 when the sum of the C_i is not sufficiently high (this happens when the estimated Bell violation is too low or when not enough test rounds were chosen). In the honest implementation, C_i are i.i.d. RVs with $\mathbb{E}\left[C_i\right] = \omega_{\mathrm{exp}}\gamma$. Therefore, we can use Hoeffding's inequality:

$$\varepsilon_{EA}^{c} = \Pr\left[\sum_j C_j \geq (\omega_{\mathrm{exp}}\gamma - \delta_{\mathrm{est}}) \cdot n\right] \leq \exp(-2n\delta_{\mathrm{est}}^2) \; . \tag{3.3}$$ □

3.3. Soundness. The EAT, Theorem 2.7, almost immediately provides a general lower bound on the amount of entropy generated by Protocol 3.1. We state the result as Lemma 3.2 below; in section 4, we will obtain a more refined bound based on an instantiation of the protocol with the game G taken to be the CHSH game.

LEMMA 3.2. *Let* D *be any device, and for* $i \in [n]$, *let* $I_i = X_iY_iT_iF_i$ *and* $\mathcal{N}_i : R_{i-1} \to R_iA_iB_iI_iC_i$ *be the CPTP map implemented by the ith round of Protocol* 3.1. *Let* ρ *be the state generated by the protocol (as defined in* (3.1)*),* Ω *the event that the protocol does not abort (as defined in* (3.2)*), and* $\rho_{|\Omega}$ *the state conditioned on* Ω. *Let* f_{min} *be a real-valued differentiable function defined on the set of probability distributions* p *over the alphabet* $\{\perp, 0, 1\}$ *of* C_i *such that*

$$\forall i \in [n], \qquad f_{\min}(p) \leq \inf_{\sigma_{R_{i-1}R'}:\mathcal{N}_i(\sigma)_{C_i}=p} H\left(A_iB_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} \; , \tag{3.4}$$

where the infimum over an empty set is defined as infinity. Then, for any $\varepsilon_{\mathrm{EA}}, \varepsilon_s \in (0,1)$, *either the protocol aborts with probability* $1 - \Pr(\Omega) \geq 1 - \varepsilon_{\mathrm{EA}}$ *or*

$$H_{\min}^{\varepsilon_s}\left(\mathbf{AB}|\mathbf{XYTF}E\right)_{\rho_{|\Omega}} > nt - v\sqrt{n}, \tag{3.5}$$

where

$$\begin{aligned} t &= \min_{p:\, p(1) \geq \omega_{\mathrm{exp}}\gamma - \delta_{\mathrm{est}}} f_{\min}(p) \; , \\ v &= 2\left(\log(1 + 2d_{A_iB_i}) + \lceil \|\nabla f_{\min}\|_\infty \rceil\right)\sqrt{1 - 2\log(\varepsilon_s \cdot \varepsilon_{\mathrm{EA}})}, \end{aligned}$$

[17] Note that $C_j \in \{0, 1, \perp\}$; the quantity $\sum_j C_j$ should be understood as $\sum_{j|C_j=1} 1$.

and $d_{A_iB_i}$ *denotes the dimension of* A_iB_i*.*

Proof. In order to apply the EAT, we first verify that the conditions stated in Definition 2.5 are fulfilled. Using that C_i is a function of A_i, B_i, X_i, and Y_i, the first two conditions in Definition 2.5 clearly hold. Moreover, the Markov chain condition

$$\forall i \in [n], \quad A_{1\dots i}B_{1\dots i} \leftrightarrow X_{1\dots i}Y_{1\dots i}T_{1\dots i}F_{1\dots i}E \leftrightarrow X_{i+1}Y_{i+1}T_{i+1}F_{i+1}$$

holds as well since the values of X_{i+1}, Y_{i+1}, T_{i+1}, and F_{i+1} are chosen independently of everything else at each round. To conclude, note that the event Ω of the protocol not aborting implies that the fraction of successful game rounds $\text{freq}_{\mathbf{c}}(1)$ is at least $\omega_{\text{exp}}\gamma - \delta_{\text{est}}$ for any $\mathbf{c}$ for which $\Pr[\mathbf{c}]_{\rho_{|\Omega}} > 0$. □

The main work remaining for a successful use of Protocol 3.1 for entropy generation consists in obtaining a good lower bound in (3.5), i.e., devising an appropriate min-tradeoff function $f_{\min}$ satisfying (3.4). In order to understand the task to be accomplished, note that $\mathcal{N}_i$ defines X_i, Y_i, T_i, and F_i, so although the infimum in (3.4) is taken over all states σ, the distributions of X_i, Y_i, T_i, and F_i are fixed. Moreover, the infimum is only taken over states with $\mathcal{N}_i(\sigma)_{C_i} = p$, a condition which fixes the Bell violation achieved by σ under the bipartite measurement performed by the device. This is precisely the sense in which the EAT can be understood as providing a reduction to the i.i.d. case.

Lower bounds of the form of (3.4) of different quality can be obtained depending on the specific Bell inequality employed in the protocol. A general method consists in using the chain rule to write

$$\begin{aligned} H\left(A_iB_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} &= H\left(A_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} + H\left(B_i|X_iY_iT_iF_iR'A_i\right)_{\mathcal{N}_i(\sigma)} \\ &\geq H_{\min}\left(A_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} . \end{aligned} \tag{3.6}$$

Note that here the RV F_i depends on the (optional) symmetrization step and was introduced precisely to enable an easier lower bound on the quantities above; we will show how it can be used in the specific case of the CHSH game in the next section.

A bound using the min-entropy $H_{\min}$, instead of H itself, is not tight in general, and one can expect to lose quite a lot by performing the relaxation above (see, for example, Figure 2). The advantage, however, is that a lower bound on $H_{\min}\left(A_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)}$ can be found using general techniques based on the semidefinite programming (SDP) hierarchies of [55]. For a slightly better bound, one should not drop the second term in (3.6). A bound on $H_{\min}\left(A_iB_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)}$ (usually called "global randomness") can also be found using the SDP hierarchies (see, e.g., [58]). For further details and references, see [17, section IV-C].

4. A bound for the CHSH game. In this section, we devise a specific min-tradeoff function f_{min} which, through an application of Lemma 3.2, leads to a concrete bound on the entropy generated by Protocol 3.1 when the game G is the CHSH game (described in section 2.3).

We use Protocol 3.1 with the following choices: $\mathcal{X}_g = \{0\}$, $\mathcal{X}_t = \{0,1\}$, $\mathcal{Y}_g = \{2\}$, and $\mathcal{Y}_t = \{0,1\}$.

In order to fully specify the protocol, it suffices to describe the symmetrization step. In this step, Alice and Bob choose together a uniform bit F_i, and they both flip their output bits if and only if $F_i = 1$. This symmetrization is helpful in the proof of the main theorem below. The downside is that it costs a lot of randomness

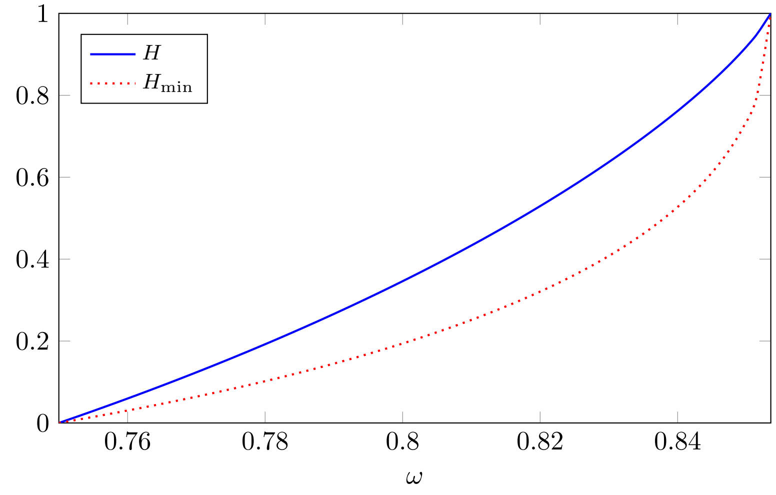

FIG. 2. *The lower bounds on* $H\big(A_i|X_iY_iT_iR'_{i-1}\big)$ *and* $H_{\min}\big(A_i|X_iY_iT_iR'_{i-1}\big)$ *as a function of the Bell violation for the CHSH inequality. The bound on* $H\big(A_i|X_iY_iT_iR'_{i-1}\big)$ *is given in* (4.7)*, while the bound on* $H_{\min}\big(A_i|X_iY_iT_iR'_{i-1}\big)$ *can be taken from* [50]*; both bounds are asymptotically tight. For nonoptimal Bell violation, the min-entropy is significantly lower than the entropy.*

to implement, which can be problematic for some applications, such as randomness expansion. At the end of the section, we show that the step is in fact not necessary in any real implementation of the protocol.

The proof of Theorem 4.1 shows that the rate of entropy generation is governed by the following functions, where h is the binary entropy and $\gamma, p(1) \in (0,1]$ such that $p(1)/\gamma \geq 3/4$:[18]

$$g(p) = \begin{cases} 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\,\frac{p(1)}{\gamma}\left(\frac{p(1)}{\gamma} - 1\right) + 3}\right), & \frac{p(1)}{\gamma} \in \left[\frac{3}{4}, \frac{2+\sqrt{2}}{4}\right], \\ 1\,, & \frac{p(1)}{\gamma} \in \left[\frac{2+\sqrt{2}}{4}, 1\right]\,, \end{cases}$$

$$f_{\min}\left(p, p_t\right) = \begin{cases} g\left(p\right)\,, & p(1) \leq p_t(1)\,, \\ \frac{\mathrm{d}}{\mathrm{d}p(1)} g(p)\big|_{p_t} \cdot p(1) + \left(g(p_t) - \frac{\mathrm{d}}{\mathrm{d}p(1)} g(p)\big|_{p_t} \cdot p_t(1)\right), & p(1) > p_t(1)\,, \end{cases}$$

$$\eta(p, p_t, \varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{e}}) = f_{\min}\left(p, p_t\right) - \frac{1}{\sqrt{n}} 2\left(\log 13 + \left\lceil \frac{\mathrm{d}}{\mathrm{d}p(1)} g(p)\big|_{p_t} \right\rceil\right)\sqrt{1 - 2\log(\varepsilon_{\mathrm{s}} \cdot \varepsilon_{\mathrm{e}})}\,,$$

$$\eta_{\mathrm{opt}}(\varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{e}}) = \max_{\frac{3}{4} < \frac{p_t(1)}{\gamma} < \frac{2+\sqrt{2}}{4}} \eta(\omega_{\exp}\gamma - \delta_{\mathrm{est}}, p_t, \varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{e}})\,. \tag{4.1}$$

THEOREM 4.1 (main theorem). *Let D be any device, ρ the state (as defined in* (3.1)*) generated using Protocol* 3.1 *when the game G is the CHSH game, Ω (as defined in* (3.2)*) the event that the protocol does not abort, and $\rho_{|\Omega}$ the state conditioned on Ω. Then, for any $\varepsilon_{\mathrm{EA}}, \varepsilon_s \in (0,1)$, either the protocol aborts with probability greater than $1 - \varepsilon_{\mathrm{EA}}$ or*

$$H_{\min}^{\varepsilon_s}\left(\mathbf{AB}|\mathbf{XYTF}E\right)_{\rho_{|\Omega}} > n \cdot \eta_{\mathrm{opt}}(\varepsilon_s, \varepsilon_{\mathrm{EA}})\,, \tag{4.2}$$

where η_{opt} is defined in (4.1)*.*

[18] We define the functions g and f_{min} only in the regime in which the protocol does not abort, i.e., $p(1)/\gamma \geq 3/4$. Any extension of g to the regime $p(1)/\gamma \in [0, 3/4]$ that keeps the function differential can be used for mathematical completeness.

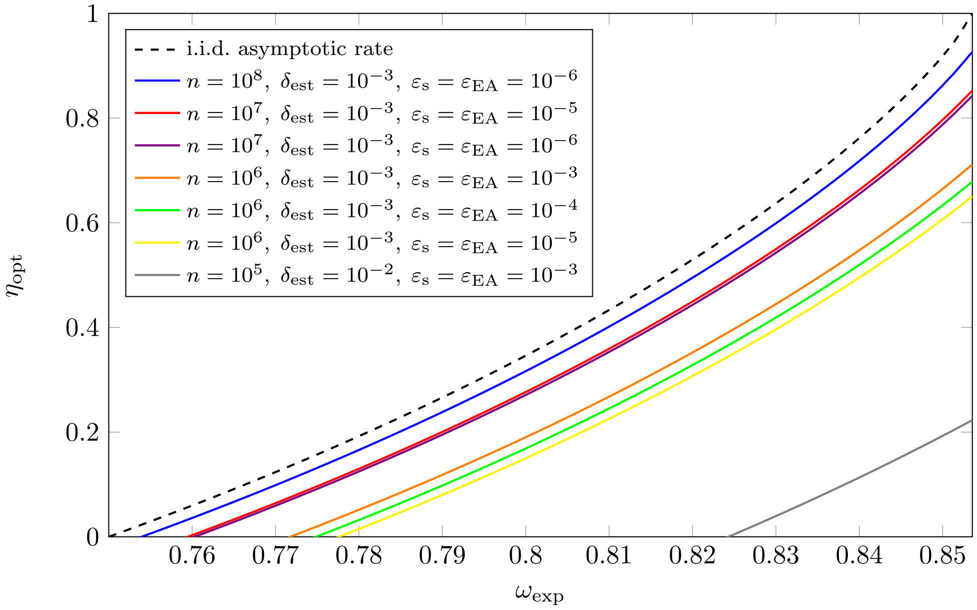

FIG. 3. *$\eta_{\rm opt}(\omega_{\rm exp})$ for $\gamma = 1$ and several choices of $\delta_{\rm est}$, n, $\varepsilon_{\rm EA}$, and the smoothing parameter ε_s. Note that for the errors of the protocols to be meaningful the number of rounds n should be at least of order $\delta_{\rm est}^{-2}$. $\varepsilon_{\rm EA}$ and ε_s affect the soundness error in the protocols of the following sections. The dashed line shows the optimal asymptotic ($n \to \infty$) rate under the assumption that the devices are such that Alice, Bob, and Eve share an (unknown) i.i.d. state.*

The rate $\eta_{\rm opt}$ as a function of the expected Bell violation $\omega_{\rm exp}$ is plotted in Figure 3 for $\gamma = 1$ and several choices of values for $\varepsilon_{\rm EA}$, $\delta_{\rm est}$, and n. For comparison, we also plot in Figure 3 the asymptotic rate ($n \to \infty$) under the assumption that the state of the device is an (unknown) i.i.d. state $\rho_{Q_AQ_BE}^{\otimes n}$. In this case, the quantum asymptotic equipartition property [74, Theorems 1 and 9] implies that the optimal rate is the Shannon entropy accumulated in one round of the protocol (as given in (4.7)). This rate, appearing as the dashed line in Figure 3, is an upper bound on the entropy that can be accumulated. One can see that as the number of rounds in the protocol increases our rate $\eta_{\rm opt}$ approaches this optimal rate.

Proof of Theorem 4.1. Based on Lemma 3.2, it will suffice to define a min-tradeoff function $f_{\rm min}$ such that (3.4) is satisfied. Using the chain rule,

$$H\left(A_iB_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} \geq H\left(A_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} .$$

Furthermore,

$$\begin{aligned} H\left(A_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} = {} & \Pr\left[X_i = 0\right] \cdot H\left(A_i|Y_iT_iF_iR', X_i = 0\right)_{\mathcal{N}_i(\sigma)} \\ & + \Pr\left[X_i = 1\right] \cdot H\left(A_i|Y_iT_iF_iR', X_i = 1\right)_{\mathcal{N}_i(\sigma)} \ . \end{aligned} \tag{4.3}$$

In the following, we find a bound on $H\left(A_i|Y_iT_iF_iR', X_i = 0\right)_{\mathcal{N}_i(\sigma)}$. Using exactly the same steps, the same bound can be derived on $H\left(A_i|Y_iT_iF_iR', X_i = 1\right)_{\mathcal{N}_i(\sigma)}$.

Due to the bipartite requirement on the untrusted device D used to implement the protocol and since Alice's actions (and her devices) are independent of Bob's choice of Y_i and T_i for the case $X_i = 0$, we have[19]

$$H\left(A_i|Y_iT_iF_iR', X_i = 0\right)_{\mathcal{N}_i(\sigma)} = H\left(A_i|F_iR', X_i = 0\right)_{\mathcal{N}_i(\sigma)} \ .$$

Defining the conditional entropy, one can rewrite $H\left(A_i|F_iR', X_i = 0\right)_{\mathcal{N}_i(\sigma)}$ as follows:

$$\begin{aligned} H\left(A_i|F_iR', X_i = 0\right) &= H\left(A_iF_iR'|X_i = 0\right) - H\left(F_iR'|X_i = 0\right) \\ &= H\left(A_i|X_i = 0\right) + H\left(F_iR'|A_i, X_i = 0\right) - H\left(F_iR'|X_i = 0\right) \\ &= H\left(A_i|X_i = 0\right) - \chi\left(A_i : F_iR'|X_i = 0\right) \\ &= 1 - \chi\left(A_i : F_iR'|X_i = 0\right) \ , \end{aligned} \tag{4.4}$$

where $\chi\left(A_i : F_iR'|X_i = 0\right) = H\left(F_iR'|X_i = 0\right) - H\left(F_iR'|A_i, X_i = 0\right)$ and the last equality follows from the symmetrization step, step 5.

For states leading to a CHSH violation of $\beta \in [2, 2\sqrt{2}]$ (for inputs restricted to $\{0,1\} \times \{0,1\}$), a tight bound on $\chi\left(A_i : F_iR'|X_i = 0\right)$ was derived in [57, section 2.3]:

$$\chi\left(A_i : F_iR'|X_i = 0\right) \leq h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{\beta^2}{4} - 1}\right) \ . \tag{4.5}$$

Since $\omega = \frac{1}{8}\beta + \frac{1}{2}$, for $\omega \in \left[\frac{3}{4}, \frac{2+\sqrt{2}}{4}\right]$ (i.e., a violation in the quantum regime), we get

$$\chi\left(A_i : F_iR'|X_i = 0\right) \leq h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega\left(\omega - 1\right) + 3}\right) \ .$$

Combining this bound with (4.3) and (4.4), we conclude that for a state with winning probability ω,

$$H\left(A_iB_i|X_iY_iT_iF_iR'\right) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega\left(\omega - 1\right) + 3}\right) \ . \tag{4.6}$$

Consider a probability distribution $p = \text{freq}_{\mathbf{c}}$ resulting from the observed data. If $p(0) + p(1) \neq \gamma$, then the set of states fulfilling $\mathcal{N}_i(\sigma)_{C_i} = p$ is empty and the condition on the min-tradeoff function given in Definition 2.6 becomes trivial. Hence, for the construction of the min-tradeoff function we can restrict our attention to p with $p(0) + p(1) = \gamma$. For such p, we can write $\omega = \frac{p(1)}{p(0)+p(1)} = \frac{p(1)}{\gamma}$. Altogether, we have for all p in the considered regime,

$$\begin{aligned} &\inf_{\sigma_{R_{i-1}R'} : \mathcal{N}_i(\sigma)_{C_i} = p} H\left(A_iB_i|X_iY_iT_iF_iR'\right)_{\mathcal{N}_i(\sigma)} \\ &\qquad \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\,\frac{p(1)}{\gamma}\left(\frac{p(1)}{\gamma} - 1\right) + 3}\right) \ . \end{aligned} \tag{4.7}$$

Define a function g over p for which $p(2)/\gamma \in [3/54, 1]$ by

$$g(p) = \begin{cases} 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\,\frac{p(1)}{\gamma}\left(\frac{p(1)}{\gamma} - 1\right) + 3}\right) \ , & \frac{p(1)}{\gamma} \in \left[\frac{3}{4}, \frac{2+\sqrt{2}}{4}\right] \ , \\ 1 \ , & \frac{p(1)}{\gamma} \in \left[\frac{2+\sqrt{2}}{4}, 1\right] \ . \end{cases} \tag{4.8}$$

[19] We assume that the value of T_i is exchanged over a classical authenticated channel to which the device D does not have access. In particular, Alice's part of the device is independent from the value of T_i.

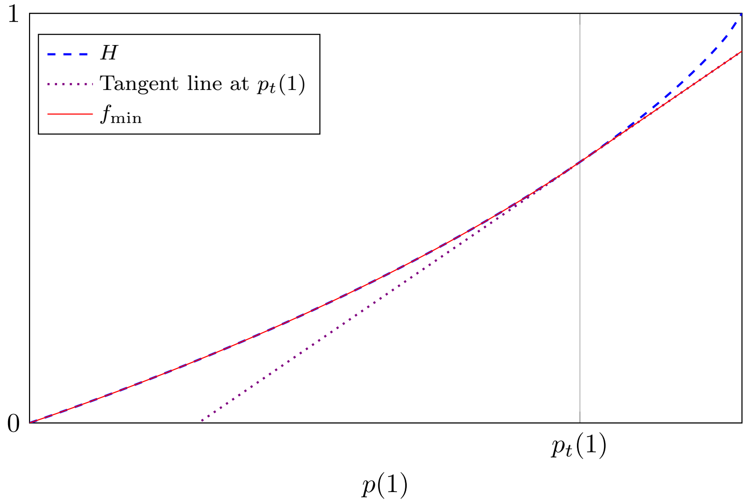

FIG. 4. *The construction of the min-tradeoff function* $f_{\min}$ *as in* (4.10)*. The plot shows the values of the min-tradeoff function on a slice* $p(0) + p(1) =$ *constant.*

From (4.7), it follows that any choice of $f_{\min}(p)$ that is differentiable and satisfies $f_{\min}(p) \leq g(p)$ for all p will satisfy (3.4).

For $\frac{p(1)}{\gamma} = \frac{2+\sqrt{2}}{4}$, the derivative of g is infinite. For the final bound of the EAT to be meaningful, $f_{\min}$ should be chosen such that $\|\nabla f_{\min}\|_\infty$ is finite. To remedy this problem, we choose $f_{\min}$ by "cutting" the function g and "gluing" it to a linear function at some point p_t (which is later optimized), while keeping the function differentiable. By doing this, we ensure that the gradient of $f_{\min}$ is bounded, at the cost of losing a bit of entropy for p with $p(1) > p_t(1)$. Towards this, denote

$$(4.9) \qquad a(p_t) = \left\lceil \frac{\mathrm{d}}{\mathrm{d}p(1)} g(p)\big|_{p_t} \right\rceil \qquad \text{and} \qquad b(p_t) = g(p_t) - a(p_t) \cdot p_t(1).$$

We then make the following choice[20] for the min-tradeoff function $f_{\min}$ (see Figure 4):

$$(4.10) \qquad f_{\min}(p, p_t) = \begin{cases} g(p) \ , & p(1) \leq p_t(1) \ , \\ a(p_t) \cdot p(1) + b(p_t) \ , & p(1) > p_t(1) \ . \end{cases}$$

From the definition of a and b in (4.9), this function is differentiable and fulfils the condition given in (3.4). Furthermore, by definition for any choice of p_t it holds that $\|\nabla f_{\min}(\cdot, p_t)\|_\infty \leq a(p_t)$.

Applying Lemma 3.2, we conclude that for any $\frac{3}{4} < \frac{p_t(1)}{\gamma} < \frac{2+\sqrt{2}}{4}$, either the protocol aborts with probability greater than $1 - \varepsilon_{\mathrm{EA}}$ or

$$(4.11) \qquad H_{\min}^{\varepsilon_{\mathrm{s}}}(\mathbf{AB}|\mathbf{XYTF}E)_{\rho_{|\Omega}} > n f_{\min}(\omega_{\exp}\gamma - \delta_{\mathrm{est}}, p_t) - \sqrt{n}\zeta(p_t)$$

[20] Note that f_{min} is nonpositive for $\frac{p(1)}{\gamma} \leq 3/4$, but this regime is not relevant, as it would lead to the protocol aborting; the extension of f_{min} to that range of values is only for mathematical convenience.

for $\zeta(p_t, \varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{AE}}) = 2\left(\log 13 + a(p_t)\right)\sqrt{1 - 2\log(\varepsilon_{\mathrm{s}} \cdot \varepsilon_{\mathrm{AE}})}$ (as $d_{A_iB_i} = 6$). To obtain the optimal rate, we optimize over p_t . Denote $\eta(p, p_t, \varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{AE}}) = f_{\min}(p, p_t) - \frac{1}{\sqrt{n}}\zeta(p_t, \varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{AE}})$, and let

$$\eta_{\mathrm{opt}}(\varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{AE}}) = \max_{\frac{3}{4} < \frac{p_t(1)}{\gamma} < \frac{2+\sqrt{2}}{4}} \eta(\omega_{\exp}\gamma - \delta_{\mathrm{est}}, p_t, \varepsilon_{\mathrm{s}}, \varepsilon_{\mathrm{AE}}) \ .$$

Plugging this into (4.11), the theorem follows. □

We end this section by showing how the particular implementation of the symmetrization step, step 5, of Protocol 3.1 made here for the CHSH game can be ignored in any implementation of the protocol. For this, rewrite (4.2) more formally as[21]

$$H_{\min}^{\varepsilon_{\mathrm{s}}}\left(g_{\mathbf{F}}\left(\mathbf{AB}\right)|\mathbf{XYTF}E\right)_{\rho_{|\Omega}} > n \cdot \eta_{\mathrm{opt}} \ , \tag{4.12}$$

where $g_{\mathbf{F}}$ is the function that flips the bits according to $\mathbf{F}$. Since for any fixed value of F, g_F is a deterministic function, it follows from [69, Lemma 1] that for any $\varepsilon_{\mathrm{s}} \geq 0$,

$$H_{\min}^{\varepsilon_{\mathrm{s}}}\left(\mathbf{AB}|\mathbf{XYT}E\right)_{\rho_{|\Omega}} \geq H_{\min}^{\varepsilon_{\mathrm{s}}}\left(g_{\mathbf{F}}\left(\mathbf{AB}\right)|\mathbf{XYTF}E\right)_{\rho_{|\Omega}} \ . \tag{4.13}$$

Combining (4.12) and (4.13) proves the following corollary.

Corollary 4.2. *Under the same assumptions as Theorem* 4.1*, but for an implementation of Protocol* 3.1 *in which the symmetrization step, step* 5*, is omitted, for any* $\varepsilon_{\mathrm{EA}}, \varepsilon_s \in (0,1)$*, either the protocol aborts with probability greater than* $1 - \varepsilon_{\mathrm{EA}}$ *or*

$$H_{\min}^{\varepsilon_s}\left(\mathbf{AB}|\mathbf{XYT}E\right)_{\rho_{|\Omega}} > n \cdot \eta_{\mathrm{opt}}(\varepsilon_s, \varepsilon_{\mathrm{EA}}) \ , \tag{4.14}$$

where η_{opt} *is defined in* (4.1)*.*

In Appendix B, we use a small modification of the entropy accumulation protocol and the above proof to get a similar bound on the entropy rate which has a better dependency on the probability of a test γ. This is of relevance for some applications, such as DIQKD. The calculations presented in Appendix B are slightly more technical than the proof given above but do not require any substantially different observations.

5. DIQKD.

5.1. The protocol. Our protocol for DIQKD is described as Protocol 5.1 below. An honest implementation is described in section 5.2.

In the first part of the protocol, Alice and Bob use their devices to produce the raw data, similarly to what is done in the entropy accumulation protocol, Protocol 3.1 (with the game G equal to the CHSH game, as in section 4). The main difference is that Bob's outputs always contains Bob's ith measurement outcome (instead of being set to $\perp$ in all rounds for which $T_i = 0$); to make the distinction explicit, we denote Bob's outputs in Protocol 5.1 with a tilde, $\tilde{\mathbf{B}}$.

In the second part of the protocol, Alice and Bob apply classical postprocessing steps to produce their final keys. We choose classical postprocessing steps that optimize the key rate, but which may not be optimal in other aspects, e.g., computation time. The protocol and the analysis can easily be adapted for other choices of classical postprocessing.

[21] Previously, for ease of notation we wrote $\mathbf{AB}$ for the flipped outputs; here we denote the same bits as $g_{\mathbf{F}}\left(\mathbf{AB}\right)$ to make the flipping operation explicit.

We now describe the three postprocessing steps, error correction, parameter estimation, and privacy amplification, in detail.[22]

Error correction. Alice and Bob use an error correction protocol EC to obtain identical raw keys K_A and K_B from their bits $\mathbf{A}, \tilde{\mathbf{B}}$. In our analysis, we use a protocol, based on universal hashing, which minimizes the amount of leakage to the adversary [16, 64] (see also section 3.3.2 in [11] for details). To implement this protocol, Alice chooses a hash function and sends the chosen function and the hashed value of her bits to Bob. We denote this classical communication by O. Bob uses O, together with his prior knowledge $\tilde{\mathbf{B}}\mathbf{XYT}$, to compute a guess $\hat{\mathbf{A}}$ for Alice's bits $\mathbf{A}$. If EC raises a "fail" flag, Alice and Bob abort; in an honest implementation, this happens with probability at most $\varepsilon^c_{\mathrm{EC}}$. The probability that Alice and Bob do not abort but hold different raw keys $K_A = \mathbf{A}$ and $K_B = \hat{\mathbf{A}} \neq K_A$ is at most $\varepsilon_{\mathrm{EC}}$.

Due to the communication from Alice to Bob, $\mathrm{leak}_{\mathrm{EC}}$ bits of information are leaked to the adversary. The following guarantee follows for the described protocol [64]:

$$\mathrm{leak}_{\mathrm{EC}} \leq H_0^{\varepsilon'_{\mathrm{EC}}}\left(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT}\right) + \log\left(\frac{1}{\varepsilon_{\mathrm{EC}}}\right) \tag{5.1}$$

for $\varepsilon^c_{\mathrm{EC}} = \varepsilon'_{\mathrm{EC}} + \varepsilon_{\mathrm{EC}}$ and where $H_0^{\varepsilon'_{\mathrm{EC}}}(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT})$ is evaluated on the state in an *honest* implementation of the protocol. For example, for quantum channels with an i.i.d. noise model, $H_0^{\varepsilon'_{\mathrm{EC}}}\big(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT}\big)$ can be bounded by above using the asymptotic equipartition property [74] (see (5.9) below for the explicit bound in that case). If a larger fraction of errors occur when running the actual DIQKD protocol (for instance, due to adversarial interference), the error correction might not succeed, as Bob will not have a sufficient amount of information to obtain a good guess of Alice's bits. If so, this will be detected with probability at least $1 - \varepsilon_{\mathrm{EC}}$ and the protocol will abort.

Parameter estimation. After the error correction step, Bob has all of the relevant information to perform parameter estimation from his data alone without any further communication with Alice. Using $\tilde{\mathbf{B}}$ and K_B, Bob sets $C_i = w_{\mathrm{CHSH}}\big(\hat{A}_i, \tilde{B}_i, X_i, Y_i\big) = w_{\mathrm{CHSH}}\big(K_{Bi}, \tilde{B}_i, X_i, Y_i\big)$ for the test rounds and $C_i = \perp$ otherwise. He aborts if the fraction of successful game rounds is too low, that is, if $\sum_j C_j < (\omega_{\mathrm{exp}}\gamma - \delta_{\mathrm{est}}) \cdot n$.

As Bob does the estimation using his guess of Alice's bits, the probability of aborting in this step in an honest implementation, $\varepsilon^c_{\mathrm{PE}}$, is bounded by

$$\begin{aligned} \varepsilon^c_{\mathrm{PE}} &\leq \Pr\left(\sum_j C_j < (\omega_{\mathrm{exp}}\gamma - \delta_{\mathrm{est}}) \cdot \sum_j T_j \Big| K_A = K_B\right) \\ &\qquad + \Pr\big(K_A \neq K_B \text{ and EC does not abort}\big) \\ &\leq \varepsilon^c_{\mathrm{EA}} + \varepsilon_{\mathrm{EC}} \end{aligned} \tag{5.2}$$

since conditioned on the error correction protocol succeeding the probability of aborting in the honest case is exactly as in the entropy accumulation protocol (Protocol 3.1).

Privacy amplification. Finally, Alice and Bob use a (quantum-proof) privacy amplification protocol PA (which takes some random seed S as input) to create their final

[22] We remark that in step 2 of Protocol 5.1 Alice and Bob choose T_i together (or exchange its value between them) in every round of the protocol and choose their inputs accordingly. This is in contrast to choosing Alice and Bob's input from a product distribution and then adding a sifting step, as usually done in QKD protocols. It follows from our proof technique that making T_i public as we do does not compromise the security of the protocol.

Protocol 5.1 CHSH-based DIQKD protocol.

```
Arguments:
    $D$ – untrusted device of two components that can play CHSH repeatedly
    $n \in \mathbb{N}_+$ – number of rounds
    $\gamma \in (0,1]$ – expected fraction of test rounds
    $\omega_{\mathrm{exp}}$ – expected winning probability in an honest (perhaps noisy) implementation
    $\delta_{\mathrm{est}} \in (0,1)$ – width of the statistical confidence interval for the estimation test
    EC – error correction protocol which leaks $\mathrm{leak}_{\mathrm{EC}}$ bits and has error probability $\varepsilon_{\mathrm{EC}}$
    PA – privacy amplification protocol with error probability $\varepsilon_{\mathrm{PA}}$

1: For every round $i \in [n]$ do steps 2–4:
2:     Alice and Bob choose a random $T_i \in \{0,1\}$ such that $\Pr(T_i = 1) = \gamma$.
3:     If $T_i = 0$, Alice and Bob choose $(X_i, Y_i) = (0,2)$ and otherwise $X_i, Y_i \in \{0,1\}$ uniformly at random.
4:     Alice and Bob use $D$ with $X_i, Y_i$ and record their outputs as $A_i$ and $\tilde{B}_i$, respectively.

5: Error correction: Alice and Bob apply the error correction protocol EC, communicating $O$ in the process. If EC aborts, they abort the protocol. Otherwise, they obtain raw keys denoted by $K_A$ and $K_B$.
6: Parameter estimation: Bob sets $C_i = w_{\mathrm{CHSH}}\big(K_{Bi}, \tilde{B}_i, X_i, Y_i\big)$ for the test rounds and $C_i = \perp$ otherwise using $\tilde{\mathbf{B}}$ and $K_B$. He aborts if $\sum_j C_j < (\omega_{\mathrm{exp}}\gamma - \delta_{\mathrm{est}}) \cdot n$;.
7: Privacy amplification: Alice and Bob apply the privacy amplification protocol PA on $K_A$ and $K_B$ to create their final keys $\tilde{K}_A$ and $\tilde{K}_B$ of length $\ell$ as defined in (5.4).
```

keys $\tilde{K}_A$ and $\tilde{K}_B$ of length ℓ, which are close to ideal keys, i.e., uniformly random and independent of the adversary's knowledge.

For simplicity, we use universal hashing [63] as the privacy amplification protocol in the analysis below. Any other quantum-proof strong extractor, e.g., Trevisan's extractor [25], can be used for this task, and the analysis can be easily adapted.

The secrecy of the final key depends only on the privacy amplification protocol used and the value of $H_{\min}^{\varepsilon_{\mathrm{s}}}(\mathbf{A}|\mathbf{XYT}OE)$, evaluated on the state at the end of the protocol, conditioned on not aborting. For universal hashing, for every $\varepsilon_{\mathrm{PA}}, \varepsilon_{\mathrm{s}} \in (0,1)$ a secure key of maximal length

$$\ell = H_{\min}^{\varepsilon_{\mathrm{s}}}(\mathbf{A}|\mathbf{XYT}OE) - 2\log\frac{1}{\varepsilon_{\mathrm{PA}}} \tag{5.3}$$

is produced with probability[23] at least $1 - \varepsilon_{\mathrm{PA}} - \varepsilon_{\mathrm{s}}$.

The main theorem of this section is the following security result for Protocol 5.1.

[23] $\varepsilon_{\mathrm{PA}}$ is the error probability of the extractor when it is applied on a normalized state satisfying the relevant min-entropy bound. For universal hashing, when only a bound on the smooth min-entropy is given, the smoothing parameter ε_{s} should be added to the error $\varepsilon_{\mathrm{PA}}$. When working with other extractors, one should adapt the parameters accordingly; see [7, section 4.3].

THEOREM 5.1. *The DIQKD protocol given in Protocol* 5.1 *is* $(\varepsilon^s_{\text{QKD}}, \varepsilon^c_{\text{QKD}}, \ell)$*-secure according to Definition* 2.3*, with* $\varepsilon^s_{\text{QKD}} \leq \varepsilon_{\text{EC}} + \varepsilon_{\text{PA}} + \varepsilon_s + \varepsilon_{\text{EA}}$*,* $\varepsilon^c_{\text{QKD}} \leq \varepsilon^c_{EC} + \varepsilon^c_{\text{EA}} + \varepsilon_{\text{EC}}$*, and*

$$\begin{aligned} \ell = \; & n \cdot \eta_{\text{opt}}\left(\varepsilon_s/4, \varepsilon_{\text{EA}} + \varepsilon_{\text{EC}}\right) - \text{leak}_{\text{EC}} - 3\log\left(1 - \sqrt{1 - (\varepsilon_s/4)^2}\right) \\ & - \gamma n - \sqrt{n}2\log 7\sqrt{1 - 2\log\left(\varepsilon_s/4 \cdot (\varepsilon_{\text{EA}} + \varepsilon_{\text{EC}})\right)} - 2\log\left(\varepsilon_{\text{PA}}^{-1}\right) \; , \end{aligned} \tag{5.4}$$

where η_{opt} *is specified in* (4.1)*.*

In section 5.5, we plot the resulting key rates, ℓ/n, for different choices of parameters.

Theorem 5.1 follows by combining Lemmas 5.2 and 5.4, which we prove in the following sections.

5.2. The honest implementation. The honest (but possibly noisy) implementation of the protocol is one where the device D performs in *every round* i of the protocol the measurements $\mathcal{M}^{a_i}_{x_i} \otimes \mathcal{M}^{b_i}_{y_i}$ on Alice and Bob's state $\rho_{Q_A Q_B}$. The state and measurements are such that the winning probability achieved in the CHSH game in a single round is ω_{exp}.[24] For the measurements $(X_i, Y_i) = (0, 2)$, we denote the quantum bit error rate, i.e., the probability that $A_i \neq B_i$ while using these measurements, by Q. Thus, in the honest case we assume the device D behaves in an i.i.d. manner (in particular, an i.i.d. noise model for the quantum channels used in the protocol is assumed): it is initialized in an i.i.d. bipartite state, $\rho^{\otimes n}_{Q_A Q_B}$, on which it makes i.i.d. measurements.

As an example, one possible realization of such an implementation is the following: Alice and Bob share the two-qubit Werner state $\rho_{Q_A Q_B} = (1-\nu)\left|\phi^+\right\rangle\left\langle\phi^+\right| + \nu\mathbb{1}/4$ for $\left|\Phi^+\right\rangle = 1/\sqrt{2}\left(|00\rangle + |11\rangle\right)$ and $\nu \in [0,1]$. The state $\rho_{Q_A Q_B}$ arises, e.g., from the state $\left|\Phi^+\right\rangle$ after going through a depolarization channel. For every $i \in [n]$, Alice's measurements $X_i = 0$ and $X_i = 1$ correspond to σ_z and σ_x, respectively, and Bob's measurements $Y_i = 0$, $Y_i = 1$, and $Y_i = 2$ correspond to $\frac{\sigma_z + \sigma_x}{\sqrt{2}}$, $\frac{\sigma_z - \sigma_x}{\sqrt{2}}$ and σ_z, respectively. The winning probability in the CHSH game (restricted to $X_i, Y_i \in \{0,1\}$) using these measurements on $\rho_{Q_A Q_B}$ is $\omega_{\text{exp}} = \frac{2+\sqrt{2}(1-\nu)}{4}$ and $Q = \frac{\nu}{2}$.

5.3. Completeness. The completeness of the protocol follows from the honest i.i.d. implementation described in section 5.2 and the completeness of the entropy accumulation protocol as shown in section 3.2.

LEMMA 5.2. *Protocol* 5.1 *is complete with completeness error* $\varepsilon^c_{\text{QKD}} \leq \varepsilon^c_{EC} + \varepsilon^c_{\text{EA}} + \varepsilon_{\text{EC}}$*. That is, the probability that the protocol aborts for an honest implementation of the device* D *is at most* $\varepsilon^c_{\text{QKD}}$*.*

Proof. There are two steps at which Protocol 5.1 may abort: after the error correction (step 5) or in the Bell violation estimation (step 6). By the union bound, the total probability of aborting is at most the probability of aborting in each of these steps. Using this and (5.2), we get

$$\varepsilon^c_{\text{QKD}} \leq \varepsilon^c_{EC} + \varepsilon^c_{PE} \leq \varepsilon^c_{EC} + \varepsilon^c_{\text{EA}} + \varepsilon_{\text{EC}} \; . \qquad \square$$

[24] Note that in our notation, the noise that affects the winning probability in the CHSH game is already included in ω_{exp}.

5.4. Soundness. To establish soundness, first note that by definition, as long as the protocol does not abort, it produces a key of length ℓ. Therefore, it remains to verify correctness, which depends on the error correction step, and security, which is based on the privacy amplification step. To prove security, we start with Lemma 5.3, in which we assume that the error correction step is successful. We then use it to prove soundness in Lemma 5.4.

Let $\tilde{\Omega}$ denote the event of Protocol 5.1 not aborting *and* the EC protocol being successful, and let $\tilde{\rho}_{\mathbf{A}\tilde{\mathbf{B}}\mathbf{XYT}OE|\tilde{\Omega}}$ be the state at the end of the protocol, conditioned on this event.

The success of the privacy amplification step is dependent on the min-entropy $H^{\varepsilon_{\mathrm{s}}}_{\min}(\mathbf{A}|\mathbf{XYT}OE)_{\tilde{\rho}_{|\tilde{\Omega}}}$ being sufficiently large. The following lemma connects this quantity to $H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\min}(\mathbf{AB}|\mathbf{XYT}E)_{\rho_{|\Omega}}$, on which a lower bound is provided by Corollary 4.2.

Lemma 5.3. *For any device D, let $\tilde{\rho}$ be the state generated in Protocol* 5.1 *right before the privacy amplification step, step* 7*. Let $\tilde{\rho}_{|\tilde{\Omega}}$ be the state conditioned on not aborting the protocol and success of the* EC *protocol. Then, for any $\varepsilon_{\mathrm{EA}}, \varepsilon_{\mathrm{EC}}, \varepsilon_s \in (0,1)$, either the protocol aborts with probability greater than $1-\varepsilon_{\mathrm{EA}}-\varepsilon_{\mathrm{EC}}$ or*

$$\begin{aligned} H^{\varepsilon_s}_{\min}\left(\mathbf{A}|\mathbf{XYT}OE\right)_{\tilde{\rho}_{|\tilde{\Omega}}} \geq{}& n\cdot\eta_{\mathrm{opt}}\left(\varepsilon_s/4, \varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}}\right) - \mathrm{leak}_{\mathrm{EC}} \\ & - 3\log\left(1-\sqrt{1-(\varepsilon_s/4)^2}\right) - \gamma n \\ & - \sqrt{n}2\log 7\sqrt{1-2\log\left(\varepsilon_s/4\cdot(\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}})\right)}\ . \end{aligned} \tag{5.5}$$

Proof. Consider the following events:

1. Ω: the event of not aborting in the entropy accumulation protocol, Protocol 3.1. This happens when the Bell violation, calculated using Alice and Bob's outputs (and inputs), is sufficiently high.
2. $\hat{\Omega}$: Suppose Alice and Bob run Protocol 3.1, and then execute the EC protocol. The event $\hat{\Omega}$ is defined by Ω *and* $K_B = \mathbf{A}$.
3. $\tilde{\Omega}$: the event of not aborting the DIQKD protocol, Protocol 5.1, *and* $K_B = \mathbf{A}$.

The state $\rho_{|\hat{\Omega}}$ then denotes the state at the end of Protocol 3.1 conditioned on $\hat{\Omega}$.

As we are only interested in the case where the EC protocol outputs the correct guess of Alice's bits, that is, $K_B = \mathbf{A}$ (which happens with probability $1-\varepsilon_{\mathrm{EC}}$), we have $\tilde{\rho}_{\mathbf{AXYT}E|\tilde{\Omega}} = \rho_{\mathbf{AXYT}E|\hat{\Omega}}$ (note that $\tilde{\mathbf{B}}$ and $\mathbf{B}$ were traced out from $\tilde{\rho}$ and ρ, respectively). Hence,

$$H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}E\right)_{\tilde{\rho}_{|\tilde{\Omega}}} = H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}}\ . \tag{5.6}$$

Using the chain rule given in [73, Lemma 6.8], together with (5.6), we get that

$$\begin{aligned} H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}OE\right)_{\tilde{\rho}_{|\tilde{\Omega}}} &\geq H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}E\right)_{\tilde{\rho}_{|\tilde{\Omega}}} - \mathrm{leak}_{\mathrm{EC}} \\ &= H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}} - \mathrm{leak}_{\mathrm{EC}}\ . \end{aligned} \tag{5.7}$$

In order for one to apply Corollary 4.2, it remains to relate $H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}}$

to $H^{\varepsilon'_{\mathrm{s}}}_{\min}\left(\mathbf{AB}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}}$ for some $\varepsilon'_{\mathrm{s}}$. For this, we first write

$$\begin{aligned}H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}} &\geq H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\min}\left(\mathbf{AB}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}} - H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\max}\left(\mathbf{B}|\mathbf{AXYT}E\right)_{\rho_{|\hat{\Omega}}}\\ &\quad - 3\log\left(1-\sqrt{1-(\varepsilon_{\mathrm{s}}/4)^2}\right)\\ &\geq H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\min}\left(\mathbf{AB}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}} - H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\max}\left(\mathbf{B}|\mathbf{T}E\right)_{\rho_{|\hat{\Omega}}}\\ &\quad - 3\log\left(1-\sqrt{1-(\varepsilon_{\mathrm{s}}/4)^2}\right) ,\end{aligned}$$

where the first inequality is due to the chain rule [73, equation (6.57)] and the second is due to strong subadditivity of the smooth max-entropy.

One can now apply the EAT to upper bound $H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\max}\left(\mathbf{B}|\mathbf{T}E\right)_{\rho_{|\hat{\Omega}}}$ in the following way. We use Theorem 2.7 with the replacements $\mathbf{AB}\to\mathbf{B}$, $\mathbf{I}\to\mathbf{T}$, $E\to E$. The Markov conditions $B_{1,\dots,i-1}\leftrightarrow T_{1,\dots,i-1}E\leftrightarrow T_i$ then trivially hold, and the condition on the max-tradeoff function reads as

$$f_{\max}(p)\geq \sup_{\sigma_{R_{i-1}R'}:\mathcal{N}_i(\sigma)} H\left(B_i|T_iR'\right)_{\mathcal{N}_i(\sigma)} .$$

By the definition of the EAT channels $\{\mathcal{N}_i\}$, $B_i\neq\perp$ only for $T_i=1$, which happens with probability γ. Hence, for any state $\sigma_{R_{i-1}R'}$, we have

$$H\left(B_i|T_iR'\right)_{\mathcal{N}_i(\sigma)}\leq H\left(B_i|T_i\right)_{\mathcal{N}_i(\sigma)}\leq\gamma$$

and the max-tradeoff function is simply $f_{\max}(p)=\gamma$ for any p (and thus $\|\triangledown f_{\max}\|_\infty=0$). Applying[25] Theorem 2.7 with this choice of $f_{\max}$, we get that

$$H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\max}\left(\mathbf{B}|\mathbf{T}E\right)_{\rho_{|\hat{\Omega}}}<\gamma n+\sqrt{n}2\log 7\sqrt{1-2\log\left(\varepsilon_{\mathrm{s}}/4\cdot(\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}})\right)} . \tag{5.8}$$

Combining (5.7) with the above inequalities, we get that

$$\begin{aligned}H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}OE\right)_{\tilde{\rho}_{|\tilde{\Omega}}}\geq H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\min}\left(\mathbf{AB}|\mathbf{XYT}E\right)_{\rho_{|\hat{\Omega}}} - \mathrm{leak_{EC}} - 3\log\left(1-\sqrt{1-(\varepsilon_{\mathrm{s}}/4)^2}\right)\\ - \gamma n-\sqrt{n}2\log 7\sqrt{1-2\log\left(\varepsilon_{\mathrm{s}}/4\cdot(\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}})\right)} .\end{aligned}$$

Finally, note that by applying the EAT on $\rho_{|\hat{\Omega}}$, as in Corollary 4.2, we have that either $1-\Pr(\hat{\Omega})\geq 1-\varepsilon_{\mathrm{EA}}-\varepsilon_{\mathrm{EC}}$ or

$$H^{\frac{\varepsilon_{\mathrm{s}}}{4}}_{\min}(\mathbf{AB}|\mathbf{XYT}E)_{\rho_{|\hat{\Omega}}}>n\cdot\eta_{\mathrm{opt}}\left(\varepsilon_{\mathrm{s}}/4,\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}}\right) .$$

The last two equations give us the desired bound on $H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}OE\right)_{\tilde{\rho}_{|\tilde{\Omega}}}$: either the protocol aborts with probability greater than $1-\varepsilon_{\mathrm{EA}}-\varepsilon_{\mathrm{EC}}$ or

$$\begin{aligned}H^{\varepsilon_{\mathrm{s}}}_{\min}\left(\mathbf{A}|\mathbf{XYT}OE\right)_{\tilde{\rho}_{|\tilde{\Omega}}}&\geq n\cdot\eta_{\mathrm{opt}}\left(\varepsilon_{\mathrm{s}}/4,\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}}\right)-\mathrm{leak_{EC}}\\ &\quad -3\log\left(1-\sqrt{1-(\varepsilon_{\mathrm{s}}/4)^2}\right)\\ &\quad -\gamma n-\sqrt{n}2\log 7\sqrt{1-2\log\left(\varepsilon_{\mathrm{s}}/4\cdot(\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}})\right)} .\end{aligned}$$ □

[25] Here a slightly more general version of the EAT than the one given in this paper is needed, in which the event Ω can be defined via A,B,X,Y and not only C; see [28] for the details.

Using Lemma 5.3, we prove that Protocol 5.1 is sound.

LEMMA 5.4. *For any device D, let $\tilde{\rho}$ be the state generated using Protocol* 5.1. *Then either the protocol aborts with probability greater than $1-\varepsilon_{EA}-\varepsilon_{EC}$ or it is $(\varepsilon_{\mathrm{EC}}+\varepsilon_{\mathrm{PA}}+\varepsilon_s)$-correct-and-secret while producing keys of length ℓ, as defined in* (5.4).

Proof. Denote all the classical public communication during the protocol by $J = \mathbf{XYT}OS$, where S is the seed used in the privacy amplification protocol PA. Let $\overset{\approx}{\Omega}$ denote the event of not aborting Protocol 5.1, and let $\tilde{\rho}_{\tilde{K}_A\tilde{K}_BJE|\overset{\approx}{\Omega}}$ be the final state of Alice, Bob, and Eve at the end of the protocol, *conditioned on not aborting*.

We consider two cases. First, assume that the EC protocol was not successful (but did not abort). Then Alice and Bob's final keys might not be identical. This happens with probability at most $\varepsilon_{\mathrm{EC}}$.

Otherwise, assume the EC protocol was successful, i.e., $K_B = \mathbf{A}$. In that case, Alice and Bob's keys must be identical also after the final privacy amplification step, that is, conditioned on $K_B = \mathbf{A}$, $\tilde{K}_A = \tilde{K}_B$.

We continue to show that in this case the key is also secret. The secrecy depends only on the privacy amplification step, and for universal hashing a secure key is produced as long as (5.3) holds. Hence, a uniform and independent key of length ℓ as in (5.4) is produced by the privacy amplification step unless the smooth min-entropy is not high enough (i.e., the bound in (5.5) does not hold) or the privacy amplification protocol was not successful, which happens with probability at most $\varepsilon_{\mathrm{PA}}+\varepsilon_{\mathrm{s}}$.

According to Lemma 5.3, either the protocol aborts with probability greater than $1-\varepsilon_{\mathrm{EA}}-\varepsilon_{\mathrm{EC}}$ or the entropy is sufficiently high for us to have

$$\|\tilde{\rho}_{\tilde{K}_AJE|\overset{\approx}{\Omega}} - \rho_{U_l}\otimes\tilde{\rho}_{JE}\|_1 \leq \varepsilon_{\mathrm{PA}}+\varepsilon_{\mathrm{s}}\ .$$

Combining both cases above, we get that Protocol 5.1 is sound (that is, it produces identical and secret keys of length ℓ for Alice and Bob) with soundness error at most $\varepsilon_{\mathrm{EC}}+\varepsilon_{\mathrm{PA}}+\varepsilon_{\mathrm{s}}$. □

5.5. Key rate analysis.

Theorem 5.1 establishes a relation between the length ℓ of the secure key produced by our protocol and the different error terms. As this relation, given in (5.4), is somewhat hard to visualize, we analyze the key rate $r=\ell/n$ for some specific choices of parameters and compare it to the key rates achieved in device-dependent QKD with finite resources [68, 69] and DIQKD with infinite resources and a restricted set of attacks [57].

The key rate depends on the amount of leakage of information due to the error correction step, which in turn depends on the honest implementation of the protocol. We use the honest i.i.d. implementation described in section 5.2 and assume that in the honest case the state of each round is the two-qubit Werner state $\rho_{Q_AQ_B} = (1-\nu)\left|\phi^+\right\rangle\left\langle\phi^+\right| + \nu\mathbb{1}/4$ (and the measurements are as described in section 5.2). The quantum bit error rate is then $Q=\frac{\nu}{2}$, and the expected winning probability is $\omega_{\mathrm{exp}} = \frac{2+\sqrt{2}(1-2Q)}{4}$.

We emphasize that this is an assumption regarding the *honest* implementation and it does not in any way restrict the actions of the adversary (and, in particular, the types of imperfections in the device). Furthermore, the analysis done below can be adapted to any other honest implementation of interest.

5.5.1. Leakage due to error correction.

To compare the rates, we first need to explicitly upper bound the leakage of information due to the error correction protocol, leak_{EC}. As mentioned before, this can be done by evaluating $H_0^{\varepsilon'_{\text{EC}}}(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT})$ on Alice and Bob's state in an honest i.i.d. implementation of the protocol, described in section 5.2.

For this, we first use the following relation between H_0^{ε} and $H_{\max}^{\varepsilon'}$ [76, Lemma 18]:

$$H_0^{\varepsilon'_{\text{EC}}}(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT}) \leq H_{\max}^{\frac{\varepsilon'_{\text{EC}}}{2}}\left(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT}\right) + \log\left(8/\varepsilon'^2_{\text{EC}} + 2/\left(2-\varepsilon'_{\text{EC}}\right)\right) \ .$$

The nonasymptotic version of the asymptotic equipartition property [74, Theorem 9] (see also [72, Result 5]) tells us that

$$H_{\max}^{\frac{\varepsilon'_{\text{EC}}}{2}}\left(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT}\right) \leq nH(A_i|\tilde{B}_iX_iY_iT_i) + \sqrt{n}\delta(\varepsilon'_{\text{EC}},\tau)$$

for $\tau = 2\sqrt{2^{H_{\max}(A_i|\tilde{B}_iX_iY_iT_i)}} + 1$ and $\delta(\varepsilon'_{\text{EC}},\tau) = 4\log\tau\sqrt{2\log\left(8/\varepsilon'^{2}_{\text{EC}}\right)}$.

For the honest implementation of Protocol 5.1, $H_{\max}(A_i|\tilde{B}_iX_iY_iT_i) = 1$ and

$$\begin{aligned}
H(A_i|\tilde{B}_iX_iY_iT_i) &= \Pr(T_i = 0)\cdot H(A_i|\tilde{B}_iX_iY_i, T_i = 0) \\
&\quad + \Pr(T_i = 1)\cdot H(A_i|\tilde{B}_iX_iY_i, T_i = 1) \\
&= (1-\gamma)\cdot H(A_i|\tilde{B}_iX_iY_i, T_i = 0) \\
&\quad + \gamma\cdot H(A_i|\tilde{B}_iX_iY_i, T_i = 1) \\
&= (1-\gamma)\, h(Q) + \gamma h(\omega_{\text{exp}}) \ ,
\end{aligned}$$

where the first equality follows from the definition of conditional entropy and the second from the way T_i is chosen in Protocol 5.1. The last equality holds since for generation rounds the error rate (i.e., the probability that A_i and $\tilde{B}_i$ differ) in the honest case is Q and for test rounds given $\tilde{B}_i, X_i$, and Y_i Bob can guess A_i correctly with probability ω_{exp}.

We thus have

$$\begin{aligned}
H_0^{\varepsilon'_{\text{EC}}}\left(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{XYT}\right) &\leq n\left[(1-\gamma)\,h(Q) + \gamma h(\omega_{\text{exp}})\right] \\
&\quad + \sqrt{n}4\log\left(2\sqrt{2}+1\right)\sqrt{2\log\left(8/\varepsilon'^{2}_{\text{EC}}\right)} \\
&\quad + \log\left(8/\varepsilon'^2_{\text{EC}} + 2/\left(2-\varepsilon'_{\text{EC}}\right)\right) \ .
\end{aligned}$$

Plugging this into (5.1), we get

$$\begin{aligned}
\text{leak}_{\text{EC}} \leq n\left[(1-\gamma)\,h(Q) + \gamma h(\omega_{\text{exp}})\right] + \sqrt{n}4\log\left(2\sqrt{2}+1\right)\sqrt{2\log\left(8/\varepsilon'^{2}_{\text{EC}}\right)} \\
+ \log\left(8/\varepsilon'^2_{\text{EC}} + 2/\left(2-\varepsilon'_{\text{EC}}\right)\right) + \log\left(\frac{1}{\varepsilon_{\text{EC}}}\right) \ .
\end{aligned} \tag{5.9}$$

5.5.2. Key rate curves. In Appendix B, a slightly modified protocol is considered in which, instead of fixing the number of rounds in the protocol, only the expected number of rounds is fixed.

The completeness and soundness proofs follow along the same lines as the proofs above, as detailed in Appendix B. The analysis presented in the appendix leads to improved key rates for the modified protocol and are the ones presented here.[26]

[26] The key rate curves for a fixed number of rounds n have the same shape as the curves presented here but require more signals to achieve the same rates (the difference is roughly two orders of magnitude).

In Figure 5, the expected key rate $r = \ell/\bar{n}$ is plotted as a function of the quantum bit error rate Q for several values of the expected number of rounds $\bar{n}$. For $\bar{n} = 10^{15}$, the curve already essentially coincides with the key rate achieved in the *asymptotic i.i.d.* case, that is, when restricting the adversary to collective attacks [57, equation (12)] (see also Figure 2 therein). As the key rate for the asymptotic i.i.d. case was shown to be optimal in [57] (for practically the same protocol), it acts as an upper bound on the key rate and the amount of tolerable noise for the general case considered in this work. Hence, for large enough number of rounds our key rate becomes optimal and the protocol can tolerate up to the maximal error rate $Q = 7.1\%$.

In an asymptotic analysis (i.e., with infinite resources $\bar{n} \to \infty$), it is well understood that the soundness and completeness errors $\varepsilon^s_{\mathrm{QKD}}, \varepsilon^c_{\mathrm{QKD}}$ should tend to zero as $\bar{n}$ increases. However, in the nonasymptotic scenario considered here these errors are always finite. We therefore fix some values for them which are considered to be realistic and relevant for actual applications. We choose the parameters such that the security parameters are at least as good (and, in general, even better) as in [68], such that a fair comparison can be made. All other parameters are chosen in a consistent way while (roughly) optimizing the key rate.

In Figure 6, r is plotted as a function of $\bar{n}$ for several values of Q. As can be seen from the figure, the achieved rates are significantly higher than those achieved in previous works. Moreover, they are practically comparable to the key rates achieved in device-*dependent* QKD (see Figure 1 in [68]). The main difference between the curves for the device-dependent case and the independent one is the minimal value of $\bar{n}$ which is required for a positive key rate. (That is, for the protocols considered in [68], one can get a positive key rate with fewer rounds.) It is possible that by further optimizing the parameters a positive key rate can also be achieved in our setting in the regime $\bar{n} = 10^4 - 10^6$ for the different error rates.

6. Randomness expansion. We show how the entropy accumulation protocol can be used to perform randomness expansion. This can be achieved based on any nonlocal game, for which one is able to prove a good bound in (3.4). For concreteness, we focus on the CHSH game, for which an explicit bound is provided by Corollary 4.2. Although the protocol can be used to achieve larger expansion factors, we give specific bounds that optimize the linear output rate, under the assumption that a small linear number of uniformly random bits is available to the experimenter for the execution of the protocol.

In order to minimize the amount of randomness required to execute the protocol, we adapt the main entropy accumulation protocol, Protocol 3.1, by deterministically choosing inputs in the generation rounds from $\mathcal{X}_g = \{0\}$ and $\mathcal{Y}_g = \{0\}$. In particular, there is no use for the input 2 to the B device, and no randomness is required for the generation rounds.[27] Aside from the last step of randomness amplification, the remainder of the protocol is essentially the same as Protocol 3.1 (in its instantiation with the CHSH game considered in section 4). The complete protocol is described as Protocol 6.1.

Corollary 4.2 provides a lower bound on the min-entropy generated by the protocol. Given that we are concerned here not only with *generating* randomness, but also with *expanding* the amount of randomness initially available to users of the protocol, we now evaluate the total number of random bits that is needed to execute

[27] This requires both users to know which rounds are selected as generation rounds, i.e., to share the RV T_i. For the purposes of randomness expansion, this does not even require communication, as we may assume the parties are co-located.

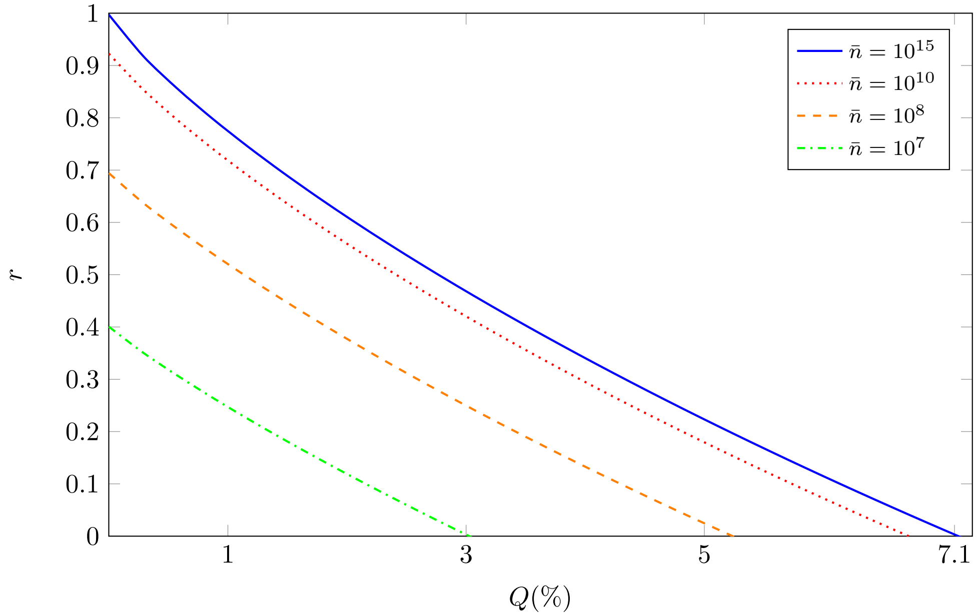

FIG. 5. *The expected key rate $r = \ell/\bar{n}$ as a function of the quantum bit error rate Q for several values of the expected number of rounds $\bar{n}$. For $\bar{n} = 10^{15}$, the curve essentially coincides with the curve for the i.i.d. asymptotic case* [57, *equation* (12)]. *The following values for the error terms were chosen: $\varepsilon_{\text{EC}} = 10^{-10}$, $\varepsilon^s_{\text{QKD}} = 10^{-5}$, and $\varepsilon^c_{\text{QKD}} = 10^{-2}$.*

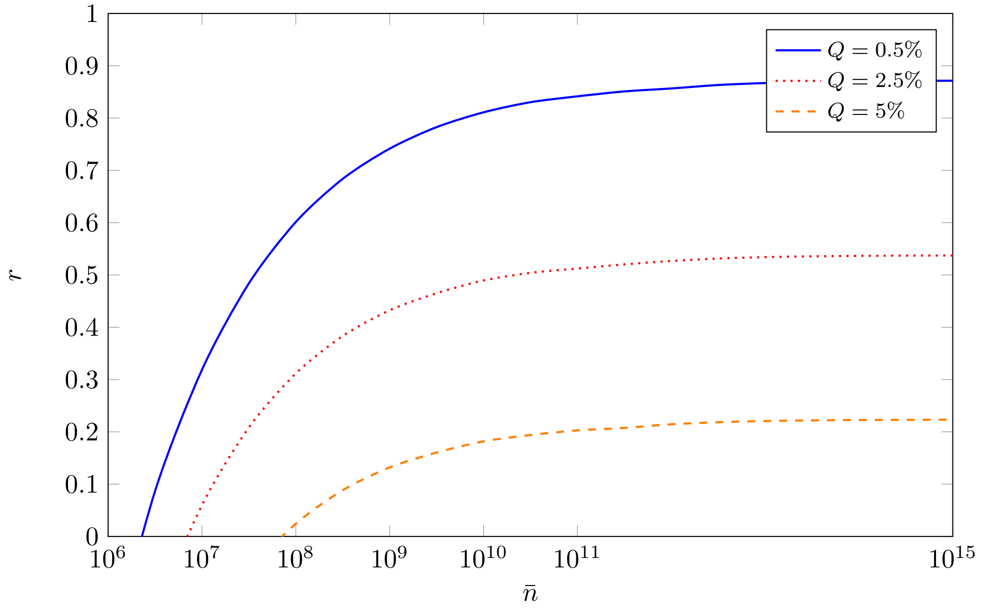

FIG. 6. *The expected key rate $r = \ell/\bar{n}$ as a function of the expected number of rounds $\bar{n}$ for several values of the quantum bit error rate Q. For $Q = 0.5\%$, 2.5%, and 5%, the achieved key rates are approximately $r = 87\%$, 53%, and 22%, respectively. The following values for the error terms were chosen: $\varepsilon_{\text{EC}} = 10^{-10}$, $\varepsilon^s_{\text{QKD}} = 10^{-5}$, and $\varepsilon^c_{\text{QKD}} = 10^{-2}$.*

Protocol 6.1 Randomness expansion protocol.

```
Arguments:
    $G$ – CHSH game restricted to $\mathcal{X}_t = \mathcal{Y}_t = \{0, 1\}$.
    $D$ – untrusted device of two components that can play $G$ repeatedly
    $n \in \mathbb{N}_+$ – number of rounds
    $\gamma \in (0, 1]$ – expected fraction of test rounds
    $\omega_{\text{exp}}$ – expected winning probability in $G$ for an honest (perhaps noisy) implementation
    $\delta_{\text{est}} \in (0, 1)$ – width of the statistical confidence interval for the estimation test

1: For every round $i \in [n]$, do steps 2–5:
2:     Bob chooses a random bit $T_i \in \{0, 1\}$ such that $\Pr(T_i = 1) = \gamma$.
3:     If $T_i = 0$, Alice and Bob choose $(X_i, Y_i) = (0, 0)$. If $T_i = 1$, they choose uniformly random inputs $(X_i, Y_i) \in \mathcal{X}_t \times \mathcal{Y}_t$.
4:     Alice and Bob use $D$ with $X_i, Y_i$ and record their outputs as $A_i$ and $B_i$, respectively.
5:     If $T_i = 1$, they set $C_i = w(A_i, B_i, X_i, Y_i)$.
6: Alice and Bob abort if $\sum_j C_j < (\omega_{\text{exp}}\gamma - \delta_{\text{est}}) \cdot n$.
7: They return $\text{Ext}(\mathbf{AB}, \mathbf{S})$, where Ext is the extractor from Lemma 6.3 and $\mathbf{S}$ is a uniformly random seed.
```

Protocol 6.1.

Input randomness. Random bits are required to select which rounds are generation rounds, i.e., the RV $\mathbf{T}$, to select inputs to the devices in the testing rounds, i.e., those for which $T_i = 0$, and to select the seed for the extractor in step 7.

The RVs T_i are chosen independently according to a biased Bernoulli(γ) distribution. The following lemma shows that approximately $8h(\gamma)n$ uniformly random bits are sufficient to generate the T_i, provided one allows for the possibility of a small deviation error.

LEMMA 6.1. *Let $\gamma > 0$. There is an efficient procedure such that for any integer n, given $r = 8h(\gamma)n$ uniformly random bits as inputs, the procedure either aborts, with probability at most $\varepsilon_{\text{SA}} = \exp(-\Omega(\gamma^3 \log^{-2} \gamma n))$, or outputs n bits $T_1, \dots, T_n$ whose distribution is within statistical distance at most ε_{SA} of n i.i.d. Bernoulli(γ) RVs.*

Proof. It is well known that using the interval algorithm [41] it is possible to sample exactly from m i.i.d. Bernoulli(γ) RVs using an expected number of random bits at most $h(\gamma)m + 2$; furthermore, the maximum number of random bits needed is at most $Cm \log \gamma^{-1}$ for some constant C.

In order to obtain a bound on the maximum number of random bits used that holds with high probability, let $\alpha = h(\gamma)$ and partition $\{1, \dots, n\}$ into at most $t = \lceil \alpha n \rceil$ chunks of $m = \lceil 1/\alpha \rceil$ consecutive integers each. Suppose we repeat the interval algorithm for each chunk. Let N_i be the number of uniform bits used to generate the T_j associated with the ith chunk. Then, by the above, $\text{E}[N_i] \leq h(\gamma)m + 2$ and $N_i \leq Cm \log \gamma^{-1}$. Applying the Hoeffding inequality,

$$\Pr\left(\sum_{i=1}^{t} N_i > 2(h(\gamma)m + 2)t\right) \leq e^{-C' \frac{(h(\gamma)m+2)^2}{m^2 \log^2 \gamma^{-1}} t} \leq e^{-C'' \frac{\gamma^3}{\log^2 \gamma^{-1}} n}$$

for some constants $C', C'' > 0$ and given our choice of α. Using $mt \leq 2n$ and $t \leq n$

gives the claimed bound. ∎

Remark 6.2. If one is willing to settle for a bound on the number of uniform bits used *in expectation*, then using the procedure from [41] it is possible to *exactly* sample n i.i.d. Bernoulli(γ) RVs using an expected number of random bits at most $h(\gamma)n+2$.

It remains to account for the random bits required to generate inputs in the testing rounds, for which $T_i = 0$. By Hoeffding's inequality, there are at most $2\gamma n$ such rounds but with probability $\exp(-\Omega(\gamma^2 n)) \leq \varepsilon_{\mathrm{SA}}$ for large enough n. Together with Lemma 6.1 we conclude that $10\gamma n$ uniformly random bits are sufficient to execute the protocol with a probability of success (up to but not including step 6) at least $1 - e^{-\tilde{\Omega}(\gamma^3)n}$. We also note that if one is only concerned with the expected number of random bits used, then $(h(\gamma)+\gamma)n+2$ bits are sufficient.

Extraction. In the last step of the protocol, step 7, the user applies a quantum-proof extractor to $\mathbf{AB}$ in order to produce a random string that is close to being uniformly distributed. This step requires the use of an additional seed $\mathbf{S}$ of uniformly random bits. We use the following construction, based on Trevisan's extractor, designed to maximize the output length while not using too much seed.

LEMMA 6.3. *For any $\delta > 0$, there is a $c = c(\delta) > 0$ such that the following holds: For all large enough integers n and any $k \geq \delta n$, there is an efficient procedure* $\mathrm{Ext} : \{0,1\}^{2n} \times \{0,1\}^d \to \{0,1\}^m$ *such that $d = \lceil \delta n \rceil$ and $m = \lceil k - 9\log k \rceil$, and is such that for $\varepsilon_{\mathrm{EX}} = \exp(-c(n/\log n)^{1/2})$ and any classical-quantum state $\rho_{\mathbf{A}E}$ such that $H_{\min}^{\varepsilon_{\mathrm{EX}}}(\mathbf{A}|E)_\rho \geq k$ it holds that*

$$\|\rho_{\mathrm{Ext}(\mathbf{A},\mathbf{S})\mathbf{S}E} - \rho_{U_m} \otimes \rho_{U_d} \otimes \rho_E\|_1 \leq 2\varepsilon_{\mathrm{EX}} \ ,$$

where $\mathbf{S} \in \{0,1\}^d$ is a uniformly distributed random seed and ρ_{U_m}, ρ_{U_d} are totally mixed states on m and d bits, respectively.

Proof. We use the construction given in [25, Corollary 5.1]. To get the parameters stated here, we note that provided c is chosen small enough with respect to δ our choice of $\varepsilon_{\mathrm{EX}}$ ensures that the seed length $d = O(\log^2(n/\varepsilon_{\mathrm{EX}})\log m)$ can be made smaller than δn. The conclusion on the trace distance follows from the guarantee of strong extractor given by [25, Corollary 5.1] using an argument similar to the proof of [7, Lemma 17]. ∎

We state the results of the above discussions as the following theorem, stating the guarantees of the randomness expansion protocol.

THEOREM 6.4. *Let $\gamma, \delta > 0$. Let $\varepsilon_{\mathrm{EX}}$ be as in Lemma* 6.3. *Then, for all large enough n, $\varepsilon_{\mathrm{EA}} \in (0,1)$, and ε_s such that $\varepsilon_{\mathrm{SA}} < \varepsilon_s + \varepsilon_{\mathrm{SA}} \leq \varepsilon_{\mathrm{EX}}$, Protocol* 3.1 *is an $(\varepsilon_{EA}^c + \varepsilon_{\mathrm{SA}}, 2\varepsilon_{\mathrm{EX}})$-secure $[(8h(\gamma)+\delta)n] \to [n \cdot \eta_{\mathrm{opt}}(\varepsilon_s - \varepsilon_{\mathrm{SA}}, \varepsilon_{\mathrm{EA}}) - 9\log n]$ randomness expansion protocol. That is, either Protocol* 3.1 *aborts with probability greater than $\varepsilon_{\mathrm{EA}}$ or it generates a string of length $m \geq n \cdot \eta_{\mathrm{opt}}(\varepsilon_s, \varepsilon_{\mathrm{EA}}) - 9\log n$ (where η_{opt} is defined in* (4.1)*) such that*

$$\|\rho_{ZRE} - \rho_{U_m} \otimes \rho_{RE}\|_1 \leq 2\varepsilon_{\mathrm{EX}} + \varepsilon_{\mathrm{SA}} \ ,$$

where R is a register holding all the initial random bits used in the protocol (including the seed $\mathbf{S}$).

Proof. Let D be any device and ρ the state (as defined in (3.1)) generated right before step 6 of Protocol 6.1. Let Ω (as defined in (3.2)) be the event that the protocol does not abort, and $\rho_{|\Omega}$ be the state conditioned on Ω. Then, applying Corollary 4.2, we obtain that for any $\varepsilon_{\mathrm{EA}}, \varepsilon'_{\mathrm{s}} \in (0,1)$, either the protocol aborts with probability greater than $1 - \varepsilon_{\mathrm{EA}}$ or

$$H_{\min}^{\varepsilon'_{\mathrm{s}}+\varepsilon_{\mathrm{SA}}} (\mathbf{AB}|\mathbf{XYT}E)_{\rho_{|\Omega}} > n \cdot \eta_{\mathrm{opt}}(\varepsilon'_{\mathrm{s}}, \varepsilon_{\mathrm{EA}}) \;, \tag{6.1}$$

where η_{opt} is as defined in (4.1) and the additional smoothness parameter $\varepsilon_{\mathrm{SA}}$ accounts for the error in the verifier's input sampling procedure, as described in Lemma 6.1.[28] Given the bound equation (6.1), the guarantee on m claimed in the theorem follows from Lemma 6.3.

Finally, the completeness of the protocol follows directly from the completeness of the entropy accumulation protocol, Protocol 3.1, as stated in Lemma 3.1, and the verifier's input sampling procedure, described in Lemma 6.1. □

Assuming a choice $\delta = \gamma$, the number of random bits required in the protocol scales linearly, roughly as $\sim 9\gamma n$.

For $\gamma \to 1$, which corresponds to randomness generation (also called randomness certification, i.e., the guarantee of "fresh" randomness independent of the inputs), the values of η_{opt} plotted in Figure 3 give a good idea of the rate of randomness generation that can be achieved from Protocol 6.1 for different choices of the security parameters. The rate is to be compared to the rate that was shown to be achievable for randomness expansion in the case of *classical* adversaries only in [58, Figure 2]; see also [59]. Our result, in contrast, holds against *quantum* adversaries. The rate is much better than the ones obtained in [77, 53].

For randomness expansion, one would select a small value of γ. If γ is a small constant, then Theorem 6.4 guarantees a constant expansion factor. One may wish to go further, by selecting a γ that scales sublinearly, polynomially, or even polylogarithmically, in the number of rounds (e.g., to achieve exponential expansion). It is possible to adapt our results to guarantee a linear production of randomness even for such parameters by suitably adapting Protocol 3.1 so that rounds are grouped in blocks, as in the modification of the entropy accumulation protocol described in Appendix B.

7. Open questions.

Several questions are left open:

1. Our results yield essentially optimal values for the leading- and second-order constants, c_1 and c_2, that govern the achievable rate curves. As loophole-free Bell tests (a necessity for DI cryptography) are finally being realized [43, 70, 37], it becomes increasingly relevant to achieve the best possible dependence of the rate curves on the number of rounds n, even for very small values of n. As can be seen from Figures 3 and 5, our rate curves approach (and essentially coincide) with the optimal curves as the number of rounds increases. One thing that can perhaps still be further optimized is the dependency on the number of rounds or, in other words, how fast the curves approach the optimal curve. The explicit dependency on n given in (5.4) is already close to optimal, but the numerical analysis used to plot the curves can be made somewhat better for the range of $n = 10^4 - 10^6$. Although this seems like a minor issue, it can make actual implementations more feasible.

[28] The log(13) term in the definition of η in (4.1) could be replaced by a log(9) to account for the fact that here $d_{B_i} = 2$, instead of $d_{B_i} = 3$ in section 4.

2. Are there similar protocols, based on a different Bell inequality, that can lead to better entropy rates? To apply our proof to other Bell inequalities, one should find a good bound on the min-tradeoff function, as done in (4.7) for the CHSH inequality. For many Bell inequalities, such bounds are known but for the min-entropy instead of the von Neumann entropy. In most cases, using a bound on the min-entropy will result in far from optimal rate curves. Therefore, to adapt our protocol to other Bell inequalities, one should probably bound the min-tradeoff function using the von Neumann entropy directly. Unfortunately, we do not know of any general technique to achieve such tight bounds.
3. Are there other protocols, e.g., with two-way classical postprocessing, which achieve better key rates? The optimality of our key rates is only with respect to the structure of the considered protocol.

Appendix A. Summary of parameters, constants, and variables.

TABLE A.1
Parameters and constants used throughout the paper.

Symbol	Meaning	Relation to other parameters
$n \in \mathbb{N}_+$	number of rounds	
$\gamma \in (0,1]$	expected fraction of Bell violation estimation rounds	
$\omega_{\text{exp}} \in [0,1]$	expected winning probability in an honest (perhaps noisy) implementation	
$\delta_{\text{est}} \in (0,1)$	width of the statistical confidence interval for the Bell violation estimation test	
ε_{s}	smoothing parameter	
ε^c_{EA}	completeness error of the entropy accumulation protocol	given in (3.3)
ε_{EA}	the error probability of the entropy accumulation protocol	
leak_{EC}	the leakage of the error correction protocol	given in (5.1)
$\varepsilon_{\text{EC}}, \varepsilon'_{\text{EC}}$	error probabilities of the error correction protocol	
$\varepsilon^c_{\text{EC}}$	completeness error of the error correction protocol	$\varepsilon^c_{\text{EC}} = \varepsilon'_{\text{EC}} + \varepsilon_{\text{EC}}$
$\varepsilon^c_{\text{PE}}$	completeness error of the parameter estimation step	given in (5.2)
ε_{PA}	error probability of the privacy amplification protocol	given in (5.3)
ℓ	final key length in the DIQKD protocol	given in (5.4)
ε^c_{QKD}	completeness error of the DIQKD protocol	$\varepsilon^c_{QKD} \leq \varepsilon^c_{EC} + \varepsilon^c_{EA} + \varepsilon_{EC}$
ε^s_{QKD}	soundness error of the DIQKD protocol	$\varepsilon^s_{\text{QKD}} \leq \varepsilon_{\text{EC}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{s}}$
ε_{SA}	error probability of the input sampling procedure used in the randomness expansion protocol	given in Lemma 6.1
ε_{EX}	error probability of the extractor used in the randomness expansion protocol	given in Lemma 6.3

TABLE A.2
RVs and quantum systems used throughout the paper.

RVs and systems	Meaning
$X_i \in \mathcal{X}$	Alice's input in round $i \in [n]$
$Y_i \in \mathcal{Y}$	Bob's input in round $i \in [n]$
$A_i \in \mathcal{A}$	Alice's output in round $i \in [n]$
$B_i \in \mathcal{B}$	Bob's output in round $i \in [n]$
$T_i \in \{0,1\}$	indicator of the estimation test in round i: $T_i = \begin{cases} 0, & i\text{th round is not a test round,} \\ 1, & i\text{th round is a test round.} \end{cases}$
$F_i \in \{0,1\}$	a random uniform bit for the symmetrization step in round $i \in [n]$
$C_i \in \{\perp,0,1\}$	indicator of the correlation in the test rounds: $C_i = \begin{cases} \perp, & T_i = 0, \\ 0, & T_i = 1 \text{ and the test fails} \\ 1, & T_i = 1 \text{ and the test succeeds.} \end{cases}$
E	register of Eve's quantum state
R_i	register of the (unknown) quantum state $\rho^i_{Q_A Q_B}$ of Alice and Bob's devices after step i of the protocol for $i \in \{0\} \cup [n]$

Appendix B. An improved dependency on the test probability γ.

In this section, we show how the EAT can be used in a slightly different way than what was done in the main text. This results in an entropy rate which has a better dependency on the probability of a test round γ, compared to the entropy rate given in (4.1) in section 4. The improved entropy rate derived here is the one used for calculating the key rates of the DIQKD protocol in section 5.5.2.

B.1. Modified entropy accumulation protocol.

We use a different entropy accumulation protocol, given as Protocol B.1. In this modified protocol, instead of considering each round separately we consider blocks of rounds. A block is defined by a sequence of rounds: in each round, a test is carried out with probability γ (and otherwise the round is a generation round). The block ends when a test round is being performed and then the next block begins. If for $s_{\max}$ rounds there was no test, the block would end without performing a test and the next would begin. Thus, the blocks can be of different lengths, but they all consist of at most $s_{\max}$ rounds.

In this setting, instead of fixing the number of rounds n in the beginning of the protocol, we fix the number of blocks m. The expected length of block is

$$\begin{aligned} \bar{s} = \sum_{s\in[s_{\max}]} \left[s(1-\gamma)^{(s-1)}\gamma \right] + s_{\max}(1-\gamma)^{s_{\max}} &= \frac{1-(1-\gamma)^{s_{\max}}}{\gamma} \\ &= \sum_{s\in[s_{\max}]} \left[(1-\gamma)^{(s-1)} \right] . \qquad \text{(B.1)} \end{aligned}$$

The expected number of rounds is denoted by $\bar{n} = m \cdot \bar{s}$.

Compared to the main text, we now have an RV $\tilde{C}_j \in \{0,1,\perp\}$ for each block, instead of each round. Alice and Bob set $\tilde{C}_j$ to be 0 or 1, depending on the result of the game in the block's test round (i.e., the last round of the block), or $\tilde{C}_j = \perp$ if a test round was not carried out in the block. By the definition of the blocks, we have $\Pr[\tilde{C}_j = \perp] = (1-\gamma)^{s_{\max}}$.

Note that the symmetrization step was dropped in Protocol B.1 just for simplicity,

Protocol B.1 Modified entropy accumulation protocol.

```
Arguments:
    $G$ – two-player nonlocal game
    $\mathcal{X}_g, \mathcal{X}_t \subset \mathcal{X}$ – generation and test inputs for Alice
    $\mathcal{Y}_g, \mathcal{Y}_t \subset \mathcal{Y}$ – generation and test inputs for Bob
    $D$ – untrusted device of (at least) two components that can play $G$ repeatedly
    $m \in \mathbb{N}_+$ – number of blocks
    $s_{\max} \in \mathbb{N}_+$ – maximal length of a block
    $\gamma \in (0,1]$ – probability of a test round
    $\omega_{\exp}$ – expected winning probability in $G$ for an honest (perhaps noisy) implementation
    $\delta_{\text{est}} \in (0,1)$ – width of the statistical confidence interval for the estimation test

1:  For every block $j \in [m]$, do steps 2–9:
2:      Set $i = 0$ and $C_j = \perp$.
3:      If $i \leq s_{\max}$:
4:          Set $i = i + 1$.
5:          Alice and Bob choose $T_i \in \{0,1\}$ at random such that $\Pr(T_i = 1) = \gamma$.
6:          If $T_i = 0$, Alice and Bob choose inputs $X_i \in \mathcal{X}_g$ and $Y_i \in \mathcal{Y}_g$, respectively. If $T_i = 1$, they choose inputs $X_i \in \mathcal{X}_t$ and $Y_i \in \mathcal{Y}_t$.
7:          Alice and Bob use $D$ with $X_i, Y_i$ and record their outputs as $A_i$ and $B_i$, respectively.
8:          If $T_i = 0$, Bob updates $B_i$ to $B_i = \perp$.
9:          If $T_i = 1$, they set $\tilde{C}_j = w\left(A_i, B_i, X_i, Y_i\right)$ and $i = s_{\max} + 1$.
10: Alice and Bob abort if $\sum_{j \in [m]} \tilde{C}_j < [\omega_{\exp}\left(1 - (1-\gamma)^{s_{\max}}\right) - \delta_{\text{est}}] \cdot m$.
```

as it plays no role in the considered modification; it can (and should) be handled exactly as done in section 4.

B.2. Modified min-tradeoff function. Below we apply the EAT on blocks of outputs instead of single rounds directly. Let $\mathcal{M}_j$ denote the EAT channels defined by the actions of steps 2–9 in Protocol B.1, combined with the quantum channels that model the device's actions in those steps. It is easy to verify that $\mathcal{M}_j$ fulfil the necessary conditions given in Definition 2.5.

We now construct a min-tradeoff function for $\mathcal{M}_j$. Let $\tilde{p}$ be a probability distribution over $\{0, 1, \perp\}$. Our goal is to find $F_{\min}$ such that

$$\forall j \in [m], \qquad F_{\min}(\tilde{p}) \leq \inf_{\sigma_{R_{j-1}R'} : \mathcal{M}_j(\sigma)_{\tilde{C}_j} = \tilde{p}} H\left(\vec{A}_j \vec{B}_j | \vec{X}_j \vec{Y}_j \vec{T}_j R'\right)_{\mathcal{M}_j(\sigma)}, \tag{B.2}$$

where $\vec{A}_j$ is a vector of varying length (but at most $s_{\max}$). We use $A_{j,i}$ to denote the ith entry of $\vec{A}_j$ and $A_{j,1}^{j,i-1} = A_{j,1} \ldots A_{j,i-1}$. Since we will only be interested in the entropy of $\vec{A}_j$, we can also describe it as a vector of length $s_{\max}$ which is initialized to be all $\perp$. For every actual round being performed in the block, the value of $A_{j,i}$ is updated. Thus, the entries of $\vec{A}_j$ which correspond to rounds which were not performed do not contribute to the entropy. We use similar notation for the other vectors of RVs.

To lower bound the right-hand side of (B.2), we first use the chain rule

$$H\left(\vec{A}_j\vec{B}_j|\vec{X}_j\vec{Y}_j\vec{T}_jR'\right) = \sum_{i\in[s_{\max}]} H(A_{j,i}B_{j,i}|\vec{X}_j\vec{Y}_j\vec{T}_jR'A_{j,1}^{j,i-1}B_{j,1}^{j,i-1}) \; . \tag{B.3}$$

Next, for every $i \in [s_{\max}]$,

$$\begin{aligned} &H(A_{j,i}B_{j,i}|\vec{X}_j\vec{Y}_j\vec{T}_jR'A_{j,1}^{j,i-1}B_{j,1}^{j,i-1}) \\ &\quad = \Pr[T_{j,1}^{j,i-1} = \vec{0}]H(A_{j,i}B_{j,i}|\vec{X}_j\vec{Y}_jR'A_{j,1}^{j,i-1}B_{j,1}^{j,i-1}T_{j,i}^{j,s_{\max}}T_{j,1}^{j,i-1} = \vec{0}) \\ &\qquad + \Pr[T_{j,1}^{j,i-1} \neq \vec{0}]H(A_{j,i}B_{j,i}|\vec{X}_j\vec{Y}_jR'A_{j,1}^{j,i-1}B_{j,1}^{j,i-1}T_{j,i}^{j,s_{\max}}T_{j,1}^{j,i-1} \neq \vec{0}) \\ &\quad = (1-\gamma)^{(i-1)}H(A_{j,i}B_{j,i}|\vec{X}_j\vec{Y}_jR'A_{j,1}^{j,i-1}B_{j,1}^{j,i-1}T_{j,i}^{j,s_{\max}}T_{j,1}^{j,i-1} = \vec{0}) \end{aligned}$$

since the entropy is not zero only if the ith round is being performed in the block, i.e., if a test was not performed before that round. Plugging this into (B.3), we get

$$\begin{aligned} &H\left(\vec{A}_j\vec{B}_j|\vec{X}_j\vec{Y}_j\vec{T}_jR'\right) \\ &\qquad = \sum_{i\in[s_{\max}]} (1-\gamma)^{(i-1)}H(A_{j,i}B_{j,i}|\vec{X}_j\vec{Y}_jR'A_{j,1}^{j,i-1}B_{j,1}^{j,i-1}T_{j,i}^{j,s_{\max}}T_{j,1}^{j,i-1} = \vec{0}) \; . \end{aligned}$$

Each term in the sum can now be identified as the entropy of a single round. We can therefore use the bound derived in the main text, as given in (4.6). For this, we denote by ω_i the winning probability in the ith round (given that a test was not performed before). Then it holds that

$$H\left(\vec{A}_j\vec{B}_j|\vec{X}_j\vec{Y}_j\vec{T}_jR'\right) \geq \sum_{i\in[s_{\max}]} (1-\gamma)^{(i-1)}\left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega_i\left(\omega_i - 1\right) + 3}\right)\right] \; , \tag{B.4}$$

where, by the actions of the EAT channel $\mathcal{M}_j$, the ω_i's must fulfil the constraint

$$\tilde{p}(1) = \sum_{i\in[s_{\max}]} \gamma(1-\gamma)^{(i-1)}\omega_i \; . \tag{B.5}$$

Note that, similarly to what was done in the main text, we only need to consider $\tilde{p}$ for which $\tilde{p}(1) + \tilde{p}(0) = 1 - (1-\gamma)^{s_{\max}}$ (otherwise the condition on the min-tradeoff function is trivial, as the infimum is over an empty set).

To find the min-tradeoff function $F_{\min}(\tilde{p})$, we therefore need to minimize (B.4) under the constraint of (B.5). The following lemma shows that the minimum is achieved when all ω_i are equal.

Lemma B.1. *The minimum of the function given on the right-hand side of* (B.4) *over* ω_i *constrained by* (B.5) *is achieved for* $\omega_i^* = \frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}}$ *for all* $i \in [s_{\max}]$.

Proof. Let $\vec{\omega} = \omega_1, \dots, \omega_{s_{\max}}$ and let

$$\begin{aligned} f(\vec{\omega}) &\equiv \sum_{i\in[s_{\max}]} (1-\gamma)^{(i-1)}\left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega_i\left(\omega_i - 1\right) + 3}\right)\right] \; , \\ g(\vec{\omega}) &\equiv \sum_{i\in[s_{\max}]} \gamma(1-\gamma)^{(i-1)}\omega_i - \tilde{p}(1) \; . \end{aligned}$$

Using the method of Lagrange multipliers, we should look for $\vec{\omega}^*$ such that $g(\vec{\omega}^*) = 0$ and $\nabla f(\vec{\omega}^*) = -\lambda \nabla g(\vec{\omega}^*)$ for some constant λ. $\nabla f(\vec{\omega}^*) = -\lambda \nabla g(\vec{\omega}^*)$ implies that for any i,

$$(1-\gamma)^{(i-1)} \frac{\mathrm{d}}{\mathrm{d}\omega_i} \left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega_i\left(\omega_i - 1\right) + 3} \right) \right] \Big|_{\omega_i^*} = -\lambda\gamma(1-\gamma)^{(i-1)}$$

and therefore

$$\frac{\mathrm{d}}{\mathrm{d}\omega_i} \left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega_i\left(\omega_i - 1\right) + 3} \right) \right] \Big|_{\omega_i^*} = -\lambda\gamma \; .$$

The function on the left-hand side of the above equation is strictly increasing. Hence, it must be that all ω_i^* are equal to some constant ω^*.

Last, we must have $g(\vec{\omega}^*) = 0$. Thus,

$$\sum_{i \in [s_{\max}]} \gamma(1-\gamma)^{(i-1)}\omega^* - \tilde{p}(1) = 0,$$

which means

$$\omega^* = \frac{\tilde{p}(1)}{\sum_{i\in[s_{\max}]} \gamma(1-\gamma)^{(i-1)}} = \frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}} \; . \qquad \square$$

Plugging the minimal values of ω_i into (B.4), we get that

$$\begin{aligned} H\left(\vec{A}_j\vec{B}_j|\vec{X}_j\vec{Y}_j\vec{T}_jR'\right) &\geq \sum_{i\in[s_{\max}]} (1-\gamma)^{(i-1)} \\ &\quad \times \left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}}\left(\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}} - 1\right) + 3} \right) \right] \\ &= \bar{s}\left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}}\left(\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}} - 1\right) + 3} \right) \right] \; , \end{aligned}$$

where we used (B.1) to get the last equality.

From this point, we can follow the same steps as in section 4 (cutting and gluing the function, etc.). The resulting min-tradeoff function is given by

$$F_{\min}\left(\tilde{p}, \tilde{p}_t\right) = \begin{cases} g\left(\tilde{p}\right) \; , & \tilde{p}(1) \leq \tilde{p}_t(1) \; , \\ \frac{\mathrm{d}}{\mathrm{d}\tilde{p}(1)} g(\tilde{p})\big|_{\tilde{p}_t} \cdot \tilde{p}(1) + \left(g(\tilde{p}_t) - \frac{\mathrm{d}}{\mathrm{d}\tilde{p}(1)} g(\tilde{p})\big|_{\tilde{p}_t} \cdot \tilde{p}_t(1) \right) \; , & \tilde{p}(1) > \tilde{p}_t(1) \; , \end{cases}$$

where

$$g(\tilde{p}) = \bar{s}\left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}}\left(\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}} - 1\right) + 3} \right) \right]$$

when $\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}} \in \left[\frac{3}{4}, \frac{2+\sqrt{2}}{4}\right]$ and $g(\tilde{p}) = \bar{s}$ when $\frac{\tilde{p}(1)}{1-(1-\gamma)^{s_{\max}}} \in \left[\frac{2+\sqrt{2}}{4}, 1\right]$.

The min-tradeoff function given above is effectively identical to the one derived in the main text; although it gives us a bound on the von Neumann entropy in a block, instead of a single round, this bound is exactly the expected length of a block, $\bar{s}$, times the entropy in one round. For $s_{\max} = 1$, the min-tradeoff function constructed in the main text is retrieved.

B.3. Modified entropy rate. Since we apply the EAT on the blocks, the entropy rate is now defined to be the entropy *per block*. We therefore get

$$\begin{aligned}\eta(\tilde{p},\tilde{p}_t,\varepsilon_{\mathrm{s}},\varepsilon_{\mathrm{e}}) &= F_{\min}\left(\tilde{p},\tilde{p}_t\right)\\ &\quad - \frac{1}{\sqrt{m}}2\left(\log(1+2\cdot 2^{s_{\max}}3^{s_{\max}}) + \left\lceil \frac{\mathrm{d}}{\mathrm{d}\tilde{p}(1)}g(\tilde{p})\Big|_{\tilde{p}_t}\right\rceil\right)\sqrt{1-2\log(\varepsilon_{\mathrm{s}}\cdot\varepsilon_{\mathrm{e}})}\ ,\\ \eta_{\mathrm{opt}}(\varepsilon_{\mathrm{s}},\varepsilon_{\mathrm{e}}) &= \max_{\frac{3}{4}<\tilde{p}_t(1)<\frac{2+\sqrt{2}}{4}} \eta(\omega_{\exp}\left[1-(1-\gamma)^{s_{\max}}\right]-\delta_{\mathrm{est}},\tilde{p}_t,\varepsilon_{\mathrm{s}},\varepsilon_{\mathrm{e}})\ ,\end{aligned}$$

and the total amount of entropy is given by

$$H_{\min}^{\varepsilon_{\mathrm{s}}}\left(\mathbf{AB}|\mathbf{XYTF}E\right)_{\rho_{|\Omega}} > m\cdot\eta_{\mathrm{opt}}(\varepsilon_{\mathrm{s}},\varepsilon_{\mathrm{EA}}) = \frac{\bar{n}}{\bar{s}}\cdot\eta_{\mathrm{opt}}(\varepsilon_{\mathrm{s}},\varepsilon_{\mathrm{EA}})\ . \tag{B.6}$$

By choosing $s_{\max} = \lceil\frac{1}{\gamma}\rceil$, the scaling of the entropy rate with γ is better than the rate derived in the main text. In particular, a short calculation reveals that the second-order term scales, roughly, as $\sqrt{\bar{n}/\gamma}$ instead of $\sqrt{n}/\gamma$.

B.4. Modified key rate. To get the final key rate, we need to repeat the same steps from the main text but this time applied to RVs varying lengths.

For this, we first observe that, with high probability, the actual number of rounds, n, cannot be much larger than the expected number of rounds, $\bar{n}$. Let S_i be the RV describing the length of block i, for $i\in[m]$, and N the RV describing the total number of rounds. Then $N = S_1+\cdots+S_m$. Since all the S_i are independent, identical, and have values in $\left[1,\frac{1}{\gamma}\right]$, we have

$$\Pr[N\geq\bar{n}+t]\leq\exp\left[-\frac{2t^2\gamma^2}{m(1-\gamma)^2}\right]\ .$$

Let $\varepsilon_t = \exp\left[-\frac{2t^2\gamma^2}{m(1-\gamma)^2}\right]$; then

$$t = \sqrt{-\frac{m(1-\gamma)^2\log\varepsilon_t}{2\gamma^2}}\ .$$

The first step in the derivation of the key rate which needs to be changed is the one given in (5.8). The quantity that needs to be upper bounded is $H_{\max}^{\frac{\varepsilon_{\mathrm{s}}}{4}}\left(\mathbf{B}|\mathbf{T}EN\right)_{\rho_{|\hat{\Omega}}}$; N can be included in the entropy since its value is fixed by $\mathbf{T}$. By the definition of the smooth max-entropy, we have

$$H_{\max}^{\frac{\varepsilon_{\mathrm{s}}}{4}}\left(\mathbf{B}|\mathbf{T}EN\right)\leq H_{\max}^{\frac{\varepsilon_{\mathrm{s}}}{4}-\sqrt{\varepsilon_t}}\left(\mathbf{B}|\mathbf{T}EN, N\leq\bar{n}+t\right)\ .$$

Following the same steps as in the proof of Lemma 5.3, we have

$$\begin{aligned}&H_{\max}^{\frac{\varepsilon_{\mathrm{s}}}{4}-\sqrt{\varepsilon_t}}\left(\mathbf{B}|\mathbf{T}EN, N\leq\bar{n}+t\right)_{\rho_{|\hat{\Omega}}}\\ &\qquad < \gamma(\bar{n}+t)+2\log 7\sqrt{\bar{n}+t}\sqrt{1-2\log\left((\varepsilon_{\mathrm{s}}/4-\sqrt{\varepsilon_t})\cdot(\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}})\right)}\ .\end{aligned}$$

With this modification and the modified entropy rate given in (B.6), we get

$$\begin{aligned}H_{\min}^{\varepsilon_{\mathrm{s}}}\left(\mathbf{A}|\mathbf{XYT}OE\right)_{\tilde{\rho}_{|\hat{\Omega}}} \geq{}& \frac{\bar{n}}{\bar{s}}\cdot\eta_{\mathrm{opt}}\left(\varepsilon_{\mathrm{s}}/4,\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}}\right)-\mathrm{leak}_{\mathrm{EC}}\\ &-3\log\left(1-\sqrt{1-(\varepsilon_{\mathrm{s}}/4)^2}\right)-\gamma(\bar{n}+t)\\ &-2\log 7\sqrt{\bar{n}+t}\sqrt{1-2\log\left((\varepsilon_{\mathrm{s}}/4-\sqrt{\varepsilon_t})\cdot(\varepsilon_{\mathrm{EA}}+\varepsilon_{\mathrm{EC}})\right)}\ .\end{aligned}$$

Similarly, the amount of leakage due to the error correction step $\mathrm{leak}_{\mathrm{EC}}$ should be modified as well. Following the steps in section 5.5.1, the quantity to be upper bounded is $H_{\max}^{\frac{\varepsilon'_{\mathrm{EC}}}{2}}\big(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{X}\mathbf{Y}\mathbf{T}N\big)$. Here as well we have

$$H_{\max}^{\frac{\varepsilon'_{\mathrm{EC}}}{2}}\left(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{X}\mathbf{Y}\mathbf{T}N\right) \leq H_{\max}^{\frac{\varepsilon'_{\mathrm{EC}}}{2}-\sqrt{\varepsilon_t}}\left(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{X}\mathbf{Y}\mathbf{T}N, N \leq \bar{n}+t\right) .$$

The asymptotic equipartition property can be used with the maximal length $\bar{n}+t$ to get

$$\begin{aligned} &H_{\max}^{\frac{\varepsilon'_{\mathrm{EC}}}{2}-\sqrt{\varepsilon_t}}\left(\mathbf{A}|\tilde{\mathbf{B}}\mathbf{X}\mathbf{Y}\mathbf{T}N, N \leq \bar{n}+t\right) \\ &\qquad \leq (\bar{n}+t)\cdot H(A_i|\tilde{B}_i X_i Y_i T_i) + \sqrt{\bar{n}+t}\;\delta(\varepsilon'_{\mathrm{EC}} - 2\sqrt{\varepsilon_t}, \tau) \end{aligned}$$

for $\tau = 2\sqrt{2^{H_{\max}(A_i|\tilde{B}_i X_i Y_i T_i)}}+1$ and

$$\delta(\varepsilon'_{\mathrm{EC}} - 2\sqrt{\varepsilon_t}, \tau) = 4\log\tau\sqrt{2\log\left(8/(\varepsilon'_{\mathrm{EC}} - 2\sqrt{\varepsilon_t})^2\right)} .$$

Continuing exactly as in section 5.5.1, we get

$$\begin{aligned} \mathrm{leak}_{\mathrm{EC}} \leq\ & (\bar{n}+t)\cdot\left[(1-\gamma)\,h(Q) + \gamma h(\omega_{\exp})\right] \\ & + 4\log\left(2\sqrt{2}+1\right)\sqrt{\bar{n}+t}\,\sqrt{2\log\left(8/(\varepsilon'_{\mathrm{EC}} - 2\sqrt{\varepsilon_t})^2\right)} \\ & + \log\left(8/\varepsilon'^2_{\mathrm{EC}} + 2/\left(2-\varepsilon'_{\mathrm{EC}}\right)\right) + \log\left(\frac{1}{\varepsilon_{\mathrm{EC}}}\right) . \end{aligned}$$

The parameter ε_t should be chosen such that the key rate is optimized. The resulting key rates are shown in Figures 5 and 6 in the main text.

REFERENCES

[1] 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 (2007), 230501, https://doi.org/10.1103/PhysRevLett.98.230501.

[2] A. Acín, N. Gisin, and L. Masanes, *From Bell's theorem to secure quantum key distribution*, Phys. Rev. Lett., 97 (2006), 120405, https://doi.org/10.1103/PhysRevLett.97.120405.

[3] A. Acín, S. Massar, and S. Pironio, *Efficient quantum key distribution secure against no-signalling eavesdroppers*, New J. Phys., 8 (2006), 126, https://doi.org/10.1088/1367-2630/8/8/126.

[4] A. Acín, S. Massar, and S. Pironio, *Randomness versus nonlocality and entanglement*, Phys. Rev. Lett., 108 (2012), 100402, https://doi.org/10.1103/PhysRevLett.108.100402.

[5] N. Aharon, S. Massar, S. Pironio, and J. Silman, *Device-independent bit commitment based on the CHSH inequality*, New J. Phys., 18 (2016), 025014, https://doi.org/10.1088/1367-2630/18/2/025014.

[6] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, *Practical device-independent quantum cryptography via entropy accumulation*, Nat. Commun., 9 (2018), 459, https://doi.org/10.1038/s41467-017-02307-4.

[7] R. Arnon-Friedman, C. Portmann, and V. B. Scholz, *Quantum-proof multi-source randomness extractors in the Markov model*, in Proceedings of the 11th Conference on the Theory of Quantum Computation, Communication and Cryptography, 2016, pp. 2:1–2:34, https://doi.org/10.4230/LIPIcs.TQC.2016.2.

[8] C. Bamps, S. Massar, and S. Pironio, *Device-independent randomness generation with sublinear shared quantum resources*, Quantum, 2 (2018), 86, https://doi.org/10.22331/q-2018-08-22-86.

[9] J. Barrett, R. Colbeck, and A. Kent, *Memory attacks on device-independent quantum cryptography*, Phys. Rev. Lett., 110 (2013), 010503, https://doi.org/10.1103/PhysRevLett.110.010503.

[10] J. Barrett, L. Hardy, and A. Kent, *No signaling and quantum key distribution*, Phys. Rev. Lett., 95 (2005), 010503, https://doi.org/10.1103/PhysRevLett.95.010503.

[11] N. J. Beaudry, *Assumptions in Quantum Cryptography*, preprint, https://arxiv.org/abs/1505.02792, 2015.

[12] J. S. Bell, *On the Einstein Podolsky Rosen paradox*, Phys. Phys. Fiz., 1 (1964), pp. 195–200, https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195.

[13] M. Ben-Or and D. Mayers, *General Security Definition and Composability for Quantum & Classical Protocols*, preprint, https://arxiv.org/abs/quant-ph/0409062, 2004.

[14] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984, pp. 175–179, https://doi.org/10.1016/j.tcs.2014.05.025.

[15] F. G. 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*, Nat. Commun., 7 (2016), 11345, https://doi.org/10.1038/ncomms11345.

[16] G. Brassard and L. Salvail, *Secret-key reconciliation by public discussion*, in Advances in Cryptology — EUROCRYPT '93, Springer, Berlin, Heidelberg, 1993, pp. 410–423, https://doi.org/10.1007/3-540-48285-7_35.

[17] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Bell nonlocality*, Rev. Modern Phys., 86 (2014), 419, https://doi.org/10.1103/RevModPhys.86.419.

[18] R. Canetti, *Universally composable security: A new paradigm for cryptographic protocols*, in Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, 2001, pp. 136–145, https://doi.org/10.1109/SFCS.2001.959888.

[19] K.-M. Chung, Y. Shi, and X. Wu, *Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions*, preprint, https://arxiv.org/abs/1402.4797, 2014.

[20] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett., 23 (1969), pp. 880–884, https://doi.org/10.1103/PhysRevLett.23.880.

[21] A. Coladangelo, A. Grilo, S. Jeffery, and T. Vidick, *Verifier-on-a-Leash: New Schemes for Verifiable Delegated Quantum Computation, with Quasilinear Resources*, preprint, https://arxiv.org/abs/1708.07359, 2017.

[22] R. Colbeck, *Quantum and Relativistic Protocols for Secure Multi-party Computation*, preprint, https://arxiv.org/abs/0911.3814, 2009.

[23] R. Colbeck and R. Renner, *Free randomness can be amplified*, Nat. Phys., 8 (2012), pp. 450–453, https://doi.org/10.1038/nphys2300.

[24] M. Coudron and H. Yuen, *Infinite randomness expansion with a constant number of devices*, in Proceedings of the 46th Annual ACM Symposium on Theory of Computing, 2014, pp. 427–436, https://doi.org/10.1145/2591796.2591873.

[25] A. De, C. Portmann, T. Vidick, and R. Renner, *Trevisan's extractor in the presence of quantum side information*, SIAM J. Comput., 41 (2012), pp. 915–940, https://doi.org/10.1137/100813683.

[26] C. Dhara, G. Prettico, and A. Acín, *Maximal quantum randomness in Bell tests*, Phys. Rev. A, 88 (2013), 052116, https://doi.org/10.1103/PhysRevA.88.052116.

[27] F. Dupuis and O. Fawzi, *Entropy Accumulation with Improved Second-Order*, preprint, https://arxiv.org/abs/1805.11652, 2018.

[28] F. Dupuis, O. Fawzi, and R. Renner, *Entropy Accumulation*, preprint, https://arxiv.org/abs/1607.01796, 2016.

[29] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev., 47 (1935), pp. 777–780, https://doi.org/10.1103/PhysRev.47.777.

[30] A. Ekert and R. Renner, *The ultimate physical limits of privacy*, Nature, 507 (2014), pp. 443–447, https://doi.org/10.1038/nature13132.

[31] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., 67 (1991), pp. 661–663, https://doi.org/10.1103/PhysRevLett.67.661.

[32] S. Fehr, R. Gelles, and C. Schaffner, *Security and composability of randomness expansion from Bell inequalities*, Phys. Rev. A, 87 (2013), 012335, https://doi.org/10.1103/PhysRevA.87.012335.

[33] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, *Phase-remapping attack in practical*

quantum-key-distribution systems, Phys. Rev. A, 75 (2007), 032314, https://doi.org/10.1103/PhysRevA.75.032314.

[34] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, *Full randomness from arbitrarily deterministic events*, Nat. Commun., 4 (2013), 2654, https://doi.org/10.1038/ncomms3654.

[35] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, *Full-field implementation of a perfect eavesdropper on a quantum cryptography system*, Nat. Commun., 2 (2011), 349, https://doi.org/10.1038/ncomms1348.

[36] A. Gheorghiu, E. Kashefi, and P. Wallden, *Robustness and device independence of verifiable blind quantum computing*, New J. Phys., 17 (2015), 083040, https://doi.org/10.1088/1367-2630/17/8/083040.

[37] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. Woo Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, *Significant-loophole-free test of Bell's theorem with entangled photons*, Phys. Rev. Lett., 115 (2015), 250401, https://doi.org/10.1103/PhysRevLett.115.250401.

[38] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, *Device-Independent Verifiable Blind Quantum Computation*, preprint, https://arxiv.org/abs/1502.02563, 2015.

[39] E. Hänggi and R. Renner, *Device-Independent Quantum Key Distribution with Commuting Measurements*), preprint, https://arxiv.org/abs/1009.1833, 2010.

[40] E. Hänggi, R. Renner, and S. Wolf, *Efficient device-independent quantum key distribution*, in Advances in Cryptology—EUROCRYPT 2010, Springer, Berlin, 2010, pp. 216–234, https://doi.org/10.1007/978-3-642-13190-5_11.

[41] T. S. Hao and M. Hoshi, *Interval algorithm for random number generation*, IEEE Trans. Inform Theory, 43 (1997), pp. 599–611, https://doi.org/10.1109/18.556116.

[42] P. Hayden, R. Jozsa, D. Petz, and A. Winter, *Structure of states which satisfy strong subadditivity of quantum entropy with equality*, Commun. Math. Phys., 246 (2004), pp. 359–374, https://doi.org/10.1007/s00220-004-1049-z.

[43] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau , and R. Hanson, *Loophole-free Bell inequality violation using electron spins separated by* 1.3 *kilometres*, Nature, 526 (2015), pp. 682–686, https://doi.org/10.1038/nature15759.

[44] J. Kaniewski and S. Wehner, *Device-independent two-party cryptography secure against sequential attacks*, New J. Phys., 18 (2016), 055004, https://doi.org/10.1088/1367-2630/18/5/055004.

[45] M. Kessler and R. Arnon-Friedman, *Device-Independent Randomness Amplification and Privatization*, preprint, https://arxiv.org/abs/1705.04148, 2017.

[46] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, *Quantum randomness extraction for various levels of characterization of the devices*, J. Phys. A, 47 (2014), 424028, https://doi.org/10.1088/1751-8113/47/42/424028.

[47] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, *High-speed device-independent quantum random number generation without a detection loophole*, Phys. Rev. Lett., 120 (2018), 010503, https://doi.org/10.1103/PhysRevLett.120.010503.

[48] 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 (2010), pp. 686–689, https://doi.org/10.1038/NPHOTON.2010.214.

[49] L. Masanes, *Universally composable privacy amplification from causality constraints*, Phys. Rev. Lett., 102 (2009), 140501, https://doi.org/10.1103/PhysRevLett.102.140501.

[50] L. Masanes, S. Pironio, and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices*, Nat. Commun., 2 (2011), 238, https://doi.org/10.1038/ncomms1244.

[51] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, *Full security of quantum key distribution from no-signaling constraints*, IEEE Trans. Inform. Theory, 60 (2014), pp. 4973–4986, https://doi.org/10.1109/TIT.2014.2329417.

[52] D. Mayers and A. Yao, *Quantum cryptography with imperfect apparatus*, in Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science, 1998, pp. 503–509, https://doi.org/10.1109/SFCS.1998.743501.

[53] C. A. Miller and Y. Shi, *Robust protocols for securely expanding randomness and distributing*

keys using untrusted quantum devices, J. ACM, 63 (2016), 33, https://doi.org/10.1145/2885493.

[54] C. A. Miller and Y. Shi, *Universal security for randomness expansion from the spot-checking protocol*, SIAM J. Comput., 46 (2017), pp. 1304–1335, https://doi.org/10.1137/15M1044333.

[55] M. Navascués, S. Pironio, and A. Acín, *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations*, New J. Phys., 10 (2008), 073013, https://doi.org/10.1088/1367-2630/10/7/073013.

[56] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK, 2002, https://doi.org/10.1017/CBO9780511976667.

[57] 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 (2009), 045021, https://doi.org/10.1088/1367-2630/11/4/045021.

[58] 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, 464 (2010), pp. 1021–1024, https://doi.org/10.1038/nature09008.

[59] S. Pironio and S. Massar, *Security of practical private randomness generation*, Phys. Rev. A, 87 (2013), 012336, https://doi.org/10.1103/PhysRevA.87.012336.

[60] C. Portmann and R. Renner, *Cryptographic Security of Quantum Key Distribution*, preprint, https://arxiv.org/abs/1409.3525, 2014.

[61] B. W. Reichardt, F. Unger, and U. Vazirani, *Classical command of quantum systems*, Nature, 496 (2013), pp. 456–460, https://doi.org/10.1038/nature12035.

[62] R. Renner, *Security of Quantum Key Distribution*, preprint, https://arxiv.org/abs/quant-ph/0512258, 2005.

[63] R. Renner and R. König, *Universally composable privacy amplification against quantum adversaries*, in Theory of Cryptography, Springer, Berlin, 2005, pp. 407–425, https://doi.org/10.1007/978-3-540-30576-7_22.

[64] R. Renner and S. Wolf, *Simple and tight bounds for information reconciliation and privacy amplification*, in Advances in Cryptology—ASIACRYPT 2005, Springer, Berlin, 2005, pp. 199–216, https://doi.org/10.1007/11593447_11.

[65] J. Ribeiro, G. Murta, and S. Wehner, *Fully device-independent conference key agreement*, Phys. Rev. A, 97 (2018), 022307, https://doi.org/10.1103/PhysRevA.97.022307.

[66] V. Scarani, *The device-independent outlook on quantum physics*, Acta Phys. Slovaca, 62 (2012), pp. 347–409.

[67] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, *Secrecy extraction from no-signaling correlations*, Phys. Rev. A, 74 (2006), 042339, https://doi.org/10.1103/PhysRevA.74.042339.

[68] V. Scarani and R. Renner, *Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing*, Phys. Rev. Lett., 100 (2008), 200501, https://doi.org/10.1103/PhysRevLett.100.200501.

[69] V. Scarani and R. Renner, *Security bounds for quantum cryptography with finite resources*, in Theory of Quantum Computation, Communication, and Cryptography, Springer, Berlin, 2008, pp. 83–95, https://doi.org/10.1007/978-3-540-89304-2_8.

[70] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, *Strong loophole-free test of local realism*, Phys. Rev. Lett., 115 (2015), 250402, https://doi.org/10.1103/PhysRevLett.115.250402.

[71] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, *Randomness extraction from bell violation with continuous parametric down-conversion*, Phys. Rev. Lett., 121 (2018), 150402, https://doi.org/10.1103/PhysRevLett.121.150402.

[72] M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, preprint, https://arxiv.org/abs/1203.2142, 2012.

[73] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, SpringerBriefs Math. Phys. 5, Springer, Cham, 2016, https://doi.org/10.1007/978-3-319-21891-5.

[74] M. Tomamichel, R. Colbeck, and R. Renner, *A fully quantum asymptotic equipartition*

property, IEEE Trans. Inform. Theory, 55 (2009), pp. 5840–5847, https://doi.org/10.1109/TIT.2009.2032797.

[75] M. Tomamichel, R. Colbeck, and R. Renner, *Duality between smooth min- and max-entropies*, IEEE Trans. Inform. Theory, 56 (2010), pp. 4674–4681, https://doi.org/10.1109/TIT.2010.2054130.

[76] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *Leftover hashing against quantum side information*, IEEE Trans. Inform. Theory, 57 (2011), pp. 5524–5535, https://doi.org/10.1109/TIT.2011.2158473.

[77] U. Vazirani and T. Vidick, *Certifiable quantum dice: Or, true random number generation secure against quantum adversaries*, in Proceedings of the 44th Annual ACM Symposium on Theory of Computing, 2012, pp. 61–76, https://doi.org/10.1145/2213977.2213984.

[78] U. Vazirani and T. Vidick, *Fully device-independent quantum key distribution*, Phys. Rev. Lett., 113 (2014), 140501, https://doi.org/10.1103/PhysRevLett.113.140501.

[79] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, *Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors*, New J. Phys., 13 (2011), 073024, https://doi.org/10.1088/1367-2630/13/7/073024.