Towards a realization of device-independent quantum key distribution

G. Murta[1], S.B. van Dam[1,2], J. Ribeiro[1], R. Hanson[1,2], and S. Wehner[1]

[1] QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands
[2] Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands

E-mail: `glauciamg.fis@gmail.com`

Abstract. In the implementation of device-independent quantum key distribution we are interested in maximizing the key rate, i.e. the number of key bits that can be obtained per signal, for a fixed security parameter. In the finite size regime, we furthermore also care about the minimum number of signals required before key can be obtained at all. Here, we perform a fully finite size analysis of device independent protocols using the CHSH inequality both for collective and coherent attacks. For coherent attacks, we sharpen the results recently derived in Arnon-Friedman *et al.*, Nat. Commun. 9, 459 (2018) [1], to reduce the minimum number of signals before key can be obtained. In the regime of collective attacks, where the devices are restricted to have no memory, we employ two different techniques that exploit this restriction to further reduce the number of signals. We then discuss experimental platforms in which DIQKD may be implemented. We analyse Bell violations and expected QBER achieved in previous Bell tests with distant setups and situate these parameters in the security analysis. Moreover, focusing on one of the experimental platforms, namely nitrogen-vacancy based systems, we describe experimental improvements that can lead to a device-independent quantum key distribution implementation in the near future.

1. Introduction

1.1. Quantum key distribution

Quantum key distribution (QKD) [2, 3] is a remarkable example of the advantages that quantum systems bring to accomplishing classical tasks. All the classical crypto-systems used for key exchange are based on computational assumptions and, therefore, are susceptible to retroactive attacks. Indeed, if an adversary keeps track of the public information exchanged during the communication of an encrypted message and, in a later future, a more efficient algorithm or faster machines become available, then the messages exchanged in the past can be decrypted. The novelties brought by quantum systems allow two parties to establish a common key that is information-theoretically secure and, therefore, can be used to achieve perfect secure communication with a one-time pad encryption.

Quantum key distribution schemes explore intrinsic properties of quantum systems, such as no-cloning [4, 5] and monogamy of entanglement [6], in order to achieve security even against an all powerful adversary who has unlimited computational power. The well known quantum key distribution scheme BB84 [2] can tolerate a reasonable amount of noise and decent rates‡ can be achieved with current technology, see for example the analyses of [9–11]. BB84-based QKD has been successfully implemented over long distances, see for example [12, 13], and even satellite-based secure quantum communication was established [14].

A successful implementation of the BB84 protocol is, however, highly dependent on a good characterisation of the underlying quantum system and the measurement devices. For example, the protocol can easily be broken if the devices are performing measurements in four dimensional systems instead of qubits, see discussions in [15, 16]. Furthermore, hacking of existent implementations that exploit experimental imperfections were presented (see e.g. [17–20]).

A good characterization of the experimental setup is a strong assumption. What is more, when quantum technologies become commercially available, we might often buy devices from a provider which is not entirely trustworthy. Fortunately, quantum properties allow us to overcome this problem: By exploring the strong correlations that arise in quantum systems, one can prove security of quantum key distribution even in the very adversarial scenario where Alice and Bob have no knowledge of the internal working of their measurement devices or the underlying quantum system that they are measuring [1, 16, 21–34]. This is the device-independent (DI) model.

---

‡ Due to finite size effects a minimal number of rounds is required in order to guarantee security. For the BB84 protocol this minimal number of rounds required is $\sim 10^4$. Moreover, a quantum bit error rate (QBER) of up to 20% can be tolerated [7, 8] for large enough number of rounds.

1.2. The device-independent scenario

The device-independent scenario models the underlying system and measurement devices as black boxes where the only relevant information is the statistics of inputs and outputs. Therefore, no assumptions on the dimension of the quantum systems or the particular measurements performed by the devices are required. This represents a significant relaxation of the assumptions present in an implementation of the BB84 protocol. However, it is important to remark which assumptions remain present in any implementation of a DI protocol.

Assumptions 1 (Device-independent model)**.** *In the device-independent model we assume:*

 (i) *Isolated labs: no information is leaked from or enters Alice's and Bob's labs, apart from the state distribution before the measurements and the public classical information dictated by the protocol.*

 (ii) *Isolated source: the preparation of states is independent of the measurements.*

(iii) *Trusted classical post-processing: all the public classical communication is performed using an authenticated channel and the local classical computations are trusted.*

(iv) *Trusted Random Number Generators: Alice and Bob possess independent and trusted random number generators.*

A bit of thought can make one conclude that completely removing any of these assumptions leads to a strategy where the key is leaked to the adversary. However, we remark that partial relaxation of these assumptions can still be considered. In Ref. [35], QKD is proved to achieve everlasting security by relaxing Assumption 1*(iii)* to a computationally secure authenticated channel, but assuming the eavesdropper to be computationally bounded during the execution of the protocol. In many device independent protocols, instead of Assumption 1*(ii)*, it is assumed that all the n systems are prepared before the measurement phase starts, so that no information other than the classical public communication is exchanged during the protocol. However, this would require quantum memory from Alice and Bob in order to store the quantum states along the protocol. In an implementation where the quantum states are generated round by round, and therefore in which no long term quantum memory is required, Assumption 1*(ii)* is necessary to avoid that the state prepared by the source leaks the raw bits generated by Alice's device in the previous round. Indeed, if the source is arbitrarily correlated with the measurement devices the state prepared can contain an additional degree of freedom that encodes the string of bits generated in the previous rounds (this strategy is detailed in [36, Appendix C]). We remark that, in experimental platforms, the preparation of states and the measurements are either performed within the same systems or optically connected ones, and therefore one needs to assume that the process of generating a quantum state is not correlated with the previously performed

measurements. This assumption is, however, often well justified based on a description of the setup.

Another assumption that is often used in security proofs is that the rounds of the experiment are *independent and identically distributed* (IID). This, in particular, implies that the measurement devices are memoryless and the state shared by Alice and Bob is the same for every round on the protocol. The IID assumption can be justified, for example, in experimental setups where Alice and Bob control to some extent the source and measurement devices, but do not have a full characterization of their working.

Assumptions 2 (IID assumption). *An IID implementation assumes:*

- *IID devices: the devices behave independently and in the same way in every round of the protocol.*
- *IID states: The state distributed is the same for every round of the protocol. In summary, the state of the n rounds can be written as $\rho_{A_1^n B_1^n E} = \rho_{ABE}^{\otimes n}$.*

The eavesdropper attacks in QKD are classified in three types: <u>Individual attacks</u>, where the eavesdropper has no memory and therefore is restricted to attack individually each round of the protocol; <u>Collective attacks:</u> where in every round the systems of Alice and Bob, as well as the measurement devices, are prepared identically but the eavesdropper is allowed to make arbitrary global operations on her quantum side information; and <u>Coherent attacks:</u> additionally to the global operations the eavesdropper can perform in her quantum side information, the states shared by Alice and Bob in each round can be arbitrarily correlated, as well as the measurement devices in the DI scenario can have memory and operate according to the results of previous rounds, *i.e.*, do not satisfy the IID assumption. The IID assumption, stated in Assumptions 2, corresponds to the scenario where the eavesdropper is restricted to collective attacks. In what follows we focus on two types of adversarial attacks: collective attacks and coherent attacks.

1.3. Device-independent quantum key distribution protocols

The first ideas of device-independent QKD arose in the E91 protocol [3], which uses a test of the CHSH inequality [37] in order to certify that Alice and Bob share a maximally entangled state. This idea of self-testing quantum devices was further explored in [15]. Indeed, device-independent quantum key distribution relies on the violation of a Bell inequality in order to certify the security of the generated key. The simplest DIQKD protocol uses the CHSH inequality for the security test:

$$\beta = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2, \tag{1}$$

where $\langle A_x B_y \rangle = p(a = b|xy) - p(a \neq b|xy)$ represents the correlation of the outputs a, b of Alice and Bob when they perform the measurement labeled by x, y respectively. The CHSH inequality can be phrased as a game [38] in which Alice and Bob receive x and y, respectively, as inputs and the winning condition is that their outputs satisfy

$a + b = x \cdot y$, with the operations $+, \cdot$ taken modulo 2. The winning probability ω of the CHSH game relates to the violation β by

$$\omega = \frac{4 + \beta}{8}. \tag{2}$$

For DIQKD based on the CHSH inequality, we consider protocols where Alice possesses a device with two possible inputs $X \in \{0, 1\}$ and Bob has a device with three possible inputs $Y \in \{0, 1, 2\}$. The inputs $X \in \{0, 1\}$ and $Y \in \{0, 1\}$ are used to test for the CHSH inequality, and the inputs $X = 0$ and $Y = 2$ are used for the other rounds, often called key generation rounds, where maximal correlation of the outputs is expected. The parameters of interest are the Bell violation β, or winning probability ω, achieved in the test rounds and the quantum bit error rate (QBER) Q of the key generation rounds. We consider that an implementation of the protocol is expected to have n rounds and a portion γn of these rounds is used for testing of the CHSH condition.

A DIQKD protocol can be divided in three phases:

- An initial phase where Alice and Bob use their respective devices to measure the quantum systems and, according to the obtained outputs, generate the n-bit strings A_1^n and B_1^n.

- A second phase where Alice and Bob publicly exchange classical information in order to perform <u>error correction</u>, to correct their respective strings generating the raw keys; and <u>parameter estimation</u>, to estimate the parameters of interest (Bell violation, β, and QBER, Q). At the end of this phase Alice and Bob are supposed to share equal n-bit strings and have an estimate of how much knowledge an eavesdropper might have about their raw key.

- In the final phase, Alice and Bob perform <u>privacy amplification</u>, where the not fully secure n-bit strings are mapped into smaller strings K_A and K_B, which represents the final keys of Alice and Bob respectively.

The specific protocols we consider for our analyses are detailed in Section 2, (see Protocol 1 and Protocol 2).

In order to define security of a DIQKD protocol, we follow Refs. [1,39] and adopt the security definition that is universally composable for standard QKD protocols [40]. Universal composability is the statement that a protocol remains secure even if it is used arbitrarily in composition with other protocols. It is important to remark that, for the device-independent case, attacks proposed in Ref. [41] show that composability is not achieved if the same devices are re-used for generation of a subsequent key. Indeed, in [41], the authors have shown that a malicious eavesdropper can program the measurement devices in such a way that information about a previously generated key may be leaked through the public communication of a subsequent run of the key generation protocol, if the devices are re-used. It is still an open problem what is the minimum set of assumptions that can lead to universal composability of DIQKD (e.g.

the attacks of Ref. [41] can be avoided if the memory of the devices are re-set after an execution of the protocol).

Let K_A and K_B denote the final key held by Alice and Bob, respectively, after they perform a DIQKD protocol. A DIQKD protocol is secure if it is correct and secret. Correctness is the statement that Alice and Bob share the same key at the end of the protocol, *i.e.*, $K_A = K_B$. Secrecy is the statement that the eavesdropper is totally ignorant about the final key.

Definition 1 (Correctness)**.** *A DIQKD protocol is ϵ_{corr}-correct if the probability that the final key of Alice, K_A, differs from the final key of Bob, K_B, is smaller than ϵ_{corr}, i.e.*

$$P(K_A \neq K_B) \leq \epsilon_{corr}. \tag{3}$$

Definition 2 (Secrecy)**.** *Let Ω denote the event of not aborting in a DIQKD protocol and $p(\Omega)$ be the probability of the event Ω. The protocol is ϵ_{sec}-secret if, for every initial state ρ_{ABE} it holds that*

$$p(\Omega) \cdot \frac{1}{2} \|\rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_E\|_1 \leq \epsilon_{sec}, \tag{4}$$

where $\tau_{K_A} = \frac{1}{|K_A|} \sum_k |k\rangle\langle k|_A$ is the maximally mixed state in the space of strings K_A, and $\|\cdot\|_1$ is the trace norm.

If a protocol is ϵ_{corr}-correct and ϵ_{sec}-secret, then it is ϵ_{DIQKD}^s-correct-and-secret for any $\epsilon_{DIQKD}^s \geq \epsilon_{corr} + \epsilon_{sec}$. See Section 4.2 for a more detailed definition of security of a DIQKD protocol.

Given an DIQKD protocol that has n rounds and generates a final correct-and-secret key of l bits, then the secret key rate is defined as

$$r = \frac{l}{n}. \tag{5}$$

Our goal is to derive the secret key rate as a function of the parameters of interest, β and Q, that Alice and Bob can estimate during the execution of the protocol.

1.4. Security proof of DIQKD

Even though the BB84 quantum key distribution scheme dates back to 1984 [2], the formal security proof in the asymptotic regime only came out more than a decade later, see e.g. [42–45]. Security in the composable paradigm in the finite regime against general coherent attacks was only formalized in 2005 [46–48]. Moreover, a finite key analysis without the IID assumption over the state preparation and with parameters compatible with current technology only came in 2012 [9, 10].

In the device-independent scenario, security against a quantum eavesdropper§ restricted to collective attacks was first proved in [16, 27]. A proof against general attacks assuming memoryless devices was presented in [28, 29]. The problem of extending the

§ A discussion on earlier security proofs that do not restrict the eavesdropper to the quantum formalism can be found in [49].

security proofs to coherent attacks in the device-independent scenario remained open for a long time. One of the main difficulties is that de Finetti techniques [47,50], used to extend security proofs against collective attacks to general coherent attacks in standard QKD, are not applicable in the DI scenario. A series of recent works [31–34] culminated in the the <u>Entropy Accumulation Theorem</u> (EAT) [1] (see [39,51] for extended versions). The EAT allows one to extend the analysis against collective attacks to the fully device-independent scenario, resulting in asymptotically tight security proofs and high rates in the finite size regime.

1.5. Experimental DIQKD

Protocols for DIQKD rely on a Bell test between two distant parties [16]. In order to certify security, this Bell test should be free of loopholes that could be exploited by an adversary. While closing the detection loophole is crucial for a DIQKD implementation, the spacelike separation required for loophole-free Bell tests can be relaxed. In a DIQKD experiment, no-communication between the devices does not have to be guaranteed by spacelike separation, since the assumption of isolated labs, Assumption 1*(i)*, is already needed to ensure that the generated key is not leaked to the eavesdropper at any point in time. We are thus interested in considering Bell violations between distant - albeit not necessarily spacelike separated - setups in which the detection-loophole is closed [52–59]. The recent performance of fully loophole-free Bell tests [52–55] mark technological progress towards Bell tests without detection loophole over increasingly distant setups, as needed for practically useful DIQKD.

Despite the experimental progress, a device-independent quantum key distribution protocol has not yet been performed. The reason for this is that a Bell violation alone is not enough to guarantee security in a DIQKD protocol. One also needs to account for the amount of information leaked during the error correction, when Alice and Bob correct their string of bits in order to achieve a perfectly correlated raw key. The amount of information required for error correction is determined by the QBER. With a finite QBER, as in practical systems, a large Bell violation is needed to achieve a positive key rate. Moreover, a high minimal number of rounds is required for security due to finite-size effects. The large number of necessary rounds requires a significantly high entangling rate. Altogether, DIQKD demands a low QBER, high Bell violation and high entangling rates. Even though some systems satisfy parts of these requirements, e.g. a high Bell violation [52,55,58,59] or high entangling rate [53,54,56,57], so far there are no systems that combine all requirements. In section 2.3 we describe the potential platforms for an experimental implementation of DIQKD in detail.

2. Results

We now present our results. In Section 2.1, we establish the key rates for DIQKD protocols based on the CHSH inequality, both for coherent and collective attacks in

the finite size regime. As a benchmark, in Section 2.2, we compare the key rates that can be achieved in the finite regime for the two adversarial scenarios (collective and coherent attacks) using an implementation with depolarizing noise. In Section 2.3, we discuss the state of the art of experimental implementations. We estimate the parameters of interest for previously performed Bell experiments and situate them in the security proofs. Additionally, focusing on Nitrogen-vacancy based systems we indicate experimental improvements that can lead to an implementation of DIQKD in the near future. Throughout this manuscript we use Log_{10} to denote logarithm to base 10 and log to denote logarithm to base 2.

2.1. Key Rates

In the following, we derive the key rates in the finite size regime for DIQKD protocols where the CHSH inequality is used for certifying security. For coherent attacks we sharpen the results recently derived in [1]. For collective attacks we perform the analysis by employing two techniques: the fintie version of the asymptotic equipartition property [60] and the additivity of the 2-Rényi entropy.

2.1.1. Key rates for coherent attacks.
In order to analyze the key rates against general coherent attacks we use the recently developed entropy accumulation theorem (EAT) [1, 39, 51] and consider the following protocol.

Protocol 1 DIQKD Protocol for coherent attacks [39]

1: **for** For every block $j \in [m]$ **do**
2:     Set $i = 0$ and $C_j = \bot$.
3:     **while** $i \leq s_{max}$ **do**
4:         Set $i = i + 1$.
5:         Alice and Bob choose a random bit $T_i \in \{0, 1\}$ such that $P(T_i = 1) = \gamma$.
6:         **if** $T_i = 0$ **then** Alice and Bob choose inputs $(X_i, Y_i) = (0, 2)$.
7:         **else** they choose $X_i, Y_i \in \{0, 1\}$ (the observables for the CHSH test).
8:         **end if**
9:         Alice and Bob use their devices with the respective inputs and record their outputs, A_i and B_i respectively.
10:         If $T_i = 1$ they set $i = s_{max} + 1$.
11:     **end while**
12: **end for**
13: **Error Correction:** Alice and Bob apply the error correction protocol EC, communicating script O_{EC} in the process. If EC aborts they abort the protocol, else they obtain raw keys $\tilde{A}_1^n$ and $\tilde{B}_1^n$.
14: **Parameter estimation:** Using B_1^n and $\tilde{B}_1^n$, Bob sets

$$C_i = \begin{cases} 1, & \text{if } T_i = 1 \text{ and } A_i \oplus B_i = X_i \cdot Y_i \\ 0, & \text{if } T_i = 1 \text{ and } A_i \oplus B_i \neq X_i \cdot Y_i \\ \bot, & \text{if } T_i = 0 \end{cases} \tag{6}$$

    He aborts if

$$\sum_j C_j < m \times (\omega_{exp} - \delta_{est}) \left(1 - (1 - \gamma)^{s_{\max}}\right),$$

    i.e., if they do not achieve the expected violation.
15: **Privacy Amplification:** Alice and Bob apply the privacy amplification protocol PA and obtain the final keys K_A and K_B of length l.

In Protocol 1, the total number of rounds is not fixed in advance, however for a number of blocks m large enough the number of rounds will correspond, with high probability, to the expected value n. This is a technicality introduced in Ref. [1, 39] in order to obtain better rates in the finite regime. A more detailed explanation can be found in [39, Appendix B]. Improvements on the second order term of the entropy accumulation theorem, that do not rely on the introduction of blocks, were recently obtained in [61]. Following the techniques of [1, 39], we derive Theorem 1.

Theorem 1 (Key rates for coherent attacks). *Either Protocol 1 abort with probability higher than $1 - (\epsilon_{EA} + \epsilon_{EC})$, or it generates a $(2\epsilon_{EC} + \epsilon_{PA} + \epsilon_s)$-correct-and-secret key of length*
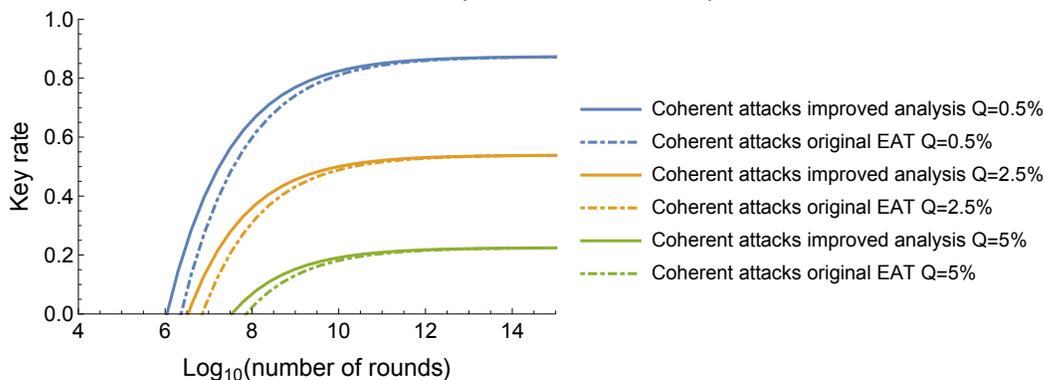
$$l \geq \frac{n}{\bar{s}}\eta_{opt} - \frac{n}{\bar{s}}h(\omega_{exp} - \delta_{est}) - \sqrt{\frac{n}{\bar{s}}}\nu_1 - leak_{EC} \tag{7}$$

$$- 3 \log \left(1 - \sqrt{1 - \left(\frac{\epsilon_s}{4(\epsilon_{EA} + \epsilon_{EC})} \right)^2} \right) + 2 \log \left(\frac{1}{2\epsilon_{PA}} \right),$$

where $leak_{EC}$ is the leakage due to error correction step and the functions $\bar{s}$, η_{opt}, ν_1 and ν_2 are specified in Table 1.

Theorem 1 sharpens the original analysis [1,39] and has slightly improved key rates in the finite regime. This results in a reduction of the minimum number of rounds (signals) required for positive rates by about a factor of two, as illustrated in Figure 1. A detailed derivation of Theorem 1 can be found in Appendix B.3.

Figure 1. Key rate r vs logarithm of the number of rounds n. Comparison of the improvements in the key rate, for an implementation where the maximally entangled is subjected to depolarizing noise and therefore $\beta = 2\sqrt{2}(1 - 2Q)$, for QBER $Q = \{0.5\%, 2.5\%, 5\%\}$. The dashed curves correspond to the key rates derived in the original analysis [1,39], the solid lines represent the key rates derived in Theorem 1. Similarly to [1], we take $\epsilon_{DIQKD}^c = 10^{-2}$ and $\epsilon_{DIQKD}^s = 10^{-5}$.

$s_{\max} = \left\lceil \frac{1}{\gamma} \right\rceil$
$\bar{s} = \frac{1 - (1-\gamma)^{\left\lceil \frac{1}{\gamma} \right\rceil}}{\gamma}$
$\eta_{opt} = \max\limits_{\frac{3}{4} < \frac{p_t(1)}{1-(1-\gamma)^{s_{max}}} < \frac{2+\sqrt{2}}{4}} \left[F_{\min}(\vec{p}, \vec{p}_t) - \frac{1}{\sqrt{m}} \nu_2 \right]$
$F_{\min}(\vec{p}, \vec{p}_t) = \frac{d}{dp(1)} g(\vec{p})\big|_{\vec{p}_t} \cdot p(1) + \left(g(\vec{p}_t) - \frac{d}{dp(1)} g(\vec{p})\big|_{\vec{p}_t} \cdot p_t(1) \right)$
$g(\vec{p}) = s \left[1 - h \left(\frac{1}{2} + \frac{1}{2} \sqrt{16 \frac{p(1)}{1-(1-\gamma)^{s_{max}}} \left(\frac{p(1)}{1-(1-\gamma)^{s_{max}}} - 1 \right) + 3} \right) \right]$
$\nu_2 = 2 \left(\log \left(1 + 2 \cdot 2^{s_{\max}} 3 \right) + \left\lceil \frac{d}{dp(1)} g(\vec{p})\big|_{\vec{p}_t} \right\rceil \right) \sqrt{1 - 2 \log \epsilon_s}$
$\nu_1 = 2 \left(\log 7 + \left\lceil \frac{|h'(\omega_{exp} + \delta_{est})|}{1-(1-\gamma)^{s_{\max}}} \right\rceil \right) \sqrt{1 - 2 \log \epsilon_s}$

Table 1. Explicit form of the terms that appear in Theorem 1. For a detailed derivation see Appendix B.3.

2.1.2. Key rates for collective attacks For collective attacks, we derive the finite key rates by employing two techniques: the finite version of the asymptotic equipartition property and the additivity property of the conditional α-Rényi entropies. To deal with

collective attacks we can use a simplified version of Protocol 1, where the number of rounds is fixed.

Protocol 2 DIQKD protocol for collective attacks

1: **for** $i = 1$ to n **do**
2:     Alice and Bob choose a random bit $T_i \in \{0, 1\}$ such that $P(T_i = 1) = \gamma$.
3:     **if** $T_i = 0$ **then** Alice and Bob choose inputs $(X_i, Y_i) = (0, 2)$.
4:     **else** they choose $X_i, Y_i \in \{0, 1\}$ (the observables for the CHSH test).
5:     **end if**
6:     Alice and Bob use their devices with the respective inputs and record the outputs, A_i and B_i respectively.
7: **end for**
8: **Error correction:** Alice and Bob apply the error correction protocol EC, communicating O_{EC} in the process. If EC aborts they abort the protocol, else they obtain raw keys $\tilde{A}_1^n$ and $\tilde{B}_1^n$.
9: **Parameter estimation:** Using B_1^n and $\tilde{B}_1^n$, Bob sets for the first test rounds

$$C_i = \begin{cases} 1, & \text{if } A_i \oplus B_i = X_i \cdot Y_i \\ 0, & \text{if } A_i \oplus B_i \neq X_i \cdot Y_i \end{cases} \tag{8}$$

    For the remaining rounds he sets $C_i = \perp$.
    He aborts if

$$\sum_j C_j < \gamma n \times (\omega_{exp} - \delta_{est}),$$

    i.e., if they do not achieve the expected violation.
10: **Privacy Amplification:** Alice and Bob apply the privacy amplification protocol PA and obtain the final keys K_A and K_B of length l.

In the following theorem we state the length of a secure key that can be derived using the asymptotic equipartition property, which is formally stated in Theorem 7.

Theorem 2. *Either Protocol 2 aborts with probability higher than $1 - (\epsilon_{con} + \epsilon_{EC})$, or it generates a $(2\epsilon_{EC} + \epsilon_s + \epsilon_{PA})$-correct-and-secret key of length:*

$$\begin{aligned}
l \geq &\ n[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16(\omega_{exp} - \delta_{est} - \delta_{con})((\omega_{exp} - \delta_{est} - \delta_{con}) - 1) + 3}\right) \\
&- (1 - \gamma)h(Q) - \gamma h(\omega_{exp})] \\
&- \sqrt{n}\left(4\log\left(2\sqrt{2} + 1\right)\left(\sqrt{\log\frac{2}{\epsilon_s^2}} + \sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right)\right) \\
&- \log\left(\frac{8}{\epsilon'^2_{EC}} + \frac{2}{2 - \epsilon'_{EC}}\right) - \log\left(\frac{1}{\epsilon_{EC}}\right) - 2\log\left(\frac{1}{2\epsilon_{PA}}\right)
\end{aligned} \tag{9}$$

A detailed derivation of Theorem 2 can be found in Appendix B.1.

Using a different technique, namely bounding the key rate by the conditional collision entropy, we derive the following result.

Theorem 3. *Either Protocol 2 aborts with probability higher than $1 - (\epsilon_{con} + \epsilon_{EC})$, or it generates a $(2\epsilon_{EC} + \epsilon_{PA})$-correct-and-secret key of length:*

$$
\begin{aligned}
l \geq n\Big[&-\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{16(\omega_{exp} - \delta_{est} - \delta_{con})(1 - (\omega_{exp} - \delta_{est} - \delta_{con}))} - 2\right) \\
&- (1 - \gamma)h(Q) - \gamma h(\omega_{exp})\Big] \\
&- \sqrt{n}\left(4\log\left(2\sqrt{2} + 1\right)\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right) \\
&- \log\left(\frac{8}{\epsilon'^2_{EC}} + \frac{2}{2 - \epsilon'_{EC}}\right) - \log\left(\frac{1}{\epsilon_{EC}}\right) - 2\log\left(\frac{1}{2\epsilon_{PA}}\right)
\end{aligned}
\tag{10}
$$

An important step in the proof of Theorem 3 is to derive a lower bound on the collision entropy as a function of the CHSH violation β. A tight lower bound is proved in Theorem 9. The detailed proof of Theorem 3 is presented in Appendix B.2.

The rates presented in Theorem 2 are asymptotically tight, while Theorem 3 achieves strictly smaller asymptotic rates. However, one can note that in Theorem 3 the term proportional to $\sqrt{n}$ has a smaller pre-factor. This can potentially lead to an advantage for the minimum number of rounds required for security. For Protocol 2, an advantage can only be observed for very low noise regime, as illustrated in Figure 2. We remark, however, that for protocols based on other Bell inequalities the techniques used for deriving Theorem 3 can present significant advantage for the collective attack analysis. This is further discussed in Section 4.3.2.

Figure 2. Key rates vs logarithm of the number of rounds n for Protocol 2 (collective attacks). The blue curve represent the key rate using Theorem 2 and the yellow curve shows the key rate using Theorem 3. It is considered an implementation with depolarizing noise and QBER $Q = 0.01\%$. The inset graph shows a zoom in the region of low number of rounds. Similarly to [1], we take $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.
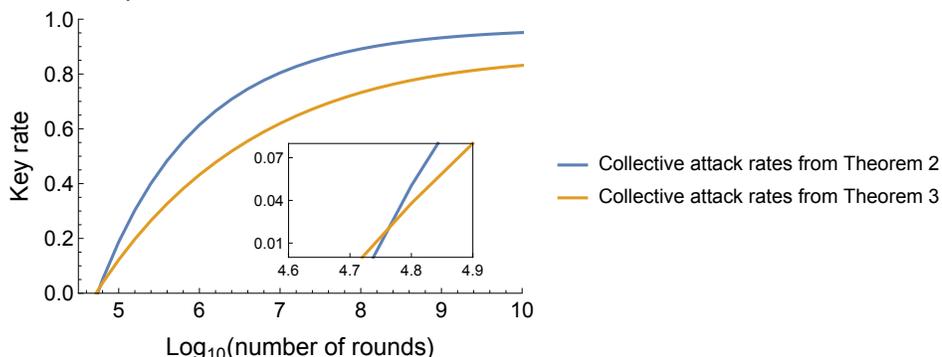
The following table lists the parameters of the DIQKD protocols in consideration.

n	expected number of rounds
l	final key length
γ	fraction of test rounds
Q	quantum bit error rate
β	CHSH violation
ω_{exp}	expected winning probability on the CHSH game in an honest implementation
δ_{est}	width of the statistical interval for the Bell test
δ_{con}	confidence interval for the Bell test in Protocol 2
ϵ_s	smoothing parameter
$\epsilon_{EC}, \epsilon'_{EC}$	error probabilities of the error correction protocol
ϵ_{EA}	error probability of Bell violation estimation in Protocol 1
ϵ_{con}	error probability of Bell violation estimation in Protocol 2
ϵ_{PA}	error probability of the privacy amplification protocol
leak_{EC}	leakage in the error correction protocol

Table 2. Parameters of the considered DIQKD protocols, Protocol 1 and Protocol 2.

2.2. Comparison of key rates for depolarizing noise model

We now compare the key rates achieved in the finite regime under the assumption of collective attacks (IID scenario) and against general coherent attacks (fully DI scenario). As a benchmark, we focus on an honest implementation where the maximally entangled state is prepared and subjected to depolarizing noise‖:

$$\rho = (1 - \nu)\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + \nu\frac{I}{4}. \tag{11}$$

In this case, the parameters of interest – the value of the CHSH inequality β and the QBER Q – relate to the noise parameter ν by

$$Q = \frac{\nu}{2} \quad \text{and} \quad \beta = 2\sqrt{2}(1 - \nu) \;\to\; \beta = 2\sqrt{2}(1 - 2Q). \tag{12}$$

In Figure 3 we compare the key rates achievable under the IID assumption, given by Theorem 1, and in the fully DI scenario, Theorem 2, for an honest implementation with depolarizing noise.

‖ This noise model can also be seen as the case where each individual qubit suffers a depolarization with parameter ν', where $\nu = 2\nu' - \nu'^2$.

Figure 3. Key rates vs logarithm of the number of rounds for collective attacks (dashed lines) and coherent attacks (solid lines). The different curves represent different values of QBER $Q = (0.5\%, 2.5\%, 5\%)$ considering an implementation where the maximally entangled state is subjected to depolarizing noise (see relation (12)). The security parameters are taken as $\epsilon_{DIQKD}^c = 10^{-2}$ and $\epsilon_{DIQKD}^s = 10^{-5}$.
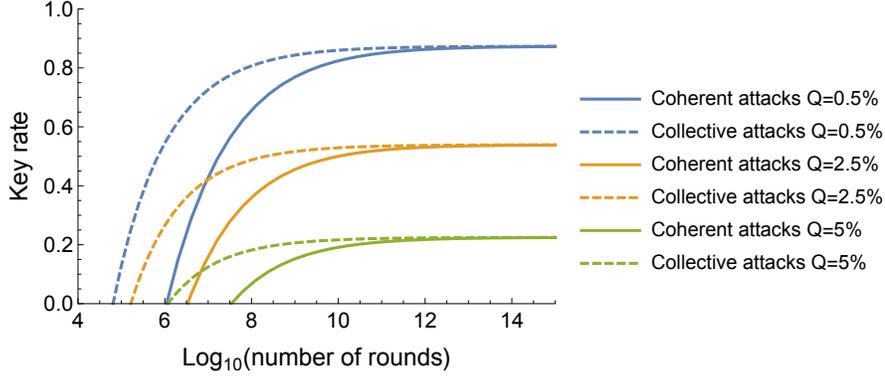

Figure 3 shows that the key rates approach the same asymptotic values, however the minimum number of rounds required to guarantee security is significantly higher for general coherent attacks. Indeed, by adding the assumption that the eavesdropper is restricted to collective attacks, the minimum number of signals required to have a positive key rate drops by about two orders of magnitude. However, even for collective attacks, this minimum number of required rounds is considerably large given the current entanglement generation rates. This is one of the big challenges to be overcome for a DIQKD implementation. In the next Section we are going to discuss the state of the art of experiments, and situate the current achievable parameters (Bell violation, QBER and entanglement generation rate) in the security proofs.

2.3. The state-of-the-art experimental DIQKD

In the following, we discuss experimental platforms in which DIQKD may be implemented. We analyse Bell violations and expected QBER achieved in previous Bell tests with distant setups and situate these parameters in the context of the key rates derived in Theorems 1 and 2. A summary of the findings is presented in Table 4 and Figures 5 and 6.

In experimental setups, distant entanglement is typically generated using photons to establish the connection. We distinguish two approaches based on the role of the photonic qubits: *(i) All-photonic schemes:* Approaches in which the entangled state is encoded in the photonic state directly. In this case, measurements of the photonic states on two remote setups enable to infer their entanglement. *(ii) Heralded schemes:* In this case, the entangled state is typically created in a long-lived system and the photons are used as a means of establishing the entanglement between two distant systems.

In this section we provide a discussion of the parameters in each of these schemes and the related challenges towards an implementation of DIQKD. We provide a more detailed discussion of one of the systems, namely nitrogen-vacancy (NV) centres in

diamonds, and describe improvements in experimental parameters that can lead to a DIQKD implementation in the near future.

2.3.1. DIQKD with all-photonic entanglement. Since in all-photonic schemes the entangled state is directly encoded on the photonic state, photon losses limit the entangled state detection efficiency. Closing the detection loophole in a Bell test thus requires very efficient entangled-photon sources and photon detectors. Recent technological advances enabled all-photonic Bell tests that close the detection-loophole [56, 57], later combined with spacelike separation in loophole-free Bell tests [53, 54].

In photonic systems the detection efficiency also impacts the entangled state fidelity. We thus may expect that Bell violations are low in photonic systems. To avoid having to deal with undetected events, photonic Bell tests typically employ the CH-Eberhard inequality [62, 63]. The CHSH and CH-Eberhard inequalities are equivalent¶, such that we can estimate the CHSH violation achieved in photonic experiments. Table 4 presents the corresponding value for the CHSH inequality achieved in the experiments of Refs. [53,54,56,57]. One can note that the violations achieved are indeed low, ranging from 2.00004 to 2.02. Combined with a finite QBER ($> 2\%$), this poses a significant challenge for the implementation of a DIQKD protocol in photonic systems.

However, if these systems would enter the regime of positive key rates, the entanglement generation rate can be very high ($\sim 10^5$ Hz), such that they could easily reach the asymptotic key rate values.

Recently, heralded schemes for all-photonic systems were proposed in [64]. In this case, the entangled state is created between photons and, also, this entanglement is heralded by the interference of other photons. The proposed scheme uses a combination of spontaneous parametric down conversion sources and single-photon sources in order to achieve a setup where a heralding process could overcome transmission photon losses. This setup is a promising proposal to bring the parameters of all-photonic systems to the region of positive asymptotic key rates (see Figure 5 and 6). However single-photon sources still lack the required performance for an implementation of these schemes.

2.3.2. DIQDK with heralded entanglement. Due to the nature of heralded entangling schemes, photon losses do not influence the entangled state detection efficiency or fidelity. Heralded schemes have been used to entangle distant atomic ensembles [65,66], trapped ions [67], atoms [68], NV centres [69], quantum dots [70], and mechanical oscillators [71]. So far, entangled state fidelities sufficiently high to violate Bell's inequalities have only been reached with trapped ions [58,59], atoms [55,68], and with NV centres [52,72]. The Bell violations observed in Refs. [52, 55, 58, 59, 72] are in the range $\beta = 2.22$ to $\beta = 2.41$, with a lower bound on the QBER, estimated from detection efficiencies alone, around 0.04 (see Table 4 for a full overview). Apart from the results reported in [59], these parameters are not in the region of positive key rate (see Figures

¶ One can see that by replacing non-detected events by the deterministic classical strategy "output 1" in a test of the CHSH inequality.

5 and 6). However, all of them are in the proximity of this region, such that setup improvements may enable to reach it.

The challenge for these implementations is however their low entangling rate, induced by photon losses. Current rates range from $(\text{minutes})^{-1}$ [55, 58, 59, 68] to $(\text{hours})^{-1}$ [52, 72]. A significant speed-up in the entanglement generation rate is thus needed in order to achieve the minimum number of rounds required for DIQKD. Higher entangling rates in heralded schemes were recently achieved with trapped ions [73] and NV centres [74, 75], although with lower state fidelities, and no Bell violations are reported. Even though in Ref. [75] the state fidelity is just high enough to be able to violate Bell inequalities, the expected Bell violation would be low. Enhancement in entangling rates, e.g. with optical cavities to improve light-matter coupling efficiency [76] is therefore crucial to achieving an implementation of DIQKD with heralded schemes.

2.3.3. Nitrogen-vacancy centre-based networks. In this section, we focus on heralded entanglement generation between nitrogen-vacancy centres in diamond for DIQKD. Nitrogen-vacancy (NV) centres are defect centres in the diamond lattice. They contain an electronic spin with good coherence properties and spin-selective optical transitions that can be used for intialization, readout and entanglement generation [69, 77]. Next to the electronic spin, nearby weakly coupled nuclear spins can serve as long-lived memories [78, 79]. These properties make the NV centre a promising quantum network node.

Entanglement between distant NV centres can be generated using an heralded scheme. Typically, local entanglement is first generated between the NV electronic spin and a photon mode. And subsequently, entanglement between distant NV centres is achieved through entanglement swapping by interfering the two photon modes from distant setups [80]. As discussed above for heralded protocols, photon attenuation does not influence the fidelity of the generated entangled state or the detection efficiency. The detection of the spin states has near-unit efficiency [81].

DIQKD parameters. In a loophole-free Bell test with NV centres [52, 72], a CHSH violation $\beta = 2.38 \pm 0.14$ was observed between systems separated by 1.3 kilometers. Taking into account the entangled state fidelity and detection efficiency, we estimate that the corresponding QBER would be $Q = 0.06 \pm 0.03$. The Bell violation achieved in [52, 72] is considerably high, especially if compared to loophole-free Bell test experiments in photonic systems [53, 54]. However, these parameters are not good enough to generate a secure key. Indeed, using Theorems 1 and 2, one concludes that it is not possible to achieve positive key rate with these parameters (see Figures 5 and 6).

In the following, we suggest two near-term experimental improvements to enhance these parameters.

Firstly, the frequency stability of the laser used to excite NV centres during the entanglement protocols can be increased using an external cavity. The instability of the

laser can influence the indistinguishability of photons emitted by the distant NV centres. The indistinguishability is crucial for photon interference, which can be quantified by the visibility of the two-photon quantum interference (TPQI). We expect that compared to previous implementation [52], the improved laser frequency stability can lead to an improvement in TPQI visibility from 0.88 to 0.90.

Secondly, both the CHSH violation β and the QBER Q are impacted by the NV electronic spin state readout. The readout can be performed using resonant excitation of a spin-selective optical transition [81]. Improvements to the detection efficiency can be obtained by storing the spin state in the nearby nitrogen spin state, and performing repeated readout [82]. We estimate that the repeated readout can lead to an average readout fidelity of ≈ 0.985, compared to an initial 0.97 [83] [+].

Other improvements can be envisioned, such as enhancement of the detection efficiency by improving the photon collection efficiency through the use of parabolic reflectors [84] or optical cavities [85]. In the following discussion we limit ourselves to the two advances listed above and summarized in Table 3.

DIQKD parameters	Ref. [52, 72]		Expected	
setup	A	B	A	B
average readout fidelity	0.974	0.969	0.985	0.985
TPQI visibility	0.88		0.90	
β	2.38 ± 0.14		2.47	
Q	0.06 ± 0.03		0.051	

Table 3. The CHSH violation β and QBER Q in NV centre-based implementations are strongly dependent on the TPQI visibility and the readout fidelity. The resulting values are shown for parameters achieved in a loophole-free Bell test, and for expected values from several readily-implementable improvements.

Taking into account these improvements, the expected DIQKD parameters are $\beta \approx 2.47$ and $Q \approx 0.051$. In Figure 4 we illustrate the rates achievable for these parameters against general coherent attacks and under the assumption that the eavesdropper is restricted to collective attacks. We see that the required minimum number of rounds is of order 10^8 for general attacks, and about 5×10^6 for collective attacks.

[+] We note that this readout method increases the readout duration, which compromises spacelike setup-separation. However, security in a DIQKD implementation does not require spacelike separation since it is superfluous with the assumption of isolated labs in place (see Assumptions 1). Therefore, an increased readout time does not present a problem for security.
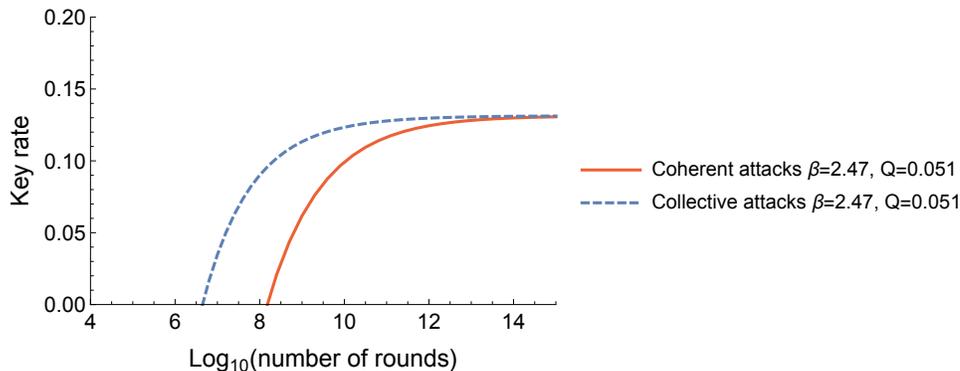
Figure 4. Key rates vs logarithm of the number of rounds n for parameters that are readily-implementable in NV centres setups (CHSH violation $\beta = 2.47$ and QBER $Q = 0.051$). The red line shows the key rates obtained against general coherent attacks, and the blue dashed line shows the key rates under the assumption of collective attacks. The security parameters are chosen to be $\epsilon_{DIQKD}^c = 10^{-2}$ and $\epsilon_{DIQKD}^s = 10^{-5}$.

Entangling rate. Although the improved parameters lead to a positive key rate, this does not mean that DIQKD with NV centres is readily achievable. The system faces another challenge: the probabilistic nature of the heralded entanglement scheme limits the entanglement generation rate.

In the heralded entanglement generation protocol used in [52,69] the photonic qubit is time-bin encoded and entanglement is heralded with the detection of a photon in each of two time-bins [80]. Since two photons have to be detected, the rate of the protocol is proportional to the square of the photon losses. For the spacelike separated setups in [52] the total emission and detection efficiency per photon is $\approx 10^{-4}$, leading to a total success probability of $\approx 10^{-8}$. Since the repetition rate, limited by the spin-state reset time, is of the order of $\approx \mu$s, generating a raw key of length 10^6 bits would take $\approx 10^3$ days. It is clear that a speed-up of entanglement generation rate is required to use NV centres in a DIQKD protocol. We describe two approaches toward this.

Firstly, this could be achieved by adapting the entanglement generation protocol. A linear dependency of the rate on photon losses can be achieved by employing an extreme-photon-loss (EPL) protocol [86] or single-photon (SP) protocol [87]. Demonstrated implementations of these protocols with NV centres indeed provide a speed-up in entanglement rate of three orders of magnitude [74,75]. However, these implementations do not yet provide the entangled state fidelities leading to Bell violations that allow for DIQKD (the entangled state fidelities are $F_{EPL} = 0.65 \pm 0.03$ and $F_{SP} = 0.81 \pm 0.02$, leading to no Bell violation for the EPL protocol and a small violation $\beta_{SP} = 2.1$ for the single photon protocol). Better parameters may be achieved with improvements of the robustness of the nuclear-spin memories [79] and with an improved photon detection versus dark-count rate [87].
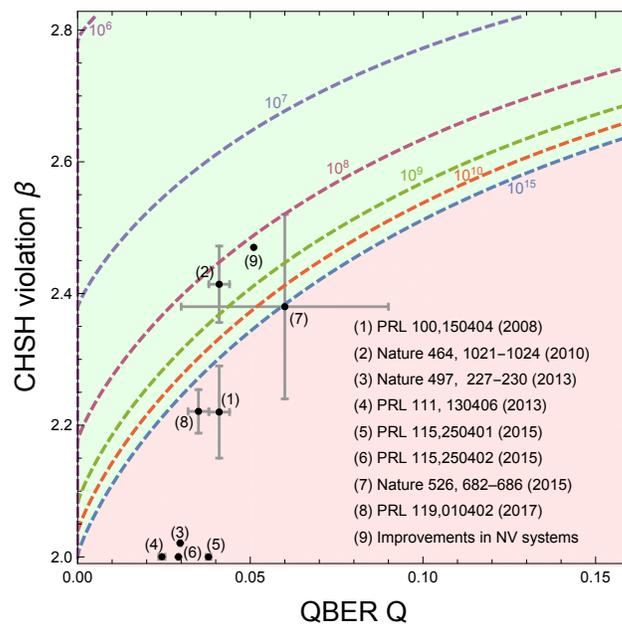
Secondly, an increase in the entanglement rate can be achieved by a reduction of the photon losses per round. These losses consist of three parts: a low coherent-photon

emission probability, a non-unit collection efficiency and fiber attenuation. The photon attenuation during transmission over fibers is ≈ 8 dB for the NV emission wavelength (637 nm). To maintain high entangling rates for distant setups, this should be reduced. This can be achieved by frequency downconversion of the photons at a wavelength of 637 nm emitted by the NV centres to telecom frequencies [88,89]. The emission probability of coherent photons, $\approx 3\%$, and subsequent collection efficiency ($\approx 10\%$, [69]) together limit the best achievable entangling rates. They can be addressed simultaneously by embedding the NV centre in an optical cavity to enhance coherent-photon emission and the collection efficiency [85]. A promising approach employs NV centres in diamond membranes in Fabry-Perot microcavities [90–92]. In such a design NV centres remain far away from the optical interface, retaining bulk-like optical coherence properties. These cavities are expected to provide three orders of magnitude enhancement in entangling rate for a two-click protocol [91]. Together with the improved DIQKD parameters described above, this makes a demonstration of DIQKD with NV centres experimentally feasible.
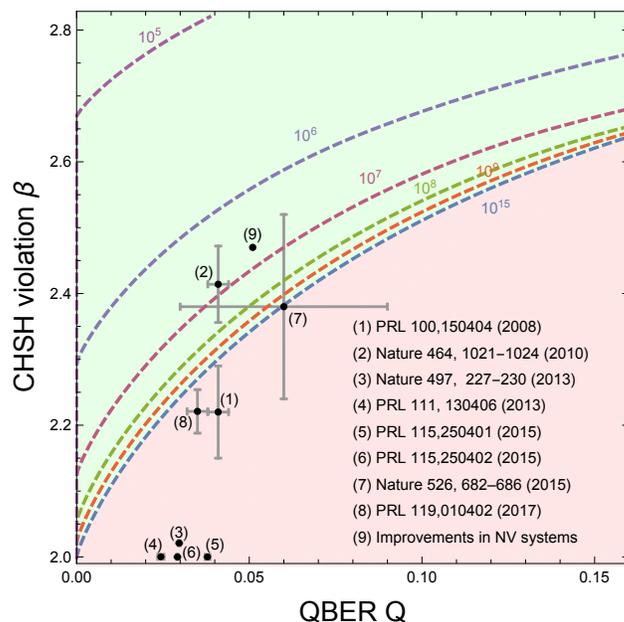
	β	Q
(1) Matsukevich et al., PRL 100, 150404 (2008) [58]	2.22 ± 0.07	0.041 ± 0.003
(2) Pironio et al., Nature 464, 1021-1024 (2010) [59]	2.414 ± 0.058	0.041 ± 0.003
(3) Giustina et al., Nature 497, 227-230 (2013) [56]	2.02096 ± 0.00032	0.0297 ± 0.0003
(4) Christensen et al., PRL 111, 130406 (2013) [57]	2.00022 ± 0.00003	0.0244 ± 0.0009
(5) Giustina et al., PRL 115, 250401 (2015) [53]	2.000030 ± 0.000002	0.0379 ± 0.0002
(6) Shalm et al., PRL 115, 250402 (2015) [54]	2.00004 ± 0.00001	0.0292 ± 0.0002
(7) Hensen et al., Nature 526 682-686 (2015) [52]	2.38 ± 0.14	0.06 ± 0.03
(8) Rosenfeld et al., PRL 119, 010402 (2017) [55]	2.221 ± 0.033	0.035 ± 0.003
(9) Expected improvements in NV systems	2.47	0.051

Table 4. Summary of the estimated parameters of interest for DIQKD. (1,2) are Bell tests with trapped ions, (3-5) are all-photonic experiments, (7) uses NV centres and (8) trapped atoms. (9) reports on near-term achievable parameters with NV centers as described in Section 2.3.3. In all experiments the detection loophole is closed; (5-8) additionally close the locality loophole. The CHSH violations for neutral atoms (8), trapped ions (1,2) and NV centres (7) are as reported in the corresponding experiments. For (3), (4) and (5), in which the value of the CH-Eberhard inequality J is reported, we make use of the relation $\beta = 4J + 2$ between the CHSH value and the CH-Eberhard value. This relation is found if one attributes "output 1" to undetected events in a CHSH inequality test. For (6) the CHSH violation was estimated directly from the reported data. For the estimation of the QBER (Q), in (1),(2) and (8) we assume perfect classical correlation in the generated state and find a lower bound for the QBER from reported detection efficiencies (0.979 ± 0.002 [93] for (1) and (2), and 0.982 ± 0.002 [94] for (8)). For NV centres (7), we additionally account for imperfections in the entangled state based on the reported density matrix. For all-photonic systems (3-6), the QBER is estimated by taking into account the detection efficiency and using the reported estimated state and the measurements performed by Alice, optimizing over measurements for Bob.

Figure 5. Region of positive key rates for <u>coherent attacks</u>: The red area is the region of values of QBER (Q) and CHSH violation (β) for which a positive key rate cannot be reached with any number of rounds. In the green area, the dashed curves represents the minimum number of rounds required to get positive key rate. For parameters above each curve, a key rate can be extracted if the number of rounds is higher than specified in the curve. The points show the Bell violation and estimated QBER achieved by previous experiments (see Table 4). They, however, do not reflect the corresponding entanglement generation rates. Similarly to [1], we take $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.

(1) PRL 100,150404 (2008)
(2) Nature 464, 1021–1024 (2010)
(3) Nature 497, 227–230 (2013)
(4) PRL 111, 130406 (2013)
(5) PRL 115,250401 (2015)
(6) PRL 115,250402 (2015)
(7) Nature 526, 682–686 (2015)
(8) PRL 119,010402 (2017)
(9) Improvements in NV systems

Figure 6. Region of positive key rates for <u>collective attacks</u>: The red area is the region of values of QBER (Q) and CHSH violation (β) for which a positive key rate cannot be reached with any number of rounds. In the green area, the dashed curves represents the minimum number of rounds required to get positive key rate. For parameters above each curve, a key rate can be extracted if the number of rounds is higher than specified in the curve. The points show the Bell violation and estimated QBER achieved by previous experiments (see Table 4). They, however, do not reflect the corresponding entanglement generation rates. Similarly to [1], we take $\epsilon_{DIQKD}^{c} = 10^{-2}$ and $\epsilon_{DIQKD}^{s} = 10^{-5}$.

3. Discussion

Detection-loophole-free Bell tests between separated setups mark an important step towards the implementation of DIQKD. Progress towards extending Bell experiments to larger distances were also achieved, in particular by the Bell tests additionally closing the locality loophole. However a DIQKD protocol has not yet been implemented.

In order to shed light on the experimental performance needed for DIQKD, we have derived the key rates in the finite size regime as a function of the experimental parameters: CHSH violation β and QBER Q. For comparison of the key rates obtained in the finite regime for coherent and collective attacks, we have used as a benchmark an implementation where the maximally entangled state is subjected to depolarizing noise. Although the asymptotic key rates against collective attacks and general coherent attacks coincide, it is known that this is not the case in the finite regime. We find that, with the currently available tools, security against coherent attacks requires a minimum number of rounds about two orders of magnitude higher than what is necessary for security against collective attacks for realistic near-term parameters.

Here, we have focused on DIQKD protocols that use the CHSH inequality. So

far the CHSH inequality is the one which leads to the best performance for a DIQKD protocol. The challenge in using other Bell inequalities is that, up to date, only non-tight lower bounds on the secure key rates can be derived. Therefore, it is still an open question whether any other Bell inequality can outperform the CHSH, either in terms of maximum tolerable QBER, higher rates or lower minimum number of rounds required.

Towards exploring the potential of different experimental platforms to implement DIQKD, we have analyzed the Bell violation and expected QBER of previously performed Bell tests and situated these parameters in the context of the derived key rates. Figures 5 and 6 summarize this analysis.

For photonic systems, a DIQKD implementation is currently barred by the very low CHSH violation. To overcome this, a strong reduction of photon losses is required.

Detection-loophole free Bell tests based on heralded entanglement schemes approach the allowed region, with the Bell test of Ref. [59], performed with trapped ions separated by 1 meter, even exhibiting parameters in the allowed region. These heralded schemes however suffer from low entangling rates resulting from photon losses. An increase in the entangling rates is expected to be achieved by improving collection efficiencies, e.g. by employing optical cavities. Moreover, with frequency downconversion these results can be extended to long ($\gg 1$ km) distances. We illustrate that with near-term experimental improvements for NV centres, in combination with optical cavities for enhancing entangling rate, described in Section 2.3.3, a demonstration of DIQKD is achievable.

4. Methods

We now present the theoretical tools that allows us to derive the key rates for the device-independent quantum key distribution protocols, Protocol 1 and Protocol 2. We start by defining some quantities that are going to play an important role in the security proof and state in more details the security definition for device-independent quantum key distribution.

4.1. Notation and definitions

In cryptographic tasks, we are often interested in estimating what is the maximum probability with which an adversary can guess the value of a classical variable A^*. This is defined as the guessing probability p_{guess}. In the general case where the adversary might have access to a quantum side information E, and therefore the state of interest is a *cq*-state (classical-quantum state) ρ_{AE}, the guessing probability is defined as:

$$p_{\text{guess}}(A|E)_\rho = \sup_{\{M_E^a\}} \sum_a p(A = a)_\rho \text{Tr}\left(M_E^a \rho_{E|A=a}\right), \tag{13}$$

* In QKD, for example, the classical variable is the string of bits that Alice holds after measuring her quantum systems.

where the supremum is taken over all POVMs $\{M_E^a\}$ that can be performed on the system E. The min-entropy of the classical variable A conditioned on the quantum side information E is then given by [95]

$$H_{\min}(A|E)_\rho = -\log p_{guess}(A|E)_\rho. \tag{14}$$

A smoothed version of the min-entropy can also be defined.

Definition 3 (Smooth min-entropy). *For a quantum state ρ_{AE} and $\epsilon \in [0,1)$*

$$H_{\min}^\epsilon(A|E)_\rho = \sup_{\tilde{\rho}_{AE} \in \mathcal{B}^\epsilon(\rho_{AB})} H_{\min}(A|E)_{\tilde{\rho}}, \tag{15}$$

where the supremum is taken over positive sub-normalized operators that are ϵ-close to ρ_{AB} in the purifying distance [96].

The smoothing parameter ϵ allows us to restrict attention to typical events (the ones that occur with probability higher than $1-\delta(\epsilon)$, where $\delta(\epsilon)$ is a function of the smoothing parameter). As a consequence, the smoothed min- and max-entropies (see Appendix A for definition) have many nice properties and find an operational interpretation in many applications [96, 97].

Other quantities of interest that will appear along the text are the conditional von-Neumann entropy, $H(A|E)_\rho$, and the conditional collision entropy $H_2(A|E)_\rho$. They are particular cases of the one-parameter family of entropies called sandwiched conditional Réyni entropies, first defined in Ref. [98].

Definition 4. *For any density operator ρ_{AE} and for $\alpha \in [\frac{1}{2},1) \cup (1,\infty)$ the sandwiched α-Réyni entropy of A conditioned on E is defined as*

$$H_\alpha(A|E)_\rho := \frac{1}{1-\alpha} \log \left(\mathrm{Tr}\left[\left(\rho_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE} \rho_E^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right] \right), \tag{16}$$

where $\rho_E^{\frac{1-\alpha}{2\alpha}}$ is a short notation for $\mathrm{I}_A \otimes \rho_E^{\frac{1-\alpha}{2\alpha}}$.

A variant can also be defined as

$$H_\alpha^\uparrow(A|E)_\rho := \sup_{\sigma_E \in \mathcal{S}} \frac{1}{1-\alpha} \log \left(\mathrm{Tr}\left[\left(\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE} \sigma_E^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right] \right), \tag{17}$$

where $\mathcal{S}$ denotes the set of quantum states and the supremum is taken over density operators σ_E.

The min- and max- entropy correspond to the extremal cases of definition (17) for $\alpha = \infty$ and $\alpha = \frac{1}{2}$ respectively. For $\alpha \to 1$, definition (16) and (17) coincide and one recover the standard conditional von-Neumann entropy. Properties of the conditional α-Réyni entropies are presented in Appendix A.

4.2. Security of DIQKD

In order to determine what it means for a DIQKD protocol to be secure, we adopt the security definition used in [39]. This security definition follows the universally composable security definition for standard QKD protocols [40]. However it is important to note that for the device-independent case composability was never proved and attacks

proposed in Ref. [41] show that composability is not achieved if the same devices are re-used for generation of a subsequent key.

In the composably secure paradigm, the security of a protocol is defined in terms of its distance to an ideal protocol [40, 99]. Following this definition, given a protocol described by the completely positive and trace preserving (CPTP) map $\text{diqkd}_{\text{real}}$, we say that the protocol is ϵ^s_{DIQKD}-secure for any $\epsilon^s_{DIQKD} \geq \epsilon$ if:

$$\epsilon := \frac{1}{2} \|\text{diqkd}_{\text{real}} - \text{diqkd}_{\text{ideal}}\|_\diamond \tag{18}$$

$$= \sup_{\rho_{ABE}} \frac{1}{2} \|\text{diqkd}_{\text{real}}(\rho_{ABE}) - \text{diqkd}_{\text{ideal}}(\rho_{ABE})\|_1. \tag{19}$$

Expression (19) can be split into two terms that reflect independently the correctness and the secrecy of the protocol (see [40]), given by Definitions 1 and 2. Correctness is the statement that Alice and Bob share equal strings of bits at the end of the protocol. And secrecy states how much information the eavesdropper can have about their shared key.

Another requirement for a good DIQKD protocol is that there exist a realistic implementation that do not lead the protocol to abort almost all the time, *i.e.*, the protocol should have some robustness. This is captured by the concept of completeness.

Definition 5 (Security). *A DIQKD protocol is $(\epsilon^s_{DIQKD}, \epsilon^c_{DIQKD}, l)$-secure if*

(i) *(Soundness) For any implementation of the protocol, either it aborts with probability greater than $1 - \epsilon^s_{DIQKD}$ or an ϵ^s_{DIQKD}-correct-and-secret key of length l is obtained.*

(ii) *(Completeness) There exists an honest implementation of the protocol such that the probability of not aborting, $p(\Omega)$, is greater than $1 - \epsilon^c_{DIQKD}$.*

The correctness of the final key is ensured by the error correction step. During error correction, Alice sends to Bob a sufficient amount of information so that he can correct his raw key. If Alice and Bob do not abort in this step, then the probability that they end up with different raw keys is guaranteed to be very small. For the secrecy of the protocol, according to Definition 2, one needs to estimate how far the final state describing Alice's key and the eavesdropper system is from a state where the eavesdropper is totally ignorant about Alice's key, see Eq. (4). The formal security proof of quantum key distribution became possible due to the quantum Leftover Hashing Lemma [48, 100] that quantifies the secrecy of a protocol as a function of a conditional entropy of the state before privacy amplification and the length of the final key.

Theorem 4 (Leftover Hashing Lemma ([48], Theorem 5.5.1)). *Let $\rho_{A_1^n E}$ be a classical-quantum state and let $\mathcal{H}$ be a 2-universal family of hash functions, from $\{0,1\}^n$ to $\{0,1\}^l$, that maps the classical n-bit string A_1^n into K_A. Then*

$$\|\rho_{K_A H E} - \tau_{K_A} \otimes \rho_{HE}\|_1 \leq 2^{-\frac{1}{2}\left(H_2^\uparrow(A_1^n|E)_\rho - l\right)}. \tag{20}$$

For the proof of the Leftover Hashing Lemma we refer to Ref. [48]. In Ref. [48], it was shown that the Leftover Hashing lemma can also be formulated in terms of the

smooth min-entropy, and the price to pay is only a linear term in the security parameter♯.

Theorem 5 (Leftover Hashing Lemma with smooth min-entropy [11, 48]). *Let $\rho_{A_1^n E}$ be a classical-quantum state and let $\mathcal{H}$ be a 2-universal family of hash functions, from $\{0,1\}^n$ to $\{0,1\}^l$, that maps the classical n-bit string A_1^n into K_A. Then*

$$\|\rho_{K_A HE} - \tau_{K_A} \otimes \rho_{HE}\|_1 \leq 2^{-\frac{1}{2}\left(H_{\min}^\epsilon(A_1^n|E)_\rho - l\right)} + 2\epsilon. \tag{21}$$

Given the Leftover Hash Lemma, stated in Theorems 4 and 5, and the definition of secrecy, Definition 2, we can now express the length of a secure key as a function of the entropy of Alice's raw key conditioned on Eve's information before privacy amplification.

Theorem 6 (Key length). *Let $p(\Omega)$ be the probability that the DIQKD protocol does not abort for a particular implementation. If the length of the key generated after privacy amplification is given by*

$$l = H_2^\uparrow(A_1^n|E)_{\rho_{|\Omega}} - 2\log\left(\frac{1}{2\epsilon_{PA}}\right). \tag{22}$$

then the DIQKD protocol is ϵ_{PA}-secret.

We can also express the key length in terms of the smooth min-entropy, where if l satisfies

$$l = H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}} - 2\log\left(\frac{p(\Omega)}{2\epsilon_{PA}}\right) \tag{23}$$

$$\geq H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}} - 2\log\left(\frac{1}{2\epsilon_{PA}}\right), \tag{24}$$

then the DIQKD protocol is $\epsilon_{PA} + \epsilon_s$-secret.

We see that the leftover hashing lemma expressed in terms of smooth min-entropy only leads to an extra ϵ_s term in the security parameter. However, the smooth min-entropy can be much larger than the 2-Rényi entropy $H_2^\uparrow$ and, therefore, it is advantageous to lower bound the key by the smooth min-entropy.

4.3. Security analysis

In the previous section we have seen that in order to determine the length of a secret key generated by a particular protocol one needs to estimate the (smooth-min or 2-Rényi) entropy of Alice's string conditioned on all the information available to the eavesdropper before privacy amplification. Now, in order to estimate this quantity for a DIQKD protocol one faces two main challenges:

- How to evaluate the entropy of a very long string of bits?
- How to evaluate the one-round entropy in the device-independent scenario?

♯ In Ref. [48], the leftover hash lemma was formulated with the smooth min-entropy defined as a supremum over states that are ϵ-close to ρ in the trace norm. The proof of Theorem 5, with the smooth min-entropy defined according to Definition 4, can be found in Ref. [11].

In Section 4.3.1 we present the theoretical tools that allow to reduce the problem of evaluating the entropy of a string of bits to the evaluation of a single round. Moreover, in the DI scenario we do not want to make any assumptions over the underlying quantum state and measurement devices. In Section 4.3.2 we present a tight bound derived in [16, 27] for the one round conditional von Neumann entropy of protocols where Alice and Bob test the CHSH inequality. Moreover we explore further this bound to prove a tight bound on the single round conditional collision entropy as a function of the CHSH violation.

4.3.1. Reducing the problem to the estimation of one round. We now present the techniques that allow to reduce the evaluation of the entropy $H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}}$ to the estimation of the conditional von Neumann entropy of a single round for the two adversarial scenarios under consideration, collective attacks and coherent attacks. Moreover, for the IID scenario, *i.e.* when the eavesdropper is assumed to be restricted to collective attacks, we show how to break the analysis of the entropy $H_2^{\uparrow}(A_1^n|E)_{\rho_{|\Omega}}$ into single rounds evaluation.

The IID scenario (collective attacks). When we restrict the eavesdropper to collective attacks, we are assuming that, even though she can perform an arbitrary operation in her quantum side information, the state distributed by the source and the behavior of Alice's and Bob's devices are the same in every round of the protocol. This implies that after n rounds, the state shared by Alice, Bob and Eve is $\rho_{A_1^n B_1^n E} = \rho_{ABE}^{\otimes n}$. In this case, the quantum asymptotic equipartition property (AEP) [60] allows to break the conditional smooth min-entropy of state $\rho_{AE}^{\otimes n}$ into n times the conditional von Neumann entropy of the state ρ_{AE}.

Theorem 7 (Asymptotic equipartition property [60]). *Let $\rho = \rho_{AE}^{\otimes n}$ be an i.i.d. state. Then for $n \geq \frac{8}{5} \log \frac{2}{\epsilon^2}$*

$$H_{\min}^{\epsilon}(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} \geq nH(A|E)_{\rho_{AE}} - \sqrt{n}\,\delta(\epsilon, \eta) \tag{25}$$

and similarly

$$H_{\max}^{\epsilon}(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} \leq nH(A|E)_{\rho_{AE}} + \sqrt{n}\,\delta(\epsilon, \eta) \tag{26}$$

where $\delta(\epsilon, \eta) = 4 \log \eta \sqrt{\log \frac{2}{\epsilon^2}}$ and $\eta = \sqrt{2^{-H_{\min}(A|E)_{\rho_{AE}}}} + \sqrt{2^{H_{\max}(A|E)_{\rho_{AE}}}} + 1$.

The quantum AEP is a generalization to quantum systems of the classical statement that, in the limit of many repetitions of a random experiment, the output sequence is one from the typical set. Therefore, under the assumption of collective attacks, the quantum AEP reduces the problem of estimating the key rate of a string of n bits to the problem of bounding the one-round conditional von Neumann entropy. We remark that the AEP implies an additional term, proportional to $\sqrt{n}$, which is significant for the finite regime analyses.

In Section 4.2, we have seen that the left-over hashing lemma can also be stated in the terms of the 2-Réyni conditional entropy $H_2^\uparrow(A|E)_\rho$. A useful property of the conditional $H_\alpha^\uparrow$ entropies is additivity [96] (see Appendix A Property 1(ii)), which implies the following lemma.

Lemma 1. *Let $\rho = \rho_{AE}^{\otimes n}$ be an i.i.d. state. Then*

$$H_2^\uparrow(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} = nH_2^\uparrow(A|E)_{\rho_{AE}} \geq nH_2(A|E)_{\rho_{AE}}, \tag{27}$$

where $H_2(A|E)_{\rho_{AE}}$ is denoted collision entropy.

Validity of Lemma 1 can be seen from the following: equality in (27) follows from the additivity property of $H_\alpha^\uparrow$ entropies, Property 1(ii) in Appendix A, and the inequality follows from the definition of α-Rényi entropies, Definition 4.

Therefore, for collective attacks one can break the analysis into the evaluation of a single-round entropy by using both, the formulation of the left-over hashing lemma in terms of the smooth-min entropy, Theorem 5, and in terms of the 2-Rényi entropy, Theorem 4. The possible advantage of using Lemma 1 over the AEP, Theorem 7, is that no extra overhead term $\mathcal{O}(\sqrt{n})$ is gained due to the additive property of the 2-Réyni conditional entropy $H_2^\uparrow(A|E)_\rho$. However, in general the von Neumann entropy can be much larger than the collision entropy, and this trade-off has to be taken into account. We remark that, for protocols based on other Bell inequalities, the techniques used for deriving Theorem 3 can be advantageous for collective attack analysis. This is due to the fact that for other Bell inequalities there is no known technique to directly bound the conditional von-neumann entropy and a good bound on the min-entropy can be found using semidefinite-programming techniques (see Section 4.3.2).

The fully DI scenario (coherent attacks). In the fully device-independent scenario the eavesdropper can perform a general coherent attack, and the state shared by the parties may not be of the form $\rho_{ABE}^{\otimes n}$. Therefore, the tools presented in the previous section are not applicable in this scenario. In standard QKD, de Finetti techniques [47,48,50] allow one to extend the proofs against collective attacks to coherent attacks for protocols that present some symmetry. The price to pay is an overhead term $\mathcal{O}(\sqrt{n})$ whose pre-factor depends on the dimension of the underlying system. However, in the device-independent scenario, we do not want to make assumptions on the dimension of the underlying system. Moreover, symmetry of the protocol is not guaranteed, as we do not know the behaviour of the measurement devices. Therefore, de Finetti techniques cannot be used to straightforwardly extend the security proofs against collective attacks to coherent attacks in the device-independent scenario.

Recently, this problem was overcome by the entropy accumulation theorem (EAT) [1,51]. In this section, we state the entropy accumulation theorem, which allows to break the entropy $H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}}$ into the entropy of single rounds and therefore extends proofs against collective attacks to coherent attacks.

An important ingredient in the formulation of the EAT is the concept of min-/max-tradeoff function of a channel.

Definition 6. *Let $\mathcal{N}_i$ be a CPTP map that maps R_{i-1} to $\hat{A}_i\hat{B}_iC_iR_i$, where $\hat{A}_i$, $\hat{B}_i$ and C_i are classical registers and the value of C_i can be inferred from $\hat{A}_i$ and $\hat{B}_i$. Let $\vec{q}$ denote a probability distribution on the possible values the random variable C_i can assume. The min- and max-tradeoff functions for the channel $\mathcal{N}_i$ are defined as:*

$$f_{\min}(\vec{q}) \leq \inf_{\sigma\in\Sigma_i(\vec{q})} H(\hat{A}_i|\hat{B}_iR)_\sigma, \tag{28}$$

$$f_{\max}(\vec{q}) \geq \sup_{\sigma\in\Sigma_i(\vec{q})} H(\hat{A}_i|\hat{B}_iR)_\sigma, \tag{29}$$

where

$$\Sigma_i(\vec{q}) = \left\{\sigma_{C_i\hat{A}_i\hat{B}_iR_iR} = (\mathcal{N}_i\otimes I_R)(\omega_{R_{i-1}R})|\sigma_{C_i} = \vec{q}\right\}, \tag{30}$$

and the infimum and supremum are set to $+\infty, -\infty$, respectively, if the set $\Sigma_i(\vec{q})$ is empty.

Definition 6 states that the min-(max-)tradeoff function is a lower (upper) bound on the conditional von Neumann entropy $H(\hat{A}_i|\hat{B}_iR)_\sigma$ of a final state $\sigma_{C_i\hat{A}_i\hat{B}_iR_iR}$, for all states that result from the action of the channel $\mathcal{N}_i$ on an arbitrary initial state and exhibit a particular distribution $\vec{q}$ over the classical variable C_i, where R is a side information. In particular, for a DIQKD protocol, where we are testing the CHSH inequality, the variable $\hat{A}_i$ can be the outputs of Alice and Bob in round i, $\hat{A} = \{A_i, B_i\}$. The variable $\hat{B}_i$ can be the inputs of Alice and Bob together with the variable that determines whether the round is a test round or a key generation round, $\hat{B}_i = \{X_i, Y_i, T_i\}$. And R can represent any quantum side information E that the eavesdropper holds. We will then be interested in defining a variable C_i that assumes value 1 if the condition of the CHSH game is satisfied (*i.e.* if the outputs of Alice and Bob satisfy $A_i + B_i = X_i \cdot Y_i$), 0 if it is not satisfied and we attribute the value $\perp$ if the inequality was not tested in that round (*i.e.* if $T_i = 0$, the key generations rounds). Now the distributions $\vec{q} = (q(0), q(1), q(\perp))$ of interest are the ones that achieve a winning probability ω for the CHSH game, *i.e.* $\frac{q(1)}{1-q(\perp)} = \omega$. The EAT channel $\mathcal{N}_i$ represents local maps that, according to the value of T_i, generate the variables X_i, Y_i randomly and independently, and then generate the outcomes A_i and B_i. Finally, the set of states $\Sigma_i(\vec{q})$ of interest are all the states resulting from the action of this channel in an arbitrary state and exhibiting a violation $\beta = 8\omega - 4$ for the CHSH inequality. For a more detailed description of the EAT channel associated to Protocol 1, we refer the reader to [1, 39].

We now state the entropy accumulation theorem.

Theorem 8 (The entropy accumulation theorem (EAT) [51]). *For an event Ω that happens with probability $p(\Omega)$, and for t such that $f_{\min}(freq(c_1^n)) \geq t \ \forall \ c_1^n \in \Omega$, it holds that*

$$H_{\min}^\epsilon(A_1^n|B_1^nE)_{\rho_{|\Omega}} > nt - \nu\sqrt{n} \tag{31}$$

and similarly, for t' such that $f_{\max}(freq(c_1^n)) \leq t' \; \forall \; c_1^n \in \Omega$,

$$H_{\max}^{\epsilon}(A_1^n|B_1^n E)_{\rho|\Omega} < nt' + \nu\sqrt{n} \tag{32}$$

with

$$\nu = 2\left(\log\left(1 + 2d_A\right) + \lceil\|\nabla f\|_\infty\rceil\right)\sqrt{1 - 2\log\left(\epsilon_s \cdot p(\Omega)\right)} \tag{33}$$

for f equals to $f_{\min}$ and $f_{\max}$ respectively .

Analogous to the AEP, the entropy accumulation theorem allows us to break the entropy of the string of bits into the entropy of a single round. Note, however, that this single-round entropy does not refer to the real entropy of each round of the protocol, but is evaluated over the hypothetical states that would achieve the observed violation. It is important to remark that a crucial assumption in the EAT [1,51] is that some of the variables of interested satisfy what is called the Markov condition. This is the case for QKD protocols performed sequentially. For definition and discussion of the implications of the Markov condition, see [51].

4.3.2. Estimating the one-round entropy. Now that we have reduced the evaluation of the secret key length to the estimation of the conditional von Neumann entropy of a single round, we are ready to face the next challenge: How to estimate the single round entropy without any assumptions on the quantum states and behavior of the measurement devices.

The CHSH scenario: The CHSH scenario [37], where Alice and Bob each perform one among two possible binary measurements, is significantly simpler than other Bell scenarios. Due to the fact that the CHSH inequality has only two binary inputs per party, a strong result [101, 102] states that the description of any realization of a CHSH experiment can be decomposed into subspaces of dimension two, where projective measurements are performed in each subspace. This allows one to restrict the analysis to qubits, which significantly simplifies the problem. Exploring these nice properties, a tight bound on the von Neumann entropy of Alice's outcome conditioned on Eve's information, as a function of the CHSH violation, was derived in [16, 27].

Lemma 2. *Given that Alice and Bob share a state ρ_{AB} that achieves a violation β for the CHSH inequality, it holds that*

$$H(A|E)_\rho \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{\beta}{2}\right)^2 - 1}\right). \tag{34}$$

In Section 4.3.1 we have seen that for collective attacks the key rate can also be estimated by the single round collision entropy. And due to the additivity property of $H_2^\uparrow$, no overhead $\sqrt{n}$ term is present. Therefore, this analysis can potentially lead to an advantage with respect to the minimum number of rounds required for positive key rate. The conditional collision entropy satisfies the following relation [96, Corollary 5.3]

$$H_2(A|E)_\rho \geq H_{\min}(A|E)_\rho. \tag{35}$$

And a lower bound for the conditional min-entropy as a function of the Bell violation was derived in [103]:

$$H_{\min}(A|E)_\rho \geq -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{\beta^2}{4}}\right). \tag{36}$$

Therefore expression (36) can be used to bound the conditional collision entropy as a function of the violation β. We now prove that this bound is actually tight.

Theorem 9. *There exist a state ρ^*_{AB} and measurements for Alice and Bob such that, ρ^*_{AB} achieves violation β and the collision entropy of Alice's output A conditioned on Eve's quantum information E is*

$$H_2(A|E)_{\rho^*} = -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{\beta^2}{4}}\right). \tag{37}$$

The proof of Theorem 9 is presented in Appendix C. Theorem 9 together with relations (35) and (36) imply a tight lower bound for the conditional collision entropy as a function of the CHSH violation β. In Figure 4.3.2 we plot $H(A|E)$ and $H_2(A|E)$ as a function of the violation β. One can see that the points of maximum and minimum entropy (corresponding to maximal violation $\beta = 2\sqrt{2}$ and no violation, respectively) coincide, but for intermediate values of β the conditional collision entropy is smaller than the conditional von Neumann entropy.
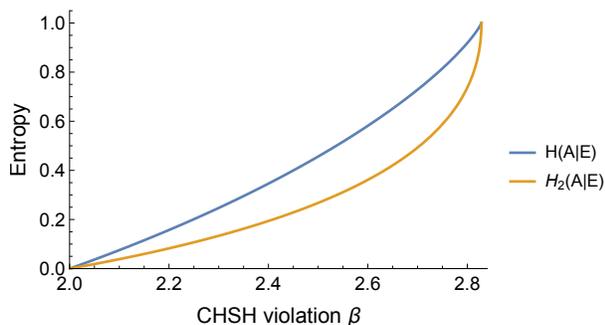
Figure 7. Graph illustrating the difference of the conditional von Neumann entropy $H(A|E)$ and the conditional collision entropy $H_2(A|E)$ as a function of the CHSH violation β.

Other Bell inequalities and the min-entropy estimation: The use of different Bell inequalities has proved to be advantageous in different taks. For example, a tilted CHSH inequality was used to certify maximal randomness in states arbitrarily close to separable [104], and inequalities with more inputs and outputs have shown to exhibit higher noise robustness [105]. Therefore it is natural to ask whether other Bell inequalities can also bring advantage to the task of device-independent quantum key distribution.

By considering an arbitrary Bell inequality, one faces the problem that the techniques used to bound the conditional von Neumann entropy as a function of the CHSH violation do not apply. Indeed, the proof of Lemma 2 is highly based on the fact that one can reduce the analysis to qubits. In fact, very few results are known on tight bounds for the conditional von Neumann entropy as a function of the Bell violation for

other inequalities. In [106] a bound was derived for a family of inequalities denoted measurement-device-dependent inequalities [107], which are very suitable for the task of randomness amplification. In [108] a tight bound was derived as a function of the violation of the multipartite MABK inequality [109–111]. However in these two cases the proof is based on a reduction to the CHSH inequality.

In general, the conditional von Neumann entropy can be lower bounded by the conditional min-entropy

$$H(A|E)_\rho \geq H_{\min}(A|E)_\rho. \tag{38}$$

The advantage of looking at the conditional min-entropy is that it can be computed as a function of the Bell violation by a semi-definite programming [103]. The idea is that in order to estimate the min-entropy one can upper bound the guessing probability, p_{guess} (see Eq. (13)), of the eavesdropper. This problem can then be expressed as an optimization over probability distributions, which is exactly the information available in the device-independent scenario. As shown in Ref. [103], for any Bell inequality, an upper bound on the p_{guess} can be obtained by a semidefinite programming making use of the NPA-hierarchy [112, 113].

Lower bounding the conditional von-Neumann entropy by the min-entropy might be far from optimal. For example, for the CHSH inequality we have that the conditional von Neumann entropy as a function of the violation is much larger than the conditional min-entropy, as illustrated in Fig. 7 (recall that, in Theorem 9, $H_{\min}(A|E)_\rho$ was shown to be a tight bound on $H_2(A|E)_\rho$ as a function of the CHSH violation). By making use of the tight bound on the conditional von Neumann entropy, eq. (34), one can prove security for DIQKD up to 7.1% of QBER [16], whereas using the min-entropy, eq. (36), security can only be guaranteed up to a QBER of 5.2% [103].

It is still an open problem whether any other Bell inequality can lead to better performance for DIQKD than the CHSH inequality. Recently, an extensive analysis of the performance of different Bell inequalities for the task of randomness expansion was presented in [114].

4.3.3. Key rates. The techniques presented in Sections 4.3.1 and 4.3.2 allows us to establish the length of a secure key that can be extracted as a function of the CHSH violation β and QBER Q.

For coherent attacks, the entropy accumulation theorem (Theorem 8) and the tight lower bound on the conditional von Neumann entropy (Lemma 2) are the key tools to establish Theorem 1. The complete proof of Theorem 1 includes several intermediate steps, and is presented in details in Appendix B.3.

For collective attacks, the key ingredients to derive Theorem 2 are the asymptotic equipartition property (Theorem 7) and Lemma 2. A detailed proof of Theorem 2 is presented in Appendix B.1. We have also presented a different technique of breaking the entropy of Alice's string into the entropy of single rounds in the IID scenario, namely by making use use of the additivity of 2-Réyni entropy, Lemma 1. This technique, together

with Theorem 9 leads to Theorem 3. A detailed proof of Theorem 3 can be found in Appendix B.2.

Acknowledgments

References

[1] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," Nature Communications, vol. 9, no. 459, 2018.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175 – 179, 1984.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, pp. 661–663, 1991.

[4] D. Dieks, "Communication by EPR devices," Physics Letters A, vol. 92, no. 6, pp. 271 – 272, 1982.

[5] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, pp. 802 – 803, 1982.

[6] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," Phys. Rev. A, vol. 61, p. 052306, 2000.

[7] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 457–475, 2003.

[8] H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate," Phys. Rev. A, vol. 66, p. 060302, 2002.

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nature Communications, vol. 3, no. 634, 2012.

[10] M. Hayashi and T. Tsurumaru, "Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths," New Journal of Physics, vol. 14, no. 9, p. 093014, 2012.

[11] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum, vol. 1, p. 14, 2017.

[12] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, "Long-distance quantum key distribution in optical fibre," New Journal of Physics, vol. 8, no. 9, p. 193, 2006.

[13] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nature Photonics, vol. 9, pp. 163–168, 2015.

[14] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer,

G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett., vol. 120, p. 030501, 2018.

[15] A. Yao and D. Mayers, "Quantum cryptography with imperfect apparatus," in Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)(FOCS), p. 503, 1998.

[16] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," New Journal of Physics, vol. 11, no. 4, p. 045021, 2009.

[17] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A, vol. 78, p. 042333, 2008.

[18] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, " Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photonics, vol. 4, p. 686, 2010.

[19] H. Weier, H. Krauss, M. Rau, M. Frst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," New Journal of Physics, vol. 13, no. 7, p. 073024, 2011.

[20] 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," Nature Communications, vol. 2, p. 349, 2011.

[21] A. Acín, N. Gisin, and L. Masanes, "From Bell's theorem to secure quantum key distribution," Phys. Rev. Lett., vol. 97, p. 120405, 2006.

[22] A. Acín, S. Massar, and S. Pironio, "Efficient quantum key distribution secure against no-signalling eavesdroppers," New Journal of Physics, vol. 8, no. 8, p. 126, 2006.

[23] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, "Secrecy extraction from no-signaling correlations," Phys. Rev. A, vol. 74, p. 042339, 2006.

[24] L. Masanes, "Universally composable privacy amplification from causality constraints," Phys. Rev. Lett., vol. 102, p. 140501, 2009.

[25] E. Hänggi, R. Renner, and S. Wolf, Efficient Device-Independent Quantum Key Distribution, pp. 216–234. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[26] S. Pironio, L. Masanes, A. Leverrier, and A. Acín, "Security of device-independent quantum key distribution in the bounded-quantum-storage model," Phys. Rev. X, vol. 3, p. 031007, 2013.

[27] 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., vol. 98, p. 230501, 2007.

[28] L. Masanes, S. Pironio, and A. Acin, "Secure device-independent quantum key distribution with causally independent measurement devices," Nature Communications, vol. 2, p. 238, 2011.

[29] E. Hänggi and R. Renner, "Device-independent quantum key distribution with commuting measurements," arXiv:1009.1833, 2010.

[30] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, "Full security of quantum key distribution from no-signaling constraints," IEEE Transactions on Information Theory, vol. 60, no. 8, pp. 4973–4986, 2014.

[31] J. Barrett, R. Colbeck, and A. Kent, "Unconditionally secure device-independent quantum key distribution with only two devices," Phys. Rev. A, vol. 86, p. 062326, 2012.

[32] B. W. Reichardt, F. Unger, and U. Vazirani, "A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games," in Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, ITCS '13, (New York, NY, USA), pp. 321–322, ACM, 2013.

[33] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," Phys. Rev. Lett., vol. 113, p. 140501, 2014.

[34] C. A. Miller and Y. Shi, "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices," J. ACM, vol. 63, no. 4, pp. 33:1–33:63, 2016.

[35] D. Unruh, "Everlasting multi-party computation," in Advances in Cryptology – CRYPTO 2013, pp. 380–397, Springer Berlin Heidelberg, 2013.

[36] J. Ribeiro, G. Murta, and S. Wehner, "Fully general device-independence for two-party cryptography and position verification," arXiv: 1609.08487, 2016.

[37] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," Phys. Rev. Lett., vol. 23, pp. 880–884, 1969.

[38] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, "Consequences and limits of nonlocal strategies," in Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004., pp. 236–249, 2004.

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

[40] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," arXiv: 1409.3525, 2014.

[41] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," Phys. Rev. Lett., vol. 110, p. 010503, 2013.

[42] D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," in Advances in Cryptology — CRYPTO '96, pp. 343–357, Springer Berlin Heidelberg, 1996.

[43] D. Mayers, "Unconditional security in quantum cryptography," J. ACM, vol. 48, no. 3, pp. 351–406, 2001.

[44] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science, vol. 283, no. 5410, pp. 2050–2056, 1999.

[45] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett., vol. 85, pp. 441–444, 2000.

[46] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," pp. 407–425, 2005.

[47] R. König and R. Renner, "A de Finetti representation for finite symmetric quantum states," Journal of Mathematical Physics, vol. 46, no. 12, p. 122108, 2005.

[48] R. Renner, Security of quantum key distribution. Diss., ETH Zürich, Nr. 16242, 2005.

[49] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," Rev. Mod. Phys., vol. 86, pp. 419–478, 2014.

[50] M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," Phys. Rev. Lett., vol. 102, p. 020504, 2009.

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

[52] B. Hensen, H. Bernien, A. E. Drau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abelln, 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, vol. 526, pp. 682 – 689, 2015.

[53] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-loophole-free test of Bell's theorem with entangled photons," Phys. Rev. Lett., vol. 115, p. 250401, 2015.

[54] 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., vol. 115, p. 250402, 2015.

[55] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, "Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes," Phys. Rev. Lett., vol. 119, p. 010402, 2017.

[56] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, "Bell violation using entangled photons without the fair-sampling assumption," Nature, vol. 497, no. 7448, pp. 227–230, 2013.

[57] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, "Detection-loophole-free test of quantum nonlocality, and applications," Phys. Rev. Lett., vol. 111, p. 130406, 2013.

[58] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe, "Bell inequality violation with two remote atomic qubits," Phys. Rev. Lett., vol. 100, p. 150404, 2008.

[59] 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, vol. 464, pp. 1021–1024, 2010.

[60] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," IEEE Transactions on Information Theory, vol. 55, no. 12, pp. 5840–5847, 2009.

[61] F. Dupuis and O. Fawzi, "Entropy accumulation with improved second-order," arXiv:1805.11652, 2018.

[62] J. F. Clauser and M. A. Horne, "Experimental consequences of objective local theories," Phys. Rev. D, vol. 10, pp. 526–535, 1974.

[63] P. H. Eberhard, "Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment," Phys. Rev. A, vol. 47, pp. R747–R750, 1993.

[64] A. Máttar, J. Kołodyński, P. Skrzypczyk, D. Cavalcanti, K. Banaszek, and A. Acín, "Device-independent quantum key distribution with single-photon sources," arXiv: 1803.07089, 2018.

[65] C. W. Chou, H. De Riedmatten, D. Felinto, S. V. Polyakov, S. J. Van Enk, and H. J. Kimble, "Measurement-induced entanglement for excitation stored in remote atomic ensembles," Nature, vol. 438, no. 7069, pp. 828–832, 2005.

[66] I. Usmani, C. Clausen, F. Bussières, N. Sangouard, M. Afzelius, and N. Gisin, "Heralded quantum entanglement between two crystals," Nature Photonics, vol. 6, no. 4, pp. 234–237, 2012.

[67] D. L. Moehring, P. Maunz, S. Olmschenk, K. C. Younge, D. N. Matsukevich, L.-M. Duan, and C. Monroe, "Entanglement of single-atom quantum bits at a distance.," Nature, vol. 449, no. 7158, pp. 68–71, 2007.

[68] J. Hofmann, M. Krug, N. Ortegel, L. Gérard, M. Weber, W. Rosenfeld, and H. Weinfurter, "Heralded entanglement between widely separated atoms," Science, vol. 336, no. 6090, pp. 72–75, 2012.

[69] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, "Heralded entanglement between solid-state qubits separated by three metres," Nature, vol. 497, no. 7447, pp. 86–90, 2013.

[70] A. Delteil, Z. Sun, W.-b. Gao, E. Togan, and S. Faelt, "Generation of heralded entanglement between distant hole spins," Nat. Phys., vol. 12, no. March, p. 218, 2016.

[71] R. Riedinger, A. Wallucks, I. Marinkovic, C. Löschnauer, M. Aspelmeyer, S. Hong, and S. Gröblacher, "Remote quantum entanglement between two micromechanical oscillators," Nature, vol. 556, pp. 473–477, 2018.

[72] B. Hensen, N. Kalb, M. S. Blok, A. Dréau, A. Reiserer, R. F. L. Vermeulen, M. Markham, D. J. Twitchen, K. Goodenough, D. Elkouss, and S. Wehner, "Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis," Scientific reports, vol. 6, p. 30289, 2016.

[73] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, and C. Monroe, " Modular entanglement of atomic qubits using photons and phonons," Nature Physics, vol. 11, pp. 37–42, 2015.

[74] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, "Entanglement distillation between solid-state quantum network nodes," Science, vol. 356, no. 6341, pp. 928–932, 2017.

[75] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, "Deterministic delivery of remote entanglement on a quantum network," Nature, vol. 558, pp. 268–273, 2018.

[76] A. Reiserer and G. Rempe, "Cavity-based quantum networks with single atoms and optical photons," Rev. Mod. Phys., vol. 87, pp. 1379–1418, 2015.

[77] D. D. Awschalom, R. Hanson, J. Wrachtrup, and B. B. Zhou, "Quantum technologies with optically interfaced solid-state spins," Nat. Photonics, vol. 12, no. 9, pp. 516–527, 2018.

[78] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, "Repeated quantum error correction on a continuously encoded qubit by real-time feedback," Nature communications, vol. 7, p. 11526, 2016.

[79] N. Kalb, P. C. Humphreys, J. J. Slim, and R. Hanson, "Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks," Phys. Rev. A, vol. 97, p. 062330, 2018.

[80] S. D. Barrett and P. Kok, "Efficient high-fidelity quantum computation using matter qubits and linear optics," Physical Review A, vol. 71, p. 060310, 2005.

[81] L. Robledo, L. Childress, H. Bernien, B. Hensen, P. F. A. Alkemade, and R. Hanson, "High-fidelity projective read-out of a solid-state spin quantum register," Nature, vol. 477, no. 7366, pp. 574–578, 2011.

[82] L. Jiang, J. S. Hodges, J. R. Maze, P. C. Maurer, J. M. Taylor, D. G. Cory, P. R. Hemmer, R. L. Walsworth, A. Yacoby, A. S. Zibrov, and M. D. Lukin, "Repetitive Readout of a Single Electron Spin via Quantum Logic with Nuclear Spin Ancillae," Science, vol. 326, no. 5950, pp. 267–272, 2009.

[83] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, and R. Hanson, "Unconditional quantum teleportation between distant solid-state quantum bits," Science, vol. 345, no. 6196, pp. 532–535, 2014.

[84] N. H. Wan, B. J. Shields, D. Kim, S. Mouradian, B. Lienhard, M. Walsh, H. Bakhru, T. Schröder, and D. Englund, "Efficient Extraction of Light from a Nitrogen-Vacancy Center in a Diamond Parabolic Reflector," Nano letters, vol. 18, no. 5, pp. 2787–2793, 2018.

[85] A. Faraon, P. E. Barclay, C. Santori, K.-M. C. Fu, and R. G. Beausoleil, "Resonant enhancement of the zero-phonon emission from a colour centre in a diamond cavity," Nature Photonics, vol. 5, pp. 301–305, 2011.

[86] E. T. Campbell and S. C. Benjamin, "Measurement-based entanglement under conditions of extreme photon loss," Phys. Rev. Lett., vol. 101, p. 130502, 2008.

[87] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller, "Creation of entangled states of distant atoms by interference," Phys. Rev. A, vol. 59, pp. 1025–1033, 1999.

[88] M. Bock, P. Eich, S. Kucera, M. Kreis, A. Lenhard, C. Becher, and J. Eschner, "High-fidelity entanglement between a trapped ion and a telecom photon via quantum frequency conversion," Nature Communications, vol. 9, no. 1998, 2018.

[89] A. Dréau, A. Tchebotareva, A. E. Mahdaoui, C. Bonato, and R. Hanson, "Quantum frequency conversion of single photons from a nitrogen-vacancy center in diamond to telecommunication wavelengths," Phys. Rev. Applied, vol. 9, p. 064031, 2018.

[90] E. Janitz, M. Ruf, M. Dimock, A. Bourassa, J. Sankey, and L. Childress, "Fabry-perot microcavity for diamond-based photonics," Phys. Rev. A, vol. 92, p. 043844, 2015.

[91] S. Bogdanović, S. B. Van Dam, C. Bonato, L. C. Coenen, A. M. J. Zwerver, B. Hensen, M. S. Liddy, T. Fink, A. Reiserer, M. Lončar, and R. Hanson, "Design and low-temperature characterization of a tunable microcavity for diamond-based quantum networks," Applied Physics Letters, vol. 110, no. 17, pp. 1–5, 2017.

[92] D. Riedel, I. Söllner, B. J. Shields, S. Starosielec, P. Appel, E. Neu, P. Maletinsky, and

R. J. Warburton, "Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond," Phys. Rev. X, vol. 7, p. 031040, 2017.

[93] S. Olmschenk, K. C. Younge, D. L. Moehring, D. N. Matsukevich, P. Maunz, and C. Monroe, "Manipulation and detection of a trapped Yb^+ hyperfine qubit," Phys. Rev. A, vol. 76, p. 052314, 2007.

[94] F. Henkel, M. Krug, J. Hofmann, W. Rosenfeld, M. Weber, and H. Weinfurter, "Highly efficient state-selective submicrosecond photoionization detection of single atoms," Phys. Rev. Lett., vol. 105, p. 253001, 2010.

[95] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Transactions on Information Theory, vol. 55, no. 9, pp. 4337–4347, 2009.

[96] M. Tomamichel, "Quantum Information Processing with Finite Resources - Mathematical Foundations," SpringerBriefs in Mathematical Physics book series (BRIEFSMAPHY, volume 5), 2016. Theorems and equations references according to arXiv: 1504.00233.

[97] M. Tomamichel, A Framework for Non-Asymptotic Quantum Information Theory. Diss., Eidgenössische Technische Hochschule ETH Zürich, Nr. 20213, 2012.

[98] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," Journal of Mathematical Physics, vol. 54, no. 12, p. 122203, 2013.

[99] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in Proceedings 2001 IEEE International Conference on Cluster Computing, pp. 136–145, 2001.

[100] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," IEEE Transactions on Information Theory, vol. 57, no. 8, pp. 5524–5535, 2011.

[101] L. Masanes, "Asymptotic violation of Bell inequalities and distillability," Phys. Rev. Lett., vol. 97, p. 050503, 2006.

[102] B. Tsirelson, "Some results and problems on quantum Bell-type inequalities," Hadronic Journal Supplement, vol. 8, pp. 329–345, 1993.

[103] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," Nature Communications, vol. 2, p. 238, 2011.

[104] A. Acín, S. Massar, and S. Pironio, "Randomness versus nonlocality and entanglement," Phys. Rev. Lett., vol. 108, p. 100402, 2012.

[105] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, "Bell inequalities for arbitrarily high-dimensional systems," Phys. Rev. Lett., vol. 88, p. 040404, 2002.

[106] M. Kessler and R. Arnon-Friedman, "Device-independent Randomness Amplification and Privatization," arXiv: 1705.04148, 2017.

[107] G. Pütz, D. Rosset, T. J. Barnea, Y.-C. Liang, and N. Gisin, "Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality," Phys. Rev. Lett., vol. 113, p. 190402, 2014.

[108] J. Ribeiro, G. Murta, and S. Wehner, "Fully device-independent conference key agreement," Phys. Rev. A, vol. 97, p. 022307, 2018.

[109] N. D. Mermin, "Extreme quantum entanglement in a superposition of macroscopically distinct states," Phys. Rev. Lett., vol. 65, pp. 1838–1840, 1990.

[110] M. Ardehali, "Bell inequalities with a magnitude of violation that grows exponentially with the number of particles," Phys. Rev. A, vol. 46, pp. 5375–5378, 1992.

[111] A. V. Belinskiĭ and D. N. Klyshko, "Interference of light and Bell's theorem," Physics-Uspekhi, vol. 36, no. 8, p. 653, 1993.

[112] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations," Phys. Rev. Lett., vol. 98, p. 010401, 2007.

[113] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," New Journal of Physics, vol. 10, no. 7, p. 073013, 2008.

[114] P. J. Brown, S. Ragy, and R. Colbeck, "An adaptive framework for quantum-secure device-

independent randomness expansion," arXiv:1810.13346, 2018.

[115] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, "Chain rules for smooth min- and max-entropies," IEEE Transactions on Information Theory, vol. 59, no. 5, pp. 2603–2612, 2013.

[116] P. Faist, "The entropy zoo." https://www.its.caltech.edu/~phfaist/entropyzoo.

[117] G. Brassard and L. Salvail, Secret-Key Reconciliation by Public Discussion, pp. 410–423. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994.

[118] R. Renner and S. Wolf, Simple and Tight Bounds for Information Reconciliation and Privacy Amplification, pp. 199–216. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.

[119] R. Horodecki, P. Horodecki, and M. Horodecki, "Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition," Physics Letters A, vol. 200, no. 5, pp. 340 – 344, 1995.

Appendix A. Definitions

In this Appendix we present some properties of the conditional sandwiched α-Réyni entropies [98], Definition 4, and the smoothed entropies that are used for the security proof.

Properties 1. *The conditional α-Rényi entropies satisfy:*

(i) **Data processing** *([96] Corollary 5.1): Let $\tau_{AB'} = I_A \otimes \mathcal{E}_B(\rho_{AB})$, where $\mathcal{E}_B$ is a $CPTP(B, B')$ channel, then*

$$H_\alpha(A|B)_\rho \leq H_\alpha(A|B')_\tau \ \text{ and } \ H_\alpha^\uparrow(A|B)_\rho \leq H_\alpha^\uparrow(A|B')_\tau. \qquad (A.1)$$

(ii) **Additivity** *([96] Corollary 5.2): For $\rho_{AB} \otimes \tau_{A'B'}$ it holds that*

$$H_\alpha^\uparrow(AA'|BB')_{\rho \otimes \tau} = H_\alpha^\uparrow(A|B)_\rho + H_\alpha^\uparrow(A'|B')_\tau. \qquad (A.2)$$

(iii) **Entropy of classical information** *([96] Lemma 5.3): For ρ_{ABX} classical in X*

$$H_\alpha(XA|B)_\rho \geq H_\alpha(A|B)_\rho \ \text{ and } \ H_\alpha^\uparrow(XA|B)_\rho \geq H_\alpha^\uparrow(A|B)_\rho. \qquad (A.3)$$

(iv) **Conditioning on classical information** *(see [96] Lemma 5.4): For ρ_{ABX} classical in X,*

$$H_\alpha^\uparrow(A|XB) \geq H_\alpha^\uparrow(A|B) - \log\left(\mathrm{rank}(\rho_X)\right) \qquad (A.4)$$

$$\geq H_\alpha^\uparrow(A|B) - \log|X|, \qquad (A.5)$$

where $\mathrm{rank}(\rho_X)$ is the rank of matrix ρ_X and $|X|$ is the dimension of system X.

(v) **Conditioning on classical information** *(see [96] Proposition 5.1): Let $\rho_{ABX} = \sum_x p_x \rho_{AB}^x \otimes |x\rangle\langle x|$ then,*

$$H_\alpha(A|BX)_\rho = \frac{1}{1-\alpha} \log\left(\sum_x p(X=x)2^{((1-\alpha)H_\alpha(A|BX=x)_\rho)}\right), \quad (A.6)$$

$$H_\alpha^\uparrow(A|BX)_\rho = \frac{\alpha}{1-\alpha} \log\left(\sum_x p(X=x)2^{\left(\frac{1-\alpha}{\alpha}H_\alpha^\uparrow(A|BX=x)_\rho\right)}\right). \quad (A.7)$$

And for the conditional von Neumann it holds that

$$H(A|BX)_\rho = \sum_x p(X=x)H(A|BX=x)_\rho. \qquad (A.8)$$

In Property 1.(iv), the relation $H_\alpha^\uparrow(A|XB) \geq H_\alpha^\uparrow(A|B) - \log|X|$ was stated in [96]. We remark that the middle inequality follows from the fact that $H_\alpha^\uparrow(A|XB)$ is invariant under local isometries. Therefore if $X' = \mathcal{V}(X)$ is a full rank operator where $\mathcal{V}(\cdot)$ is an isometry, we have that

$$H_\alpha^\uparrow(A|XB) = H_\alpha^\uparrow(A|X'B) \geq H_\alpha^\uparrow(A|B) - \log|X'| \tag{A.9}$$

and since $\mathcal{V}(\cdot)$ is an isometry $|X'| = \text{rank}(\rho_X)$.

The min- and max- entropy are the particular extreme cases of $H_\alpha^\uparrow$ for $\alpha = \infty$ and $\alpha = \frac{1}{2}$ respectively. For $\alpha \to 1$ one recovers the standard conditional von-Neumann entropy. The smoothed min- and max-entropies are defined as an optimization over operators that are ϵ-close, in the purified distance, to the state of interest. This optimization takes into account also operators that are sub-normalized, *i.e.* positive operators with trace smaller than 1.

Definition 7 (Smoothed entropies [96])**.** *Let ρ_{AB} be a quantum state and $\epsilon \geq 0$. The smooth min-entropy of system A conditioned on B is defined as*

$$H_{\min}^\epsilon(A|B)_\rho = \max_{\tilde{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}. \tag{A.10}$$

The smooth max-entropy is

$$H_{\max}^\epsilon(A|B)_\rho = \min_{\tilde{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} H_{\max}(A|B)_{\tilde{\rho}}. \tag{A.11}$$

In Definition 7, $\mathcal{B}^\epsilon(\rho_{AB})$ is an ϵ-ball of sub-normalized operators around state ρ_{AB} defined in terms of the purified distance.

Definition 8 (Purified distance [96])**.** *For sub-normalized positive operators X and Y, i.e. $X, Y \geq 0$ and $\text{Tr}(X) \leq 1, \text{Tr}(Y) \leq 1$, the purified distance is given by*

$$\mathcal{D}(X, Y) = \sqrt{1 - F_*(X, Y)}, \tag{A.12}$$

where $F_*(\cdot, \cdot)$ is the generalized fidelity, defined as

$$F_*(X, Y) = \left(\text{Tr}\,|\sqrt{X}\sqrt{Y}| + \sqrt{(1 - \text{Tr}\,\rho)(1 - \text{Tr}(Y))}\right)^2. \tag{A.13}$$

The smoothed entropies satisfy several chain rules. Some of them are stated below. A more complete list of chain rule relations can be found in [96, 115].

Properties 2 (Chain rules for the smooth min-entropy)**.** *The smooth min-entropy satisfy the following relations*

(i) For a quantum state ρ_{ABC},

$$H_{\min}^\epsilon(A|BC)_\rho \geq H_{\min}^{\frac{\epsilon}{4}}(AB|C)_\rho - H_{\max}^{\frac{\epsilon}{4}}(B|C)_\rho \tag{A.14}$$
$$- 2\log\left(1 - \sqrt{1 - \left(\frac{\epsilon}{4}\right)^2}\right).$$

(ii) *If X is a classical register and ρ_{ABX} a quantum-quantum-classical state, it holds that*††

$$H_{\min}^\epsilon(A|XB)_\rho \geq H_{\min}^\epsilon(A|B)_\rho - \log\left(\text{rank}(\rho_X)\right), \quad \text{(A.15)}$$

where $\text{rank}(\rho_X)$ *is the rank of state* ρ_X.

A fully contained overview with properties and relations between different entropies can be found in [96] (see also, [116]).

Appendix B. Security proof

According to Definition 5, a security proof of a DIQKD protocol consists in completeness and soundness. We start by proving completeness of Protocols 1 and 2.

Theorem 10 (Completeness)**.** *The DIQKD protocols in consideration, Protocols 1 and 2 are ϵ_{DIQKD}^c complete, with*

$$\epsilon_{DIQKD}^c \leq \epsilon_{EC}^c + \epsilon_{est} + \epsilon_{EC}. \quad \text{(B.1)}$$

Proof. The protocols in consideration can abort in two steps. Either because the error correction fail, or because the estimated Bell violation is not high enough. Let us consider an honest implementation consisting of IID rounds where the expected winning CHSH probability is ω_{exp}.

$$p(\text{abort}) = p((\text{EC abort}) \text{ or } (\text{EC does not abort and Bell test fail}))$$
$$\leq p(\text{EC abort}) + p(\text{EC does not abort and Bell test fail})$$

Now, the probability that the error correction protocol abort for an honest implementation is $p(\text{EC abort}) \leq \epsilon_{EC}^c$. And for the other term we have

$$p(\text{EC does not abort and Bell test fail})$$
$$= p(K_A = K_B)p(\sum_i C_i < \sum_i T_i \times (\omega_{exp} - \delta_{est})\,|K_A = K_B)$$
$$+ p(K_A \neq K_B)p(\sum_i C_i < \sum_i T_i \times (\omega_{exp} - \delta_{est})\,|K_A \neq K_B)$$
$$\leq \epsilon_{est} + \epsilon_{EC},$$

where $\epsilon_{est} = \mathrm{e}^{-2\gamma n(\delta_{est})^2}$ follows from Hoeffding's inequality. $\square$

For the soundness proof we have to evaluate correctness and secrecy, Definitions 1 and 2. For an error correction protocol with error parameter ϵ_{EC} we have that given that the error correction protocol does not abort, the probability that the string $\tilde{B}$ after error correction is equal to A_1^n with probability higher than $1 - \epsilon_{EC}$ and consequently

$$P(K_A \neq K_B) \leq \epsilon_{EC}. \quad \text{(B.2)}$$

††In [96] relation $H_{\min}^\epsilon(A|XB)_\rho \geq H_{\min}^\epsilon(A|B)_\rho - \log|X|$ was proved. Relation (A.15) with the rank of ρ_X follows as pointed out in Property 1.(iv).

For the secrecy let us recall that, for each considered Protocol, Ω is defined as the event that the respective protocols do not abort. That happens when the error correction protocol does not abort and they achieved the required violation of CHSH according to Bob's estimation of Alice's string. Now, let us the define the event $\hat{\Omega}$ as the event Ω of the Protocol not aborting **and** the error correction being successful, *i.e.* $\tilde{B}_1^n = A_1^n$. Now the quantity we need to estimate for the secrecy, relates to the event $\hat{\Omega}$ by

$$\left\|\rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_E\right\|_1 \leq \left\|\rho_{K_A E|\Omega} - \rho_{K_A E|\hat{\Omega}}\right\|_1 + \left\|\rho_{K_A E|\hat{\Omega}} - \tau_{K_A} \otimes \rho_E\right\|_1$$
$$\leq \epsilon_{EC} + \left\|\rho_{K_A E|\hat{\Omega}} - \tau_{K_A} \otimes \rho_E\right\|_1 \qquad \text{(B.3)}$$

which follows from the fact that, since when error correction succeeds, the probability of $\tilde{B}_1^n = A_1^n$ is higher than $(1 - \epsilon_{EC})$ then the following operator inequality holds: $\rho_{K_A E|\Omega} \geq (1 - \epsilon_{EC})\rho_{K_A E|\hat{\Omega}}$.

In the following, we proceed to evaluate $\left\|\rho_{K_A E|\hat{\Omega}} - \tau_{K_A} \otimes \rho_E\right\|_1$ in order to prove Theorems 1, 2 and 3.

Appendix B.1. Proof of Theorem 2

In this Appendix we present the proof of Theorem 2, that determines the size of a secret key one can extract from Protocol 2 under the assumption that the eavesdropper is restricted to collective attacks. Importantly, Theorem 2 is based on the asymptotic equipartition property, Theorem 7, in order to break the entropy of the n rounds into the one-round entropy.

The collective attacks assumption implies that in each round of the protocol the state distributed to Alice and Bob is the same, as well as their devices function in the same way, *i.e.* the rounds are independent and identically distributed (IID). Therefore the state shared between Alice, Bob and Eve after Alice and Bob measure their raw keys is described by a tensor product form $\rho_{ABE}^{\otimes n}$.

The asymptotic equipartition property (AEP) [60], Theorem 7, states that the smooth min-entropy of a tensor product of states is almost equivalent (up to terms of order of $\sqrt{n}$) to n times the von-Neumann entropy of an individual system. We now make use of the quantum AEP to derive the length of a secure key that one can achieve for Protocol 2.

As established by the leftover hashing lemma, Theorem 5, the maximal length of a secure key is determined by the smooth min-entropy of Alice's raw key conditioned on all information available to the eavesdropper, given that the protocol did not abort. In the case of Protocol 2, it is given by

$$H_{\min}^{\frac{\epsilon_s}{p(\hat{\Omega})}}(A_1^n | X_1^n Y_1^n T_1^n E O_{EC})_{\rho_{|\hat{\Omega}}}. \qquad \text{(B.4)}$$

Here we recall that O_{EC} is the information exchanged by Alice and Bob during the error correction protocol. T_1^n, X_1^n, Y_1^n are, respectively, the variable that determines whether the round is a test or a key generation round, and Alice and Bob's inputs, which are communicated publicly. $\hat{\Omega}$ is the event that error correction protocol succeeds, *i.e.*

$K_A = K_B$ and the CHSH probability estimated by Bob is $\omega \geq \omega_{exp} - \delta_{est}$. In the following we describe the steps to estimate (B.4).

Step 1: *Accounting for the leakage in the error correction.*

Using the chain rule relation for the smooth min-entropy conditioned on classical information, Property 2*(ii)*, we have

$$H_{\min}^{\frac{\epsilon_s}{P(\Omega)}}(A_1^n|X_1^nY_1^nT_1^nEO_{EC})_{\rho_{|\hat{\Omega}}} \geq H_{\min}^{\frac{\epsilon_s}{P(\Omega)}}(A_1^n|X_1^nY_1^nT_1^nE)_{\rho_{|\hat{\Omega}}} - \text{leak}_{EC}, \quad \text{(B.5)}$$

where $\text{leak}_{EC} = \text{rank}(\rho_{O_{EC}})$ represents the minimum amount of classical information that needs to be communicated from Alice to Bob in order to perform error correction†. We consider that Alice and Bob use a protocol based on universal hashing which has minimum leakage [117]. In [118] it was proved that the minimum leakage is given by

$$\text{leak}_{EC} \leq H_0^{\epsilon'_{EC}}(A_1^n|B_1^nX_1^nY_1^nT_1^n) + \log\left(\frac{1}{\epsilon_{EC}}\right), \quad \text{(B.6)}$$

where, if Alice and Bob do not abort, then $K_A = K_B$ with probability at least $1 - \epsilon_{EC}$. And for an honest implementation, the error correction protocol aborts with probability at most $\epsilon_{EC}^c = \epsilon'_{EC} + \epsilon_{EC}$. Here H_0 is a Rényi entropy first introduced in Ref. [48] (in Ref. [96], it is denoted $\bar{H}_0^{\uparrow}$). The entropy H_0^ϵ, relates to the smooth max-entropy in the following way [100, Lemma 18],

$$H_0^{\epsilon'_{EC}}(A_1^n|B_1^nX_1^nY_1^nT_1^n) \leq H_{\max}^{\frac{\epsilon'_{EC}}{2}}(A_1^n|B_1^nX_1^nY_1^nT_1^n) \quad \text{(B.7)}$$
$$+ \log\left(\frac{8}{\epsilon'^2_{EC}} + \frac{2}{2 - \epsilon'_{EC}}\right).$$

We now can use of the Asymptotic equipartition property, Theorem 7, to decompose (B.7) into the sum of the entropy of single rounds. Moreover, for an honest implementation with winning CHSH probability ω_{exp} and QBER Q we have that for the test rounds $H(A|BXYT = 1) = h(\omega_{exp})$ and for the key generation rounds $H(A|BXYT = 0) = h(Q)$. Therefore the one round entropy is given by

$$H(A|BXYT) = p(T = 0)H(A|BXYT = 0) + p(T = 1)H(A|BXYT = 1)$$
$$= (1 - \gamma)h(Q) + \gamma h(\omega_{exp}), \quad \text{(B.8)}$$

where in the first equality we have use Property 1*(v)*.

Therefore, the leakage due to error correction is given by

$$\text{leak}_{EC} \leq n((1 - \gamma)h(Q) + \gamma h(\omega_{exp})) + \sqrt{n}\left(4\log\left(2\sqrt{2} + 1\right)\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right)$$
$$+ \log\left(\frac{8}{\epsilon'^2_{EC}} + \frac{2}{2 - \epsilon'_{EC}}\right) + \log\left(\frac{1}{\epsilon_{EC}}\right). \quad \text{(B.9)}$$

† Note that in a realistic implementation Alice might send the error correction information using an encoding in order to overcome errors in the transmission due to channel losses. Therefore, in general $\rho_{O_{EC}}$ may not be full rank.

Step 2: *Breaking the entropy into single rounds.*

We now can use the asymptotic equipartition property in order to bound $H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(A_1^n|X_1^nY_1^nT_1^nE)_{\rho_{|\Omega}}$. The assumption of collective attacks implies that the state under consideration has the tensor product form and therefore

$$H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(A_1^n|X_1^nY_1^nT_1^nE)_{\rho_{|\hat\Omega}} \geq n\,H(A|XYTE)_{\rho_{|\hat\Omega}} - \sqrt{n}\delta(\epsilon_s,\eta), \qquad (\text{B.10})$$

where $\delta(\epsilon_s,\eta)$ and η are specified in Theorem 7.

For the scenario under consideration we have

$$\eta \leq 2\sqrt{2^{H_{\max}(A|XYTE)_\rho}} + 1 \leq 2\sqrt{2} + 1. \qquad (\text{B.11})$$

The first inequality follows from the fact that A is a classical register and therefore has positive conditional min-entropy, which implies $-H_{\min}(A|XYTE)_\rho \leq H_{\min}(A|XYTE)_\rho \leq H_{\max}(A|XYTE)_\rho$. The second inequality follows from the fact that since A is a binary variable $H_{\max}(A|XYTE)_\rho \leq 1$. Therefore,

$$\delta(\epsilon_s,\eta) \leq 4\log\left(2\sqrt{2}+1\right)\sqrt{\log\left(\frac{2}{\epsilon_s^2}\right)}. \qquad (\text{B.12})$$

Step 3: *Estimating the one-round entropy.*

Now it only remains to lower bound $H(A|XYTE)_{\rho_{|\hat\Omega}}$. Lemma 2 states the tight lower bound for the conditional von-Neumann entropy as a function of the winning probability ω for the CHSH game derived in [16, 39]. Using this bound we have that if ρ is a state that achieves winning probability ω then

$$H(A|XYTE)_{\rho_{|\hat\Omega}} \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega(\omega-1)+3}\right). \qquad (\text{B.13})$$

Now, Protocol 2 aborts if the observed frequency of winning events is smaller than $\omega_{exp} - \delta_{est}$. Therefore, given the event $\hat\Omega$ that Protocol 2 does not abort and $K_A = K_B$, we have that Alice and Bob observe a violation higher than $\omega_{exp} - \delta_{est}$. Now we need to take into account that the CHSH violation is estimated with a finite number of rounds. So in order to infer the real winning probability ω^* of the IID implementation, we can make use of the Hoeffding's inequality in order to define a confidence interval: If $\omega^* < \omega_{exp} - \delta_{est} - \delta_{con}$ then

$$Prob\left(\omega_{observed} \geq \omega_{exp} - \delta_{est}\right) \leq e^{-2\gamma n(\delta_{con})^2} := \epsilon_{con}. \qquad (\text{B.14})$$

Therefore, given that Alice and Bob do not abort the protocol, we infer that the expected winning probability of the system under consideration is higher than $\omega_{exp} - \delta_{est} - \delta_{con}$, and therefore

$$H(A|XYTE)_{\rho_{|\hat\Omega}} \geq \qquad (\text{B.15})$$
$$1 - h\left(\tfrac{1}{2} + \tfrac{1}{2}\sqrt{16(\omega_{exp} - \delta_{est} - \delta_{con})((\omega_{exp} - \delta_{est} - \delta_{con})-1)+3}\right).$$

Putting the results of these steps together we have that either Protocol 2 aborts with probability higher than $1 - (\epsilon_{con} + \epsilon_{EC})$, or the probability of aborting is smaller than $(\epsilon_{con} + \epsilon_{EC})$ and a $(2\epsilon_{EC} + \epsilon_s + \epsilon_{PA})$-correct-and-secret key can be generated of size

$$
\begin{aligned}
l \geq{} & n\Big[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16(\omega_{exp} - \delta_{est} - \delta_{con})((\omega_{exp} - \delta_{est} - \delta_{con}) - 1) + 3}\right) \\
& - (1 - \gamma)h(Q) - \gamma h(\omega_{exp})\Big] \\
& - \sqrt{n}\left(4\log\left(2\sqrt{2} + 1\right)\left(\sqrt{\log\frac{2}{\epsilon_s^2}} + \sqrt{\log\frac{8}{\epsilon_{EC}'^2}}\right)\right) \\
& - \log\left(\frac{8}{\epsilon_{EC}'^2} + \frac{2}{2 - \epsilon_{EC}'}\right) - \log\left(\frac{1}{\epsilon_{EC}}\right) - 2\log\left(\frac{1}{2\epsilon_{PA}}\right).
\end{aligned}
\tag{B.16}
$$

This establishes Theorem 2.

Appendix B.2. Proof of Theorem 3

We now present the proof of Theorem 3, that determines the size of a secret key one can extract from Protocol 2 for collective attacks, but differently from Theorem 2, we now use the additivity property of the 2-Rényi entropy, Lemma 1, in order to break the entropy of the string into the one-round entropy.

We are now interested in estimate the length of a secure key as established in Theorem 4, which is given by

$$
H_2^\uparrow(A_1^n|X_1^nY_1^nT_1^nEO_{EC})_{\rho_{|\hat{\Omega}}}.
\tag{B.17}
$$

As in Appendix B.1 we now present the steps that lead to the proof of Theorem 3.

Step 1: *Accounting for the leakage in the Error Correction.*

Using Property 1 *(v)*, we have

$$
H_2^\uparrow(A_1^n|X_1^nY_1^nT_1^nEO_{EC})_{\rho_{|\hat{\Omega}}} \geq H_2^\uparrow(A_1^n|X_1^nY_1^nT_1^nE)_{\rho_{|\hat{\Omega}}} - \text{leak}_{EC},
\tag{B.18}
$$

where $\text{leak}_{EC} = \text{rank}(\rho_{O_{EC}})$ represents the minimum amount of classical information that needs to be communicated from Alice to Bob in order to perform error correction.

Now the error correction leakage leak_{EC} is the same as derived in Equation (B.9).

Step 2: *Breaking the entropy into single rounds.*

We can now make use of the additivity property of 2-Réyni entropy, Lemma 1, in order to bound $H_2^\uparrow(A_1^n|X_1^nY_1^nT_1^nE)_{\rho_{|\hat{\Omega}}}$. The assumption of collective attacks implies that the state under consideration has the tensor product form and therefore

$$
H_2^\uparrow(A_1^n|X_1^nY_1^nT_1^nE)_{\rho_{|\hat{\Omega}}} \geq n\, H_2(A|XYTE)_{\rho_{|\hat{\Omega}}},
\tag{B.19}
$$

where now the single round entropy in consideration is the conditional collision entropy.

Step 3: *Estimating the one-round entropy.*

Now it only remains to lower bound $H_2(A|XYTE)_{\rho_{|\hat{\Omega}}}$. Theorem 9 shows that a tight lower bound for the conditional collision entropy as a function of the violation β coincides with the previously derived conditional min-entropy [103], eq.(36). In terms of the winning probability ω for the CHSH game we have

$$H_2(A|XYTE)_{\rho_{|\hat{\Omega}}} \geq -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega(1-\omega) - 2}\right). \tag{B.20}$$

Again, given that Alice and Bob do not abort the protocol, we infer that the expected winning probability of the system under consideration is higher than $\omega_{exp} - \delta_{est} - \delta_{con}$, and

$$H_2(A|XYTE)_{\rho_{|\hat{\Omega}}} \geq \tag{B.21}$$

$$-\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{16(\omega_{exp} - \delta_{est} - \delta_{con})(1 - (\omega_{exp} - \delta_{est} - \delta_{con})) - 2}\right)$$

In conclusion we have that, either Protocol 2 aborts with probability higher than $1 - (\epsilon_{con} + \epsilon_{EC})$, or the probability of not aborting is greater than $(\epsilon_{con} + \epsilon_{EC})$ and a $(2\epsilon_{EC} + \epsilon_{PA})$-correct-and-secret key is generated of size:

$$l \geq n\left[-\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{16(\omega_{exp} - \delta_{est} - \delta_{con})(1 - (\omega_{exp} - \delta_{est} - \delta_{con})) - 2}\right)\right.$$
$$\left. - (1-\gamma)h(Q) - \gamma h(\omega_{exp})\right] \tag{B.22}$$
$$-\sqrt{n}\left(4\log\left(2\sqrt{2} + 1\right)\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right)$$
$$-\log\left(\frac{8}{\epsilon'^2_{EC}} + \frac{2}{2 - \epsilon'_{EC}}\right) - \log\left(\frac{1}{\epsilon_{EC}}\right) - 2\log\left(\frac{1}{2\epsilon_{PA}}\right).$$

This establishes Theorem 3.

Appendix B.3. Proof of Theorem 1

In this Appendix we present the proof of Theorem 1, which establishes the size of a secure key that can be extracted from Protocol 1 for general coherent attacks. We follow closely the proof developed in [1, 39].

In Protocol 1, the number of rounds is not fixed. Instead, Protocol 1 has a fixed number of blocks m, such that the maximum number of rounds inside a block is set to $s_{max} = \lceil\frac{1}{\gamma}\rceil$. This is a technicality introduced in [1,39] in order to get a better pre-factor for the overhead terms that scale with $\sqrt{n}$. For each block j Alice and Bob run the protocol until they have a test round or they reach the maximum number of rounds s_{max}. At each round j_i Alice and Bob choose a random bit T_{j_i}, such that $P(T_{j_i} = 1) = \gamma$, which determines whether they are going to test the CHSH inequality or make a key generation round. They repeat the process until they obtain $T_{j_i} = 1$ or $i = s_{max}$. With these constraints the expected number of rounds in a block is given by

$$\bar{s} = \frac{1 - (1-\gamma)^{\lceil\frac{1}{\gamma}\rceil}}{\gamma}, \tag{B.23}$$

and the expected number of rounds is

$$n = m\bar{s}. \tag{B.24}$$

For details on the derivation of equations (B.23) and (B.24) see Ref. [39, Appendix B]

We now proceed to derive the key rates against a general coherent attack. In order to calculate the size of the key we need to estimate

$$H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m EO)_{\rho_{|\hat{\Omega}}}. \tag{B.25}$$

Now $\vec{A}_1^m$ denotes the total string of bits, expected to be of size n, and $\vec{A}_i$ denotes the string of outputs generated in the block i, and similarly for the other variables. In the following, we proceed step by step in order to lower bound $H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m EO)_{\rho_{|\hat{\Omega}}}$ and we detail the changes introduced to the original analysis [1, 39].

Step 1: *Accounting for the leakage in the error correction.*

Similar to the proof of Protocol 2, we have that

$$H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m EO)_{\rho_{|\hat{\Omega}}} \geq H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} - \text{leak}_{EC}, \tag{B.26}$$

and

$$\text{leak}_{EC} \leq H_0^{\epsilon'_{EC}}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m) + \log\left(\frac{1}{\epsilon_{EC}}\right) \tag{B.27}$$

$$\leq H_{\max}^{\frac{\epsilon'_{EC}}{2}}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m) \tag{B.28}$$

$$+ \log\left(\frac{8}{\epsilon'_{EC}{}^2} + \frac{2}{(2-\epsilon'_{EC})}\right) + \log\left(\frac{1}{\epsilon_{EC}}\right).$$

However, now we need to take into account for the fact that the number of rounds in the protocol is not fixed. Following the steps of Ref. [39], we first note that the number of rounds N obtained in an implementation of the Protocol 1 satisfies:

$$P[N \geq n + t] \leq \exp\left(-\frac{2t^2\gamma^2}{m(1-\gamma)^2}\right) := \epsilon_t, \tag{B.29}$$

where $n = m\bar{s}$ is the expected number of rounds and $t = \sqrt{-\frac{m(1-\gamma)^2 \log \epsilon_t}{2\gamma^2}}$. Moreover, by the definition of smooth max-entropy one have that

$$H_{\max}^{\epsilon}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m N) \leq H_{\max}^{\epsilon-\sqrt{\epsilon_t}}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m N \leq n + t). \tag{B.30}$$

Note that N can be included in the entropy since it is completely determined by $\vec{T}_1^m$.

Now applying the asymptotic equipartition property, Theorem 7, to the maximal length $N = n + t$ we have

$$\text{leak}_{EC} \leq (\bar{n} + t) \cdot [(1-\gamma)h(Q) + \gamma h(\omega_{exp})]$$

$$+ \sqrt{\bar{n}+t}\,\nu_2 + \log\left(\frac{8}{\epsilon'_{EC}{}^2} + \frac{2}{(2-\epsilon'_{EC})}\right) + \log\left(\frac{1}{\epsilon_{EC}}\right),$$

where $\nu_2 = 4\log\left(2\sqrt{2}+1\right)\sqrt{2\log\left(\frac{8}{\left(\epsilon'_{EC}-2\sqrt{\epsilon_t}\right)^2}\right)}$ and ϵ_t is a free parameter to be optimised.

If the error correction protocol does not abort, then

$$P(K_A \neq K_B) \leq \epsilon_{EC}. \tag{B.31}$$

And the completeness of the error correction protocol (*i.e.*, the probability of not aborting in an honest IID implementation) is given by $\epsilon_{EC}^c = \epsilon_{EC}' + \epsilon_{EC}$.

Step 2: *Chain rule.*

In Protocol 1, a statistical test is performed on the variable C_i which accounts for the condition of winning the CHSH game being satisfied or not. In order to use the entropy accumulation theorem, we need to be able to infer the value of this variable C_i from the variables that appear in the smooth min-entropy we are calculating.

Here we choose to use a chain rule, relation (A.14), with the variable C_i itself, as opposed to using the variable B_i as is done in [39]. The reason is that the dimension of the variable C_i is smaller than B_i, as for each block the variable C_i assumes one out of three values. This leads to a slight improvement in rates achieved in the finite regime:

$$H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m | \vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \geq H_{\min}^{\frac{\epsilon_s}{4p(\Omega)}}(\vec{A}_1^m C_1^m | \vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$$
$$- H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m | \vec{A}_1^m \vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \tag{B.32}$$
$$- 3\log\left(1 - \sqrt{1 - \left(\frac{\epsilon_s}{4p(\Omega)}\right)^2}\right)$$
$$\geq H_{\min}^{\frac{\epsilon_s}{4p(\Omega)}}(\vec{A}_1^m C_1^m | \vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$$
$$- H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m | \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \tag{B.33}$$
$$- 3\log\left(1 - \sqrt{1 - \left(\frac{\epsilon_s}{4(\epsilon_{EA} + \epsilon_{EC})}\right)^2}\right).$$

In inequality (B.33) we use the fact that $p(\Omega) \geq (\epsilon_{EA} + \epsilon_{EC})$ and that removing the conditioning on classical variables can only increase the entropy, which can be seen as a particular case of data processing, Property 1 *(i)*.

Step 3: *Upper bound on $H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m | \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$.*

We can use the entropy accumulation theorem to upper bound $H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m | \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$. In order to do that we only have to find a max-tradeoff function for a protocol with m rounds. We have that for any distribution $\vec{p} = (p(1), p(0), p(\perp))$ of the variable C:

$$H(C_i | \vec{T}_i E)_{\rho_{|\hat{\Omega}}} = p(\vec{T}_i = \vec{0}) H(C_i | \vec{T}_i = \vec{0} E)_{\rho_{|\hat{\Omega}}} \tag{B.34}$$
$$+ p(\vec{T}_i \neq \vec{0}) H(C_i | \vec{T}_i \neq \vec{0} E)_{\rho_{|\hat{\Omega}}}$$
$$= p(\vec{T}_i \neq \vec{0}) H(C_i | \vec{T}_i \neq \vec{0} E)_{\rho_{|\hat{\Omega}}} \tag{B.35}$$
$$\leq h\left(\frac{p(1)}{1 - p(\perp)}\right) = h\left(\frac{p(1)}{1 - (1-\gamma)^{s_{\max}}}\right) = h(\omega), \tag{B.36}$$

where in (B.35) we use the fact that $H(C_i|\vec{T}_i = \vec{0}E) = 0$, and in (B.36) we use that $p(\vec{T}_i \neq \vec{0}) \leq 1$ and that $\frac{p(1)}{1-(1-\gamma)^{s_{\max}}} \equiv \omega$. Note that $h(\cdot)$ is a concave function.

Now we can take $f_{\max} = h(\omega_{exp} - \delta_{est})$ and $\|\nabla f_{\max}\|_\infty = \frac{1}{1-(1-\gamma)^{s_{\max}}} \times \frac{\partial h}{\partial \omega}\Big|_{\omega_{exp}-\delta_{est}}$, where ω_{exp} is the expected winning probability of the CHSH game in an honest implementation and δ_{est} accounts for the statistical confidence interval of the experiment. Using the entropy accumulation theorem, Theorem 8, we have

$$H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m|\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \leq m\, h(\omega_{exp} - \delta_{est}) + \sqrt{m}\, \nu_1 \tag{B.37}$$

where

$$\nu_1 = 2\left(\log 7 + \left\lceil \frac{|h'(\omega_{exp} + \delta_{est})|}{1-(1-\gamma)^{s_{\max}}} \right\rceil\right)\sqrt{1 - 2\log \epsilon_s}, \tag{B.38}$$

and h' represents the derivative of the binary entropy function, $\frac{\partial h(\omega)}{\partial \omega}$.

Step 4: *Lower bound on* $H_{min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m C_1^m|\vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$.

Finally, we apply the entropy accumulation theorem to lower bound the term $H_{min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m C_1^m|\vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$. Therefore we need to find a min-tradeoff function such that

$$f_{\min}(\vec{q}) \leq \inf_{\sigma_{R_{j-1}E}:\mathcal{M}_j(\sigma)_{C_j}=\vec{q}} H(\vec{A}_j C_j|\vec{X}_j \vec{Y}_j \vec{T}_j E)_{\mathcal{M}_j(\sigma)} \tag{B.39}$$

Note that the length of each block is variable. However, we can consider that all the blocks have size $s_{\max}$ and set all the variables to $\perp$ for the rounds which are not performed.

First note that

$$H(\vec{A}_j C_j|\vec{X}_j \vec{Y}_j \vec{T}_j E) \geq H(\vec{A}_j|\vec{X}_j \vec{Y}_j \vec{T}_j E). \tag{B.40}$$

And from now on, we follow the same steps as Ref. [39].

Using the chain-rule for Von Neuman, Property 1(v), entropy we have

$$H(\vec{A}_j|\vec{X}_j \vec{Y}_j \vec{T}_j E) = \sum_{i=1}^{s_{\max}} H(A_{j,i}|\vec{X}_j \vec{Y}_j \vec{T}_j E A_{j_1}^{i-1}). \tag{B.41}$$

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

$$H(A_{j,i}|\vec{X}_j \vec{Y}_j \vec{T}_j E A_{j_1}^{i-1}) =$$
$$= p(T_{j_1}^{i-1} = \vec{0})H(A_{j,i}|\vec{X}_j \vec{Y}_j E A_{j_1}^{i-1} T_{j_i}^{s_{\max}}, T_{j_1}^{i-1} = \vec{0}) \tag{B.42}$$
$$+ p(T_{j_1}^{i-1} \neq \vec{0})H(A_{j,i}|\vec{X}_j \vec{Y}_j E A_{j_1}^{i-1} T_{j_i}^{s_{\max}}, T_{j_1}^{i-1} \neq \vec{0})$$
$$= (1-\gamma)^{(i-1)}H(A_{j,i}|\vec{X}_j \vec{Y}_j E A_{j_1}^{i-1} T_{j_i}^{s_{\max}}, T_{j_1}^{i-1} = \vec{0}), \tag{B.43}$$

where we used the fact that $H(A_{j,i}|\vec{X}_j \vec{Y}_j E A_{j_1}^{i-1} T_{j_i}^{s_{\max}}, T_{j_1}^{i-1} \neq \vec{0}) = 0$. Therefore

$$H(\vec{A}_j|\vec{X}_j \vec{Y}_j \vec{T}_j E) = \tag{B.44}$$
$$\sum_{i=1}^{s_{max}} (1-\gamma)^{(i-1)}H(A_{j,i}|\vec{X}_j \vec{Y}_j E A_{j_1}^{i-1} T_{j_i}^{s_{\max}}, T_{j_1}^{i-1} = \vec{0}).$$

Each term $H(A_{j,i}|\vec{X}_j\vec{Y}_jEA_{j1}^{i-1}T_{j_i}^{s_{\max}}, T_{j1}^{i-1} = \vec{0})$ can be seen as the entropy of a single round. An expression for the entropy of a single round was derived for collective attacks in [16]. This gives us:

$$H(\vec{A}_jC_j|\vec{X}_j\vec{Y}_j\vec{T}_jE) = \tag{B.45}$$
$$\sum_{i=1}^{s_{max}} (1-\gamma)^{(i-1)} \left[1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega_i(\omega_i-1)+3} \right) \right]$$

such that

$$p(1) = \sum_{i=1}^{s_{max}} \gamma(1-\gamma)^{(i-1)}\omega_i. \tag{B.46}$$

Now, in [39] it is proved that the minimum of (B.45) is achieved for

$$\omega_i^* = \frac{p(1)}{1-(1-\gamma)^{s_{\max}}} \quad \forall i, \tag{B.47}$$

and therefore we have a min-tradeoff function:

$$g(\vec{p}) = s\left[1 - h\left(\tfrac{1}{2} + \tfrac{1}{2}\sqrt{16\tfrac{p(1)}{1-(1-\gamma)^{s_{max}}}\left(\tfrac{p(1)}{1-(1-\gamma)^{s_{max}}} - 1 \right) + 3} \right) \right]; \tag{B.48}$$

for $\frac{p(1)}{1-(1-\gamma)^{s_{max}}} \in \left[\frac{3}{4}, \frac{2+\sqrt{2}}{4} \right]$.

Note that as $p(1) \to ((1-(1-\gamma)^{s_{\max}})\frac{2+\sqrt{2}}{4}$, the gradient of $g(\vec{p})$ tends to infinity, which compromises the $\sqrt{n}$ term that depends on the norm of the gradient of f. Since $g(\vec{p})$ is a convex function, the tangent line in any point $\vec{p}_t$ is a lower bound to $g(\vec{p})$. Therefore, as in [1, 39], we take the min-tradeoff function to be a tangent g in a point $\vec{p}_t$ to be optimized†:

$$F_{\min}(p, p_t) = \frac{d}{dp(1)}g(p)\Big|_{\tilde{p}_t} \cdot p(1) + \left(g(p_t) - \frac{d}{dp(1)}g(p)\Big|_{p_t} \cdot p_t(1) \right). \tag{B.49}$$

Then we have

$$H_{min}^{\frac{\epsilon_s}{4p(\Omega)}}(\vec{A}_1^mC_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^mE)_{\rho_{|\hat{\Omega}}} > m \cdot \eta_{opt} = \frac{\bar{n}}{\bar{s}} \cdot \eta_{opt}, \tag{B.50}$$

where

$$\eta_{opt} = \max_{\frac{3}{4} < \frac{\tilde{p}_t(1)}{1-(1-\gamma)^{s_{max}}} < \frac{2+\sqrt{2}}{4}} \left[F_{\min}(\tilde{p}, \tilde{p}_t) - \frac{1}{\sqrt{m}}\nu_3 \right], \tag{B.51}$$

such that

$$\nu_3 = 2\left(\log\left(1 + 2\cdot 2^{s_{\max}}3\right) + \left\lceil \frac{d}{dp(1)}g(\tilde{p})\big|_{p_t} \right\rceil \right)\sqrt{1 - 2\log\epsilon_s}. \tag{B.52}$$

† In [1, 39] the authors consider the following min-tradeoff function

$$f_{\min}(\vec{p}) = \begin{cases} g(\vec{p}) & \text{if } p_t(1) > p(1) \\ F_{\min}(\vec{p}, \vec{p}_t) = & \text{if } p_t(1) \le p(1) \end{cases}.$$

We remark that, since the gradient of $g(\vec{p})$ is an increasing function of $p(1)$, the optimum value for η_{opt} is always achieved for $p_t(1) \le p(1)$.

Finally, the length of a secure key that can be extracted is given by

$$
\begin{aligned}
l \geq{} & \frac{\bar{n}}{\bar{s}}\eta_{opt} - \frac{\bar{n}}{\bar{s}}h(\omega_{exp} - \delta_{est}) - \sqrt{\frac{\bar{n}}{\bar{s}}}\nu_1 \\
& - (\bar{n} + t) \cdot [(1 - \gamma)h(Q) + \gamma h(\omega_{exp})] \\
& - \sqrt{\bar{n} + t}\,\nu_2 - \log\left(\frac{8}{\epsilon'_{EC}{}^2} + \frac{2}{(2 - \epsilon'_{EC})}\right) - \log\left(\frac{1}{\epsilon_{EC}}\right) \\
& - 3\log\left(1 - \sqrt{1 - \left(\frac{\epsilon_s}{4}\right)^2}\right) - 2\log\left(\frac{1}{2\epsilon_{PA}}\right).
\end{aligned}
\tag{B.53}
$$

Appendix C. Proof of Theorem 9

Theorem 9. *There exist a state ρ^*_{AB} and measurements for Alice and Bob such that, ρ^*_{AB} achieves violation β and the collision entropy of Alice's output A conditioned on Eve's quantum information E is*

$$
H_2(A|E)_{\rho^*} = -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{\beta^2}{4}}\right). \tag{C.1}
$$

Proof. The proof consists in exhibiting a state ρ^*_{AB} and measurements for Alice and Bob such that the lower bound given by eq.(36) is saturated. Our derivation is based on the techniques presented in Ref. [16], which led to a tight lower bound for the conditional von-Neumann entropy.

Let us consider that Alice and Bob share a Bell diagonal state ρ_{AB}

$$
\rho_{AB} = \lambda_{00}\Phi_{00} + \lambda_{01}\Phi_{01} + \lambda_{10}\Phi_{10} + \lambda_{11}\Phi_{11} \tag{C.2}
$$

where $\Phi_{ij} = |\Phi_{ij}\rangle\langle\Phi_{ij}|$ and $|\Phi_{ij}\rangle = I \otimes X^i Z^j \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$. We first prove the following result:

Lemma 3. *For a Bell-diagonal state where Alice performs a measurement in the Z-basis we have that*

$$
H_2(A|XYE)_\rho \geq -\log\left(\frac{1}{2} + \sqrt{\lambda_{00}\lambda_{01}} + \sqrt{\lambda_{11}\lambda_{10}}\right). \tag{C.3}
$$

Proof. Given a Bell diagonal state $\rho_{AB}(\lambda_{00}, \lambda_{01}, \lambda_{10}, \lambda_{11})$, a purification $|\Psi\rangle_{ABE}$ of this state is given by

$$
\begin{aligned}
|\Psi\rangle_{ABE} ={} & \sqrt{\lambda_{00}}\,|\Phi_{00}\rangle_{AB}\,|e_1\rangle_E + \sqrt{\lambda_{01}}\,|\Phi_{01}\rangle_{AB}\,|e_2\rangle_E \\
& + \sqrt{\lambda_{10}}\,|\Phi_{10}\rangle_{AB}\,|e_3\rangle_E + \sqrt{\lambda_{11}}\,|\Phi_{11}\rangle_{AB}\,|e_4\rangle_E.
\end{aligned}
\tag{C.4}
$$

After Alice measures in the Z basis we have

$$
\rho_{AE} = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_{E|0} + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_{E|1} \tag{C.5}
$$

where

$$
\rho_{E|0} = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| \quad \text{and} \quad \rho_{E|1} = |\psi_3\rangle\langle\psi_3| + |\psi_4\rangle\langle\psi_4|, \tag{C.6}
$$

with non-normalized states

$$|\psi_1\rangle = \left(\sqrt{\lambda_{00}}\,|e_1\rangle + \sqrt{\lambda_{01}}\,|e_2\rangle\right),$$

$$|\psi_2\rangle = \left(\sqrt{\lambda_{10}}\,|e_3\rangle + \sqrt{\lambda_{11}}\,|e_4\rangle\right),$$

$$|\psi_3\rangle = \left(\sqrt{\lambda_{10}}\,|e_3\rangle - \sqrt{\lambda_{11}}\,|e_4\rangle\right),$$

$$|\psi_4\rangle = \left(\sqrt{\lambda_{00}}\,|e_1\rangle - \sqrt{\lambda_{01}}\,|e_2\rangle\right).$$

The collision entropy of a cq-state ρ_{AE} is given by

$$H_2(A|E)_\rho = -\log \operatorname{Tr}\left(\rho_E^{-1/2}\rho_{AE}\rho_E^{-1/2}\rho_{AE}\right), \tag{C.7}$$

which, evaluated for the state (C.5) gives

$$H_2(A|E)_\rho = -\log\left(\frac{1}{2} + \left(\sqrt{\lambda_{00}}\sqrt{\lambda_{01}} + \sqrt{\lambda_{10}}\sqrt{\lambda_{11}}\right)\right).$$

$\square$

Now let us consider a Bell diagonal state ρ_{AB}^* such that

$$\lambda_{00} = R\cos\theta, \quad \lambda_{01} = R\sin\theta, \quad \lambda_{10} = \lambda_{11} = 0, \tag{C.8}$$

$$\text{s.t.} \quad \cos\theta + \sin\theta = \frac{1}{R}$$

which can hold for $R > \frac{1}{\sqrt{2}}$. This choice is inspired by the optimal strategy that maximizes the conditional von Neumann entropy as shown in [16].

For these parameters we have that

$$H_2(A|XYE)_{\rho^*} \geq -\log\left(\frac{1}{2} + R\sqrt{\frac{1}{2}\left(\frac{1}{R^2} - 1\right)}\right) \tag{C.9}$$

Finally, we know from [119] that for a state $\rho_{AB}(\lambda_{00}, \lambda_{01}, \lambda_{10}, \lambda_{11})$, the maximal violation $\beta_{\max}$ of the CHSH inequality is given by

$$\beta_{\max} = \max\left\{2\sqrt{2}\sqrt{(\lambda_{00} - \lambda_{11})^2 + (\lambda_{01} - \lambda_{10})^2},\right. \tag{C.10}$$

$$\left.2\sqrt{2}\sqrt{(\lambda_{00} - \lambda_{10})^2 + (\lambda_{01} - \lambda_{11})^2}\right\}$$

and that this violation can be achieved with one of Alice's measurement being in the Z basis.

Therefore, for the state ρ_{AB}^*, specified by (C.8), and Alice and Bob performing the measurements that gives the maximum violation achievable for the CHSH inequality, we have that $\beta = 2\sqrt{2}R$. This implies

$$H_2(A|XYE)_{\rho^*} = -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{\beta}{4}}\right). \tag{C.11}$$

$\square$