Device-independent quantum key distribution based on routed Bell tests

Tristan Le Roy-Deloison, Edwin Peter Lobo, Jef Pauwels, Stefano Pironio

Device-independent quantum key distribution based on routed Bell tests

Tristan Le Roy-Deloison[1,2], Edwin Peter Lobo[3], Jef Pauwels[4,5], and Stefano Pironio[3]

[1]Univ Lyon, Inria, ENS Lyon, UCBL, LIP, Lyon, France
[2]Télécom Paris-LTCI, Institut Polytechnique de Paris, Palaiseau, France
[3]Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Belgium
[4]Department of Applied Physics, University of Geneva, 1211 Geneva, Switzerland
[5]Constructor University, 1211 Geneva, Switzerland

April 1, 2023

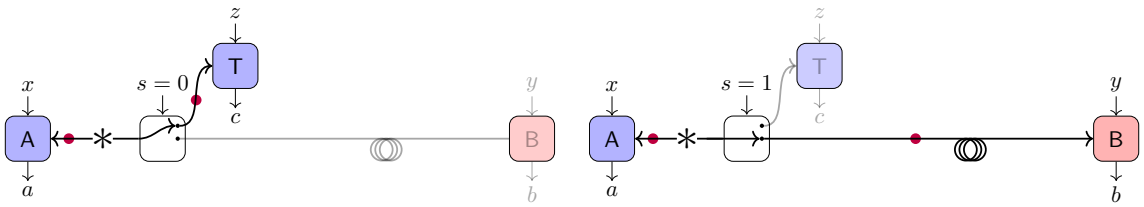
Photon losses are the main obstacle to fully photonic implementations of device-independent quantum key distribution (DIQKD). Motivated by recent work showing that routed Bell scenarios offer increased robustness to detection inefficiencies for the certification of long-range quantum correlations, we investigate DIQKD protocols based on a routed setup. In these protocols, in some of the test rounds, photons from the source are routed by an actively controlled switch to a nearby test device instead of the distant one. We show how to analyze the security of these protocols and compute lower bounds on the key rates using non-commutative polynomial optimization and the Brown-Fawzi-Fazwi method. We determine lower bounds on the asymptotic key rates of several simple two-qubit routed DIQKD protocols based on CHSH or BB84 correlations and compare their performance to standard protocols. We find that in an ideal case routed DIQKD protocols can significantly improve detection efficiency requirements, by up to $\sim 30\%$, compared to their non-routed counterparts. Notably, the routed BB84 protocol achieves a positive key rate with a detection efficiency as low as 50% for the distant device, the minimal threshold for any QKD protocol featuring two untrusted measurements. However, the advantages we find are highly sensitive to noise and losses affecting the short-range correlations involving the additional test device.

1 Introduction

A prerequisite for device-independence quantum information protocols is the ability to certify genuine quantum correlations between the devices involved [ABG+07, BCP+14]. In practice, this requires the ability to perform Bell tests free of the detection loophole [Pea70, CH74, GM87], i.e., to detect quantum particles with a high enough efficiency. In full photonic implementations, this is one of the main obstacles to overcome because of unavoidable losses in the quantum optical channel. In particular, the distance record for full photonic loophole-free Bell tests is of the order of 200 m [SZB+21, LZL+21, LLR+21]. This is far from the distances required for practical applications.

One possible way to overcome optical losses and reach high enough detection efficiencies is to use an 'event-ready' scheme [BA04], where the presence of entanglement between the two remote devices is heralded before they perform their measurements. This may be achieved through entanglement swapping [ZZHE93, SSC+11, CM11], quantum amplifier [GPS10], local precertification of the photons [CS12] or full quantum repeaters [AEE+23]. In each case, this requires additional sources of quantum particles and/or joint measurements, substantially increasing the implementation complexity.

Recently, the idea of routed Bell tests has been proposed [CVP24, LPP23] as a simple modification to standard Bell tests that can reduce the detection efficiency required for loophole-free experiments, hence extend the distance over which quantum correlations can be certified. The



(a) Bob's particle is routed to the closeby device when $s = 0$.

(b) Bob's particle is routed to the distant device when $s = 1$.

Figure 1: The routed Bell scenario.

basic idea behind a routed Bell test is depicted in Fig. 1. As in a standard Bell test, it features a measurement device A for Alice, a measurement device B for Bob, and a source of entangled particles. In each experimental trial, Alice and Bob can operate their devices independently, submitting random inputs x and y, respectively, (the measurement settings), and obtaining classical outputs a and b. However, in the routed configuration, an additional element is introduced: the possibility for Bob's particle to be routed via a switch to a different measurement device than B. We denote this additional device T and its corresponding input and output z and c. The switch is controlled by a classical input s, which determines whether Bob's particle is routed to T or B. E.g., $s = 0$ routes it to T and $s = 1$ routes it to B. Depending on the switch setting s, one can thus either perform a Bell test in the A/T configuration or the A/B configuration. The purpose of the A/T test is to certify, as best as possible, the quantum behavior of the particle source and of the device A. To minimize losses in these tests, and reach a high Bell violation, the devices A and T are thus situated close to the source of entangled particles. Performing a Bell test with the A/T setup for a randomly selected subset of the trials will then ensure that Alice's device A behaves (almost) honestly, even when it is part of the long-distance A/B test. This limits how A can collude with B to simulate genuine quantum correlations, thereby lowering the detection efficiency threshold required to authenticate such correlations in the A/B configuration.

As in standard DIQKD, all components of the setup, including the switch and the additional measurement device T are untrusted and their internal functioning is uncharacterized. The only assumption made on the devices is that they obey certain no-signaling constraints preventing them from signaling arbitrarily to each other. Specifically, the behavior of the devices on Alice's side of the entangled source should not influence the devices on Bob's side, and vice versa. Thus, in a given trial, the classical input x and output a on Alice's side should not influence Bob's particle and the measurements performed at T or B. Similarly, the classical inputs and outputs s, z, c, y and b on Bob's side should not influence Alice's quantum particle or the measurement performed at A. This last condition is crucial to ensure that the source and the measurement device A behave identically whether Bob's particle is routed to B or T. This is necessary to ensure that the A/T tests are a reliable indicator of the behavior of A also in the A/B configuration.

In [LPP23], criteria and tools are introduced to certify long-range quantum correlations between A and B, given that certain correlations are observed in the short-range A/T test. Though the required detection efficiency at B can be lowered compared to standard Bell tests which lack the intermediate A/T test, the improvements are modest.

Nevertheless, the routed Bell scenario exhibits features that could be of interest to DIQKD. For instance, the BB84 correlations, which are emblematic in QKD, and can be produced from a maximally two-qubit state $|\phi_+\rangle$ by carrying out σ_z and σ_x Pauli measurements at A and B, can be replicated classically in a standard Bell setup, hence are unsuitable for standard DIQKD. However, their quantum nature can be certified in a routed Bell experiment by performing random CHSH tests in the A/T configuration, with the testing device T using the CHSH bases $(\sigma_z \pm \sigma_x)/\sqrt{2}$ [LPP23]. Furthermore, when the short-distance A/T test achieves the maximal CHSH value, the detection efficiency threshold for the device B is 50%, the minimal one for a two-measurement device [MP03].

Alice's measurements at A can also be seen as remotely preparing states for Bob's device B. The A/T tests within a routed Bell framework self-test the entangled particle source and Alice's device A, hence they self-test those remotely prepared states. When this self-test is perfect, these

remotely prepared states are fully characterized. Hence, the additional measurements made at T effectively turn a DIQKD protocol into a one-sided DI prepare-and-measure QKD protocol, which is typically more efficient and noise-robust.

The above observations, and the relative simplicity of implementing routed Bell tests, motivate the study of their applications to DIQKD, both for improving the experimental prospects for DIQKD and our conceptual interest. In the present paper, we introduce simple DIQKD protocols based on routed Bell tests and show how lower bounds on the key rates can be computed numerically using non-commutative polynomial optimization (NPO) [NPA07, NPA08, PNA10] and the BFF method [BFF21a]. We determine such lower bounds for several simple routed DIQKD (rDIQKD) protocols and compare their performance to standard DIQKD protocols.

2 Routed DIQKD

2.1 Setup

The rDIQKD protocols that we introduce are based on the routed Bell configuration, represented in Fig. 1 and succinctly described in the Introduction. As in standard DIQKD, we assume that Alice and Bob are in safe laboratories and that they each operate independently the untrusted measurement devices A and B, respectively. In most of the rounds, the outputs of these devices are kept secret and will constitute the raw key. In the remaining rounds, the outputs are publicly announced and contribute to statistical data collection for parameter estimation.

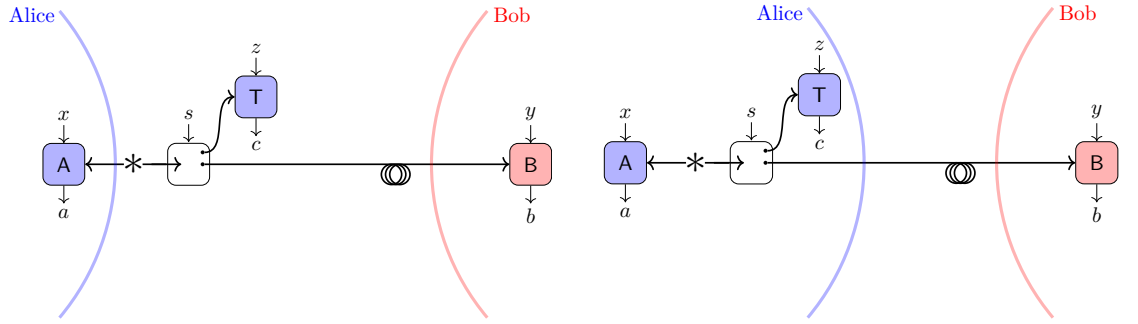
Part of the time, Bob's particle is also randomly routed to the testing device T instead of B. The outputs of such rounds are never used to generate a key but always contribute to parameter estimation. As regards the location of the device T, as well as of the entangled source and the switch, there are then two possibilities.

The first, depicted in Fig. 2a, is to consider them as being outside Alice's and Bob's laboratories and in full control of the eavesdropper, similar to the entangled source in standard entanglement-based QKD or the joint measurement in measurement-device-independent QKD. We can then think[1] of, say, Alice as providing through public announcements the classical inputs s and z, and the device T as answering back with a publicly announced classical output c. The difficulty with this setup is that we should ensure that, upon learning s or z, the eavesdropper does not modify Alice's quantum state before it enters her laboratory and her measurement is completed, as this would violate the no-signaling requirements discussed in the Introduction. In principle, Alice could announce the value of s or z after her measurement is completed and she has recorded her output a. However, this would require delaying the operation of the switch until that moment, which in practice would require the use of a quantum memory to store the quantum state until the announcement is made. This is a significant experimental complication.

The other option is to assume that the switch and the device T are all situated in Alice's laboratory, as depicted in Fig. 2b, and that these devices cannot arbitrarily communicate their private inputs to Alice's device A. This is a customary assumption in DI quantum cryptography [PAM+10], which can, e.g., be enforced through shielding of the devices. This is a setup that amounts effectively to viewing Alice as holding a measurement-based preparation device that prepares quantum states that are sent to Bob on an untrusted public quantum channel; part of the time, these states are not sent by Alice on the public channel but are instead locally measured by T in her laboratory to verify their quantum properties. We stress that even though in this setup we assume that we can control and restrict the classical and quantum communication that goes in and out of the devices involved in the protocol, they are all still viewed as black boxes whose internal functioning is untrusted.

Though it is more natural to think of rDIQKD as implemented in the setup of Fig. 2b, we will analyze in the following its security in the setup of Fig. 2a, where Eve can freely control and access

[1]The alternative possibility of incorporating a trusted intermediary between A and B to supply random inputs to the switch and device T departs from our focus, which is on direct, secure communication between Alice and Bob. Furthermore extending QKD at a large distance through third-party trusted intermediaries is always possible, but opens new additional points of potential vulnerability.



(a) rDIQKD setup assuming the switch and the device T are outside Alice's and Bob's safe laboratories.

(b) rDIQKD setup where the switch and the device T are located in Alice's laboratory.

Figure 2: Two possible setups for rDIQKD.

the internal state of the switch and the device T. Clearly, security in this later case also implies security in the case of Fig. 2b, as we are giving more power to Eve.

2.2 Generic protocols

We now outline the general procedure of a generic rDIQKD protocol based on the setup described above. In each measurement round $i = 1, \dots, n$ of the protocol, Alice generates independent random variables $X_i \in \mathcal{X}$ and $S_i \in \{0, 1\}$ and feeds them, respectively, to her device A and the switch. If $S_i = 0$, indicating the choice to route Bob's quantum particle to T, she also generates a random variable $Z_i \in \mathcal{Z}$ and feeds it to T. She records the output variables $A_i \in \mathcal{A}$ and, if applicable, $C_i \in \mathcal{C}$. She publicly announces S_i. If $S_i = 1$, indicating the choice to route Bob's quantum particle to B, Bob generates a random variable $Y_i \in \mathcal{Y}$, feeds it to his device B, and records the output $B_i \in \mathcal{B}$. Alice and Bob then start a new round $i \to i + 1$.

Once all n measurement rounds have been completed, Alice and Bob communicate on a public classical channel with two main goals. On one hand, they disclose part of the data they generated to check that a statistical test Γ is passed, such as verifying a significant violation of a routed Bell inequality. On the other hand, they agree on a subset of the rounds for which they will keep the variables A_i and B_i secret. These variables will constitute the raw key. Typically, these key generation rounds will be those for which the inputs of Alice and Bob belong to a certain subset $\mathcal{K}$ of all their possible input pairs $\mathcal{X} \times \mathcal{Y}$ (e.g. they may generate a key only when Alice uses input $x = 0$ and Bob uses input $y = 3$).

The probabilities with which the input variables are chosen in the n measurement rounds are usually fixed to maximize the key rate, while at the same time ensuring that enough data is obtained for the test Γ to be statistically significant. One might for instance choose these probabilities so that the number of key generation rounds is roughly of order $n - \sqrt{n}$, while the number of rounds used for parameter estimation is of order $\sqrt{n}$.

Finally, if the statistical test Γ is passed, Alice and Bob apply error correction and privacy amplification techniques to their copy of the raw key to extract the finally shared secret key.

2.3 Long-range quantum correlations are necessary for security

Before explaining how the security of rDIQKD protocols can be analyzed and key rates computed, we first point out that long-range quantum correlations, as defined in [LPP23], are necessary for the security of rDIQKD protocol, in the same way that nonlocal correlations are necessary for the security of standard DIQKD protocols.

Routed Bell scenarios feature a short-range Bell test, involving the A/T devices, and a long-distance Bell test, involving the A/B devices. In any given round, the quantum strategy that is used gives rise to the correlations

$$\begin{cases} p(a, c|x, z) = \mathrm{tr}\left(\rho_{AB}\, \mathsf{A}_{a|x} \otimes \mathsf{T}_{c|z}\right) & \text{if } s = 0\,, \\ p(a, b|x, y) = \mathrm{tr}\left(\rho_{AB}\, \mathsf{A}_{a|x} \otimes \mathsf{B}_{b|y}\right) & \text{if } s = 1\,, \end{cases} \tag{1}$$

where ρ_{AB} is the entangled state produced by the sources and $\mathsf{A}_x = \{\mathsf{A}_{a|x}\}_a$, $\mathsf{T}_z = \{\mathsf{T}_{c|z}\}_c$ and $\mathsf{B}_y = \{\mathsf{B}_{b|y}\}_b$ are the POVMs performed by the devices A, T and B, respectively.

Following [LPP23], we say that the correlations $\{p(a,c|x,z), p(a,b|x,y)\}$ are short-range quantum (SRQ) correlations if they can be simulated by a quantum model in which the measurements performed at B are jointly measurable. Formally, this means that the correlations can be written as

$$\begin{cases} p(a,c|x,z) = \mathrm{tr}\left(\tilde{\rho}_{AB}\, \tilde{\mathsf{A}}_{a|x} \otimes \tilde{\mathsf{T}}_{c|z}\right) & \text{if } s = 0\,, \\ p(a,b|x,y) = \sum_\lambda p(b|y,\lambda)\ \mathrm{tr}\left(\tilde{\rho}_{AB}\, \tilde{\mathsf{A}}_{a|x} \otimes \mathsf{N}_\lambda\right) & \text{if } s = 1\,, \end{cases} \tag{2}$$

for some quantum state $\tilde{\rho}_{AB}$, POVMs $\tilde{\mathsf{A}}_x = \{\tilde{\mathsf{A}}_{a|x}\}_a$ for A, $\tilde{\mathsf{T}}_z = \{\tilde{\mathsf{T}}_{c|z}\}_c$ for T, and a single 'parent' POVM $\mathsf{N} = \{\mathsf{N}_\lambda\}_\lambda$ for B, independent of the input y. The outcome b at B is then outputted with probability $p(b|y,\lambda)$ depending on the classical outcome λ. Given that the parent POVM N is independent of y, it can be carried out near the switch, eliminating the need to transmit Bob's quantum particle to the distant device B. Instead, only the classical outcome λ of this parent measurement needs to be communicated to B. Quantum correlations that cannot be written as in (2) are called long-range quantum (LRQ) correlations in [LPP23]. These require the transmission of quantum information to B for a genuine quantum measurement to occur after the input y to B is provided.

In our rDIQKD context, if the quantum devices of Alice and Bob only generate SRQ correlation of the form (2), then the parent POVM N can be performed by Eve on the public channel between the switch and the device B. As Eve can keep a copy of the classical outcome λ, the correlations between A and B factorize when conditioned on Eve's information, i.e., $p(a,b|x,y,\lambda) = p(b|y,\lambda)\ \mathrm{tr}\left(\tilde{\rho}_{AB}\, \tilde{\mathsf{A}}_{a|x} \otimes \mathsf{N}_\lambda\right) / \mathrm{tr}\left(\tilde{\rho}_{AB}\, \mathbb{I} \otimes \mathsf{N}_\lambda\right) = p(a|x,\lambda)p(b|y,\lambda)$, where $p(a|x,\lambda)$ $= \mathrm{tr}\left(\tilde{\rho}_{AB}\, \tilde{\mathsf{A}}_{a|x} \otimes \mathsf{N}_\lambda\right) / \mathrm{tr}\left(\tilde{\rho}_{AB}\, \mathbb{I} \otimes \mathsf{N}_\lambda\right)$, implying that no secure key can be extracted [MW99].

In [LPP23], techniques are introduced for determining when a given set of correlations is SRQ and minimal detection efficiencies required to exhibit LRQ correlations are presented for various cases. These results put constraints on the required detection efficiencies for rDIQKD. For instance, it is shown that in a routed Bell scenario, where Alice and Bob have two inputs, i.e., $\mathcal{X} = \mathcal{Y} = \{0,1\}$, no LRQ correlations can be generated if the detection efficiencies η_A of A and η_B of B satisfy

$$\eta_\mathsf{B} \leq \frac{\eta_\mathsf{A}}{3\eta_\mathsf{A} - 1}\,. \tag{3}$$

For instance, when $\eta_\mathsf{A} = 1$, no key can be extracted if $\eta_\mathsf{B} \leq 1/2$.

2.4 Proving security of rDIQKD protocols

As in standard DIQKD, and other QKD protocols, proving the security of an rDIQKD protocol amounts to finding, given that the statistical test Γ is passed, a lower bound on the smooth min-entropy $H_{\min}^\epsilon(A^n|E)$ of Alice's final raw string $A^n = A_1 \ldots A_n$ conditioned on the eavesdropper's information E, which includes all information publicly disclosed in the protocol as well as Eve's quantum side information acquired during the protocol by interacting with Alice's and Bob's quantum systems. Provided the bound is sufficiently high, it guarantees that privacy amplification can be performed to extract a secure key of the desired length.

The security of standard DIQKD protocols composed of n measurement rounds, which may generally not follow an independent and identically distributed (i.i.d.) model and where memory effects can be present in the devices, can be reduced to a single-round analysis through the use of the Entropy Accumulation Theorem (EAT)[DFR20, AFDF+18, AFRV19] or the Generalized Entropy Accumulation Theorem (GEAT) [MFSR22]. One then finds that the smooth min-entropy is basically the same, up to sublinear terms in n, as in the case where the devices behave identically and independently in each round of the protocol. That is, roughly, $H_{\min}^\epsilon(A^n|E) \geq nH(A|E) - O(\sqrt{n})$ where $H(A|E)$ is the conditional von Neumann entropy of Alice's output A given Eve's information E in a single i.i.d. round. In particular, the asymptotic key rate (when $n \to \infty$) of the protocol against the most general attacks is the same as the i.i.d. key rate given by the Devetak-Winter bound [DW05].

To apply the EAT or GEAT following the approach of [AFDF+18, AFRV19], the CPTP maps $\mathcal{P}_i$ describing the individual steps of an intermediary 'entropy accumulation' (EA) protocol, to which

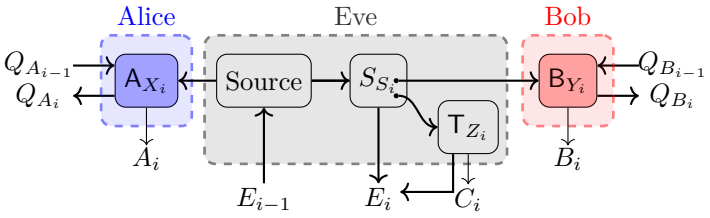


Figure 3: Structure of the CPTP maps $\mathcal{M}_i$ describing the quantum measurement phase of the protocol at step i.

the security of the entire protocol can be reduced, must satisfy a certain Markov condition, in the case of EAT, or a no-signaling condition, in the case of the GEAT. These conditions capture the idea that any side-information Eve may hold about the measurement results at step i is outputted at step i and not recorded in Alice or Bob's quantum systems to be later passed out to Eve in a subsequent round. This is essentially the only non-trivial technical requirement that has to be satisfied for applying either the EAT or GEAT.

An rDIQKD protocol mainly differs from a DIQKD protocol only in the purely quantum phase of the protocol, where Alice and Bob's entangled systems are measured to produce classical outputs A_i, B_i, and C_i. Other aspects of the protocol, like public communication, sifting, parameter estimation, error correction, etc, are essentially identical and can be analyzed in the same way. In particular, the reduction from a multi-round analysis to a single-round analysis using the EAT or GEAT can be done following the approach outlined in [AFDF+18, AFRV19] for DIQKD protocols. The sole requirement is to verify that the no-signaling condition necessary for applying the GEAT is satisfied.

Since rDIQKD and DIQKD mainly differ in the quantum measurement phases $\mathcal{M}_i$ of the protocol, let us focus on this basic building block. At step i, and conditioning on the input classical variables X_i, S_i, Z_i, Y_i, we can describe this process as a CPTP map $\mathcal{M}_i : Q_{A_{i-1}}Q_{B_{i-1}}E_{i-1} \to A_iB_iC_iQ_{A_i}Q_{B_i}E_i$ that takes as input the quantum registers $Q_{A_{i-1}}$, $Q_{B_{i-1}}$, and E_{i-1} of, respectively, Alice's private measurement device A, Bob's private measurement device B, and the eavesdropper Eve, and produces as output the classical variables A_i, B_i, C_i along with updated quantum registers Q_{A_i}, Q_{B_i}, and E_i[2]. This CTPT map has the structure outlined in Fig 3. It is essentially similar to the corresponding map of a standard DIQKD protocol, except for the middle part under the control of Eve, which depends on additional random inputs S_i and Z_i and produces an additional outcome C_i. However, this additional data is part of Eve's side information E_i and thus does not affect the no-signaling condition necessary to apply the GEAT. More specifically,

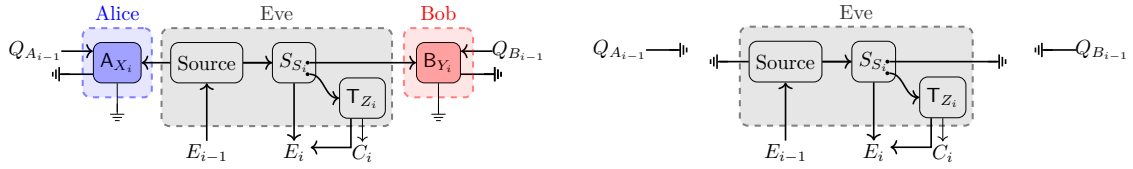
$$\mathrm{tr}_{A_iB_iQ_{A_i}Q_{B_i}} \circ \mathcal{M}_i = \mathcal{E}_i \circ \mathrm{tr}_{Q_{A_{i-1}}Q_{B_{i-1}}} \tag{4}$$

where this identity is easily visualized in Fig. 4 and where $\mathcal{E}_i$ is a map from E_{i-1} to C_iE_i. The map $\mathcal{M}_i$ is thus non-signaling in the sense that tracing out Alice's and Bob's output quantum and classical registers $A_iB_iQ_{A_i}Q_{B_i}$, yields a map on Eve's systems that do not depend on the input systems $Q_{A_{i-1}}$ and $Q_{B_{i-1}}$ of Alice and Bob. This no-signalling condition in the quantum measurement phase $\mathcal{M}_i$ of rDIQKD protocols allows the GEAT to be applied just in the same way as it would in DIQKD protocols and as outlined in [AFDF+18, AFRV19], ensuring that the no-signaling conditions of the maps $\mathcal{P}_i$ describing the intermediary EA protocol are satisfied.

2.5 Asymptotic key rate computation

Consider a rDIQKD protocol where, according to the honest, ideal implementation, the source produces in each round the state ρ_{AB} and the devices A, T, and B perform the POVMs $\mathsf{A}_x = \{\mathsf{A}_{a|x}\}_a$, $\mathsf{T}_z = \{\mathsf{T}_{c|z}\}_c$, and $\mathsf{B}_y = \{\mathsf{B}_{b|y}\}_b$, respectively, giving rise to the correlations $p(a, c|x, z)$ and $p(a, b|x, y)$ in (1).

[2]Strictly speaking in any given round of the protocol, either the output C_i is generated if $S_i = 0$, or the output B_i is generated if $S_i = 1$. However, we can always assume that values are assigned both to C_i and B_i at each step i. For instance, we can set $C_i = \perp$ if $S_i = 1$ and $B_i = \perp$ if $S_i = 0$.



(a) **(b)**

Figure 4: (a) The map $\mathrm{tr}_{A_iB_iQ_{A_i}Q_{B_i}} \circ \mathcal{M}_i$ obtained by tracing out the map in Fig. 3 over the output systems of Alice and Bob. As depicted in (b), it does not depend anymore on the input registers $Q_{A_{i-1}}$ and $Q_{B_{i-1}}$, i.e., it is of the form $\mathcal{E}_i \circ \mathrm{tr}_{Q_{A_{i-1}}Q_{B_{i-1}}}$, where $\mathcal{E}_i$ is a map from E_{i-1} to C_iE_i corresponding to Eve's box.

The above discussion implies, as in the standard DIQKD setting, that the asymptotic key rate of such a rDIQKD protocol, assuming one-way public communication from Alice to Bob, is given by the i.i.d. Devetak-Winter rate [DW05]

$$r = H(A|XE) - H(A|B)\,, \tag{5}$$

where $H(A|XE)$ is the conditional von Neumann entropy of Alice's output A conditioned on the eavesdropper information E and Alice's input X, and $H(A|B)$ is the Shannon entropy of Alice's output conditioned on Bob's. Both entropies are computed by averaging over the input choices used for key generation, which are typically a subset $\mathcal{K} \subseteq \mathcal{X} \times \mathcal{Y}$ of all possible input pairs of Alice and Bob.

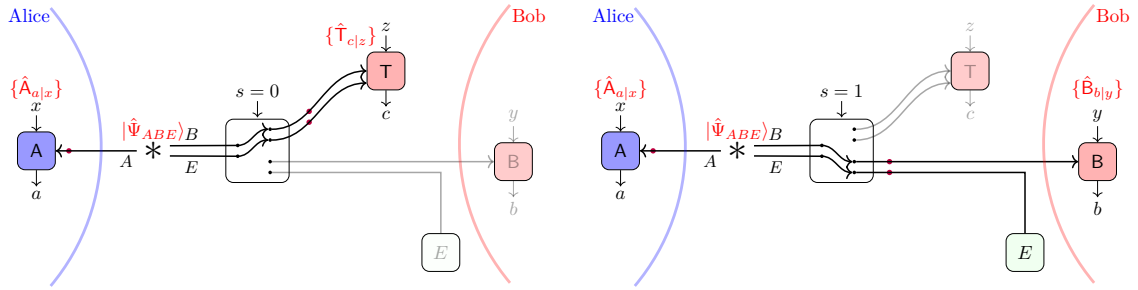
The term $H(A|B)$ captures the cost of error correction and can straightforwardly be computed from the distribution $p(a, b|x, y)$ fixed by the honest quantum strategy. The term $H(A|XE)$ captures Eve's uncertainty about the measurement outcomes of Alice's measurements used for key generation. It is hard to compute because, in a DI setting where the devices are untrusted, it must be determined by taking the worst-case value over all possible quantum strategies compatible with the correlations $p(a, c|x, z)$ and $p(a, b|x, y)$ (which may differ from the honest strategy on the right-hand side of (1)).

We briefly explain how $H(A|XE)$ can be lower-bounded using NPO [NPA07, NPA08, PNA10] and the BFF method [BFF21a]. We use this method in Section 3 to provide numerical lower bounds on the key rate of various rDIQKD protocols of interest. The same techniques can be used to obtain min-tradeoff functions and determine finite-size corrections to the Devetak-Winter rate.

We start by modeling the general behavior of the devices and Eve (in the setup of Fig. 2a), which may differ from the honest implementation. This is depicted in Fig. 5. The source first produces a state $\hat{\rho}_{ABE}$, where subsystem A goes to Alice's device, subsystem B will eventually go to Bob's device (if the switch setting is $s = 1$) and subsystem E characterizes Eve's initial quantum correlations with A and B[3]. Subsystem A is measured by device A through a measurement $\hat{\mathsf{A}}_x = \{\hat{\mathsf{A}}_{a|x}\}_a$. If $s = 1$, subsystem B is similarly measured by device B through a measurement $\hat{\mathsf{B}}_y = \{\hat{\mathsf{B}}_{b|y}\}$. If $s = 0$, on the other hand, Eve, who holds the measurement device T performs a measurement $\hat{\mathsf{T}}_z = \{\hat{\mathsf{T}}_{c|z}\}_c$ that acts jointly on subsystems B and E, as this is the most general thing she can do to simulate the honest correlations between A and T. This potentially produces a post-measurement state for Eve, but a description of this state is unnecessary for our purposes; since no key is extracted from a round where $s = 0$, Eve's side information from such rounds is irrelevant to the analysis.

Without loss of generality, we can assume the initial state $\hat{\rho}_{ABE}$ to be a pure state $|\hat{\Psi}_{ABE}\rangle$, as any purifying system can be included in subsystem E. We can also assume that the measurements $\hat{\mathsf{A}}_x$, $\hat{\mathsf{B}}_y$ and $\hat{\mathsf{T}}_z$ are all projective, if necessary by considering enlarged systems. Finally, one might consider the possibility for Eve to do a joint operation on subsystems B and E, depending on the value of the switch setting s, before proceeding as above. Without loss of generality, we can assume that these operations are unitary $\hat{U}^s_{BE}$, again by enlarging the Hilbert space if necessary. But then

[3]Unlike the sequential depiction in Fig. 3, there is no need to account for input and output quantum registers for either Alice or Bob, as we are focusing on a single round of an i.i.d. scenario. Furthermore, we address separately the cases where the switch input is $s = 0$ and $s = 1$. This simplifies the description of Eve's potential strategies



(a) Case $s = 0$. **(b)** Case $s = 1$.

Figure 5: Quantum model of Eve's strategies used to compute the single-round $H(A|E)$ bound.

we can absorb the unitary $\hat{U}^1_{BE}$ in the definition of the initial state, $|\hat{\Psi}_{ABE}\rangle \leftarrow \hat{U}^1_{BE}|\hat{\Psi}_{ABE}\rangle$, and redefine the measurements at T as $\mathsf{T}_{c|z} \leftarrow \hat{U}^1_{BE}\hat{U}^{0\dagger}_{BE}\mathsf{T}_{c|z}\hat{U}^0_{BE}\hat{U}^{1\dagger}_{BE}$. There is thus actually no need to consider the operations $\hat{U}^s_{BE}$ explicitly in the modeling of the devices and Eve's strategies.

Altogether, the possible quantum strategies $\hat{\mathcal{Q}} = \{|\hat{\Psi}_{ABE}\rangle, \hat{\mathsf{A}}_{a|x}, \hat{\mathsf{B}}_{b|y}, \hat{\mathsf{T}}_{c|z}\}$ that Eve can use are fully characterized by the initial state $|\hat{\Psi}_{ABE}\rangle$, and the projective measurements $\{\hat{\mathsf{A}}_{a|x}\}_a$, $\{\hat{\mathsf{B}}_{b|y}\}_b$, and $\{\hat{\mathsf{T}}_{c|z}\}_c$. These should be constrained by the fact that they return the honest correlations $p(a, c|x, z)$ and $p(a, b|x, y)$:

$$p(a, c|x, z) = \langle\hat{\Psi}_{ABE}|\, \hat{\mathsf{A}}_{a|x} \otimes \hat{\mathsf{T}}_{c|z}\, |\hat{\Psi}_{ABE}\rangle\,, \tag{6}$$

$$p(a, b|x, y) = \langle\hat{\Psi}_{ABE}|\, \hat{\mathsf{A}}_{a|x} \otimes \hat{\mathsf{B}}_{b|y} \otimes \mathbb{I}_E\, |\hat{\Psi}_{ABE}\rangle\,, \tag{7}$$

where we remind that $\hat{\mathsf{T}}_{c|z}$ acts jointly on subsystems B and E.

To each strategy $\hat{\mathcal{Q}}$, we can associate the post-measurement state σ_{AXE}

$$\sigma_{AXE} = \sum_{ax} p(x)\, |ax\rangle\langle ax| \otimes \sigma_E^{a,x}\,, \tag{8}$$

where

$$\sigma_E^{a,x} = \mathrm{tr}_{AB}(|\hat{\Psi}_{ABE}\rangle\langle\hat{\Psi}_{ABE}|\, (\hat{\mathsf{A}}_{a|x} \otimes \mathbb{I}_B \otimes \mathbb{I}_E))\,, \tag{9}$$

is the unnormalized state held by Eve conditioned on Alice's input x and output a. The conditional min-entropy can then be computed as

$$H(A|XE) = \inf_{\hat{\mathcal{Q}}|p} H(A|XE)_{\sigma_{AXE}}\,,$$

where the optimization runs over all quantum strategies $\hat{\mathcal{Q}}$ compatible with the honest correlations $p(a, c|x, z)$ and $p(a, b|x, y)$.

Notice now that the above optimization problem is almost identical to the optimization problem in a corresponding standard DIQKD protocol where Bob uses the input set $\mathcal{T} \times \mathcal{Y}$ and performs the measurements $\{\hat{\mathsf{T}}_z\} \times \{\hat{\mathsf{B}}_y\}$. The only difference with a regular DIQKD scenario is that the subset of measurements $\{\hat{\mathsf{T}}_z\}$ act on the joint systems BE, instead of just B. The BFF method [BFF21a] based on NPO [NPA07, NPA08, PNA10] can then be used for lower bounding the conditional entropy $H(A|XE)$ in rDIQKD in almost the same way as in DIQKD. Since operators acting on different systems are replaced by commuting operators in NPO, the only difference with a standard BFF computation for DIQKD is that no commutation relations should be imposed between the T_z measurements and the BFF operators acting on Eve's system. We detail the NPO formulation corresponding to rDIQKD in Appendix A.

3 Numerical results

Using the numerical technique discussed in the previous section, we now compute lower bounds on the key rate of several simple rDIQKD protocols. We are interested in an rDIQKD setup in

which the devices A and T have high detection efficiencies, i.e., are situated close to the source. For simplicity, we assign them identical (high) efficiencies, $\eta_{\mathsf{A}} = \eta_{\mathsf{T}} \equiv \eta_{\mathsf{S}}$. Conversely, since we want to establish key over long distances, Bob's device B must be situated far away and consequently has a lower efficiency, $\eta_{\mathsf{B}} \equiv \eta_{\mathsf{L}} \ll \eta_{\mathsf{S}}$. For a given short-path efficiency η_{S}, we compute lower bounds on the asymptotic key rate r as a function of the long-path detection efficiency η_{L}.

In computing the key rate, we can use the Devetak-Winter formula corresponding to one-way communication from Alice to Bob, as in (5), or from Bob to Alice given by $r = H(B|YE) - H(B|A)$. The entropy $H(B|YE)$ quantifies how well Eve can guess Bob's outcome. As Bob's device has a lower efficiency than Alice's, we expect that this will typically be easier for her than to guess Alice's outcome. Furthermore, since Bob holds a simple untrusted measurement device, Eve can apply to it the convex-combination attacks based on joint-measurability introduced in [MS24], which imply particularly stringent limits on the minimal efficiency η_{L} required to distill a secret key. We carried out numerical exploratory tests that confirm that the key rate is lower when computing it using one-way communication from Bob to Alice instead of the other direction. In the following, we thus compute all key rates using the bound (5) holding for one-way communication from Alice to Bob.

Nondetection events $\emptyset$ corresponding to the situation where a detector fails to click can either be treated as separate measurement outcomes or binned with one of the other outcomes, say $\emptyset \mapsto +1$. This choice need not be the same in testing and key generation rounds and may also differ between the devices A, T and B. Binning the outcomes of Alice's device A in key generation rounds decreases the entropies $H(A|E)$ and $H(A|B)$. However, numerical tests indicate that the decrease in $H(A|B)$ is more pronounced than for $H(A|E)$ and thus the net effect on the key rate is positive. This is also what one observes in standard DIQKD protocols. Conversely, binning the outcomes of the device B in key generation rounds increases $H(A|B)$, as it decreases the information available to Bob for error correction, and thus lowers the key rate. In the following, we will therefore always bin the outcomes of A and keep the outcomes of B unbinned in key generation rounds, i.e., in computing the entropies $H(A|E)$ and $H(A|B)$, the random variable A corresponds to the binned version of Alice's outcome and the random variable B to the unbinned version of Bob's outcome.

The bound on $H(A|E)$ computed from the BFF method depends on the correlations $p(a, b|x, y)$ and $p(a, c|x, z)$ in testing rounds through the constraints (6) and (7). Binning the outcomes of the devices A, T, and B for testing rounds induces fewer restrictions on these correlations, yielding potentially lower values of $H(A|E)$. Unfortunately, keeping no-click events separate in testing rounds substantially increases the size of the SDP relaxation problem used to compute $H(A|E)$. For these reasons, we focus on protocols in which the outcomes of the devices A and T are always binned in testing rounds. For the outcomes of B, we consider both situations where they are binned or not. Although the latter scenario should yield higher key rates, binning the outcomes could enable us to implement SDP relaxation of the BFF NPO problem at a higher level, possibly resulting in improved key rates.

Besides detection efficiency, another important consideration in any experimental implementation is the impact of noise. We will consider a simple noise model, in which the state ρ distributed by the source is mixed with white noise $\rho_{\text{noise}} = \nu\rho + (1-\nu)\mathbb{1}/4$, where ν is the visibility.

3.1 A family of CHSH-BB84 type protocols

We study a family of protocols where on Alice's side $\mathcal{X} = \{0, 1\}$, $\mathcal{Z} = \{0, 1\}$ and, in the honest implementation, the shared state is the two-qubit maximally entangled state $|\phi_+\rangle$ and the measurements are $\mathcal{X} = \{\sigma_z, \sigma_x\}$, $\mathcal{Z} = \{\frac{\sigma_z \pm \sigma_x}{\sqrt{2}}\}$. Thus the A/T correlations are CHSH correlations and perfectly self-test the honest implementation when the efficiency $\eta_{\mathsf{S}} = 1$ and the visibility $\nu = 1$.

The protocols in our family only differ in the measurements of Bob and the subset of measurements used for key generation. We list the protocols we consider in Table 1.

The protocol rCHSH is the routed version of the standard DIQKD CHSH protocol introduced in [ABG+07], the only difference being the added T measurements in the routed version. Bob has three inputs $\{0, 1, 2\}$ where the first one is used to establish the raw key shared with Alice and the rest are used to estimate the CHSH violation between Alice and Bob. To simplify the SDP relaxation used to compute $H(A|XE)$, we do not include the probabilities $p(ab|xy)$ corresponding to the inputs $y = 0$ in the NPO problem detailed in Appendix A.

The protocol rBB84 is the routed version of the standard BB84 protocol, in which the key is

Protocol	$\mathcal{Y}$	Ideal measurements	$\mathcal{K}$	y in SDP
rCHSH	$\{0,1,2\}$	$\{\sigma_z, \frac{\sigma_z \pm \sigma_x}{\sqrt{2}}\}$	$\{(0,0)\}$	$\{1,2\}$
rBB84	$\{0,1\}$	$\{\sigma_z, \sigma_x\}$	$\{(0,0)\}$	$\{0,1\}$
rCHSH-BB84	$\{0,1,2,3\}$	$\{\sigma_z, \sigma_x, \frac{\sigma_z \pm \sigma_x}{\sqrt{2}}\}$	$\{(0,0)\}$	$\{0,1,2,3\}$
2-basis rBB84	$\{0,1\}$	$\{\sigma_z, \sigma_x\}$	$\{(0,0),(1,1)\}$	$\{0,1\}$

Table 1: Family of routed rDIQKD protocols considered in this work. For each protocol, we indicate in each column: the inputs $\mathcal{Y}$ of Bob, the corresponding ideal measurements in the honest implementation, the settings $\mathcal{K}$ used for key generation, and finally which inputs are included in the SDP relaxation for $H(A|XE)$.

built from the $(x, y) = (0, 0)$ inputs. This protocol is insecure in the DIQKD setting since the corresponding correlations admit a local model. However, the rBB84 correlations are LRQ for sufficiently high efficiencies η_{S} and η_{L}, and visibility ν [LPP23]. We will show that they lead to a positive key rate in the rDIQKD setting for a range of parameters. We also studied a two-basis version of the rBB84 protocol in which the key is built from the inputs $(x, y) \in \{(0, 0), (1, 1)\}$. While in principle, it could give an improvement over the one-basis version, the size of the corresponding SDP relaxation was too large to run it at the same level as the one-basis version and we did not observe this improvement. We therefore do not consider this protocol further in the following.

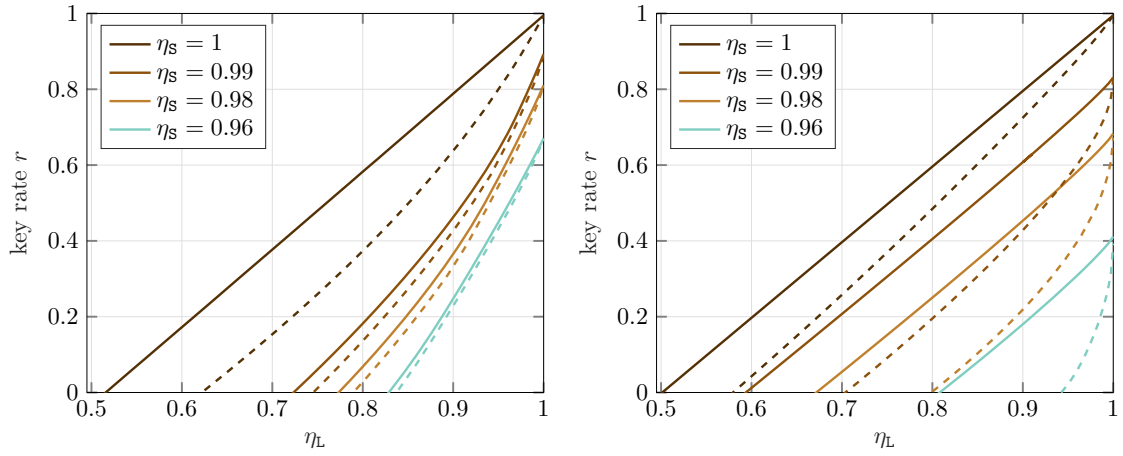
Finally, the rCHSH-BB84 protocol is a combination of the rCHSH and rBB84 protocols in which Bob performs the measurements appearing both in the rCHSH and rBB84 protocols.

We note that the rDIQKD protocols that we analyze have not only a corresponding DIQKD version, obtained by removing the intermediate T measurements but also a semi-DIQKD prepare-and-measure analogue. Indeed, the A/T CHSH test effectively self-tests that Alice is remotely preparing the BB84 states when the efficiency $\eta_{\mathsf{S}} = 1$ and the visibility $\nu = 1$. In this ideal case, all the above protocols are thus equivalent to a semi-DI prepare-and-measure (PM) version in which Alice's preparation is trusted to prepare the BB84 states and in which Bob's measurements are fully untrusted. In particular, the security of the rBB84 protocol in this ideal case is then equivalent to the security of the BB84 PM protocol in the one-sided DI setting [May01, BCC+10, Woo16, MS24]. However, the rBB84 protocol has the advantage that it is fully device-independent, with the measurements performed at T certifying the BB84 preparations, while these preparations are instead assumed to be the correct ones in the one-sided DI PM version. When the efficiency $\eta_{\mathsf{S}} < 1$ and/or the visibility $\nu < 1$, the rBB84 then can be thought of as a semi-DI BB84 protocol in which Alice's preparation is non-ideal and only partly trusted. Similarly, the rCHSH protocol can be seen to be related to the semi-DI PM CHSH protocol considered in [WP15] and the rCHSH-BB84 protocol to the semi-DI PM CHSH-BB84 protocol of [WLP12].

We computed bounds on the key rates for each of the protocols listed in Table 1 for different values of the short-path detection efficiency η_{S} and the long-path detection efficiency η_{L} and different visibilities ν using the BFF method and SDP relaxations. These results, as well as the codes used to generate them, are available at [Git]. Below, we discuss several interesting aspects of the results.

Binning vs not binning

We first compare the key rates for every routed protocol with and without binning for the measurements at B in testing rounds (remember that we always view the no-click outcome $\emptyset$ of Bob as a separate outcome in key generation rounds and that we always bin the outcomes of A and T). In every case, we find that the key rate is significantly better when Bob does not bin. This is consistent with the findings of [LPP23], where it was shown that keeping no-click outcomes significantly decreases the critical efficiency at which correlations become SRQ. We plot the comparison in Fig. 6 for the rCHSH and rBB84 protocols for visibility $\nu = 1$.



(a) rCHSH protocol. **(b)** rBB84 protocol.

Figure 6: *Binning vs no binning for* B. Lower bounds on the asymptotic key rate r as a function of η_{L} for different values of η_{S} with binning (dashed curves) and without binning (solid curves) and visibility $\nu = 1$. Bounds are obtained at NPA level $2 + ABZ + AZB + AABZ + AAZB$.

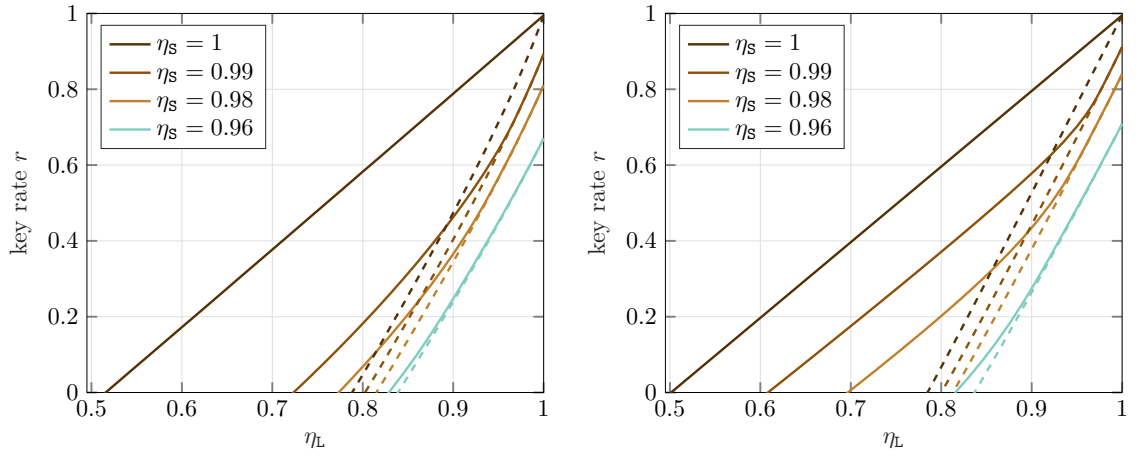
Comparison to non-routed protocols

Let us now compare routed protocols to their non-routed counterparts. There are two natural ways to do so. First, we can simply consider the effect of removing the device T from the routed protocols on the key rate. We plot the key rate of the rCHSH and rCHSH-BB84 protocols against their non-routed versions in Fig. 7 for visibility $\nu = 1$. In both cases, we see that the introduction of a testing device T significantly improves the key rate. In particular, for $\eta_{\mathsf{S}} = 0.99$, we obtain a critical detection efficiency of respectively $\eta_{\mathsf{L}} \sim 0.72$ and $\eta_{\mathsf{L}} \sim 0.61$ for the rCHSH and rCHSH-BB84 protocols, which represents an $\sim 11\%$ and $\sim 31\%$ improvement over their corresponding non-routed protocols. However, this improvement declines rapidly for lower values of η_{S} due to the fact that the testing device T is less effective in certifying the correlations when the short-path test is of lower quality.

The above comparison between DIQKD and rDIQKD protocols is not meaningful for the rBB84 protocol, since BB84 correlations are local without the testing device T and thus cannot be used for DIQDK. A second way to compare rDIQKD to DIQKD protocols is to view the routed protocols as a DIQKD protocol in which some of the measurements of Bob used for testing rounds have been moved closer to the source, to the T device. The rBB84 protocol can be seen in this way as originating from a standard CHSH-BB84 DIQKD protocol in which the remote $\frac{\sigma_z \pm \sigma_x}{\sqrt{2}}$ measurements of Bob are moved to the T device. While this increases the quality of these measurements due to improved detection efficiency at shorter distances, it comes at the cost of revealing to Eve that certain rounds are only used for testing. We clearly see this tradeoff in Fig. 8. For high values of η_{S} and low values of η_{L}, the routed protocol performs better due to the advantage gained in certifying Alice's devices. But as η_{S} decreases and η_{L} increases, the non-routed protocol improves and eventually outperforms the routed one, as it reveals less information to Eve about which measurements Bob's device is performing. At $\eta_{\mathsf{S}} = 0.96$, the non-routed protocol outperforms the routed protocol for all values of η_{L}, while at $\eta_{\mathsf{S}} = 1$, the routed protocol outperforms the non-routed protocol for all values of η_{L}.

Comparison of different protocols

We compare in Fig. 9 the key rates for the different routed protocols listed in Table 1, in the case where the outcomes of B are not binned. For high-quality short-range tests, the rBB84 protocol performs better than the rCHSH protocol, but this performance decreases more rapidly with η_{S}. The best performance should be obtained from the rCHSH-BB84 protocol since the key rates for this protocol are in principle at least as good as the ones obtained for the rCHSH and rBB84 protocols. Though we do find that the rCHSH-BB84 protocol always outperforms the rCHSH



(a) CHSH vs rCHSH protocols.

(b) CHSH-BB84 vs rCHSH-BB84 protocols.

Figure 7: *Comparison to standard DIQKD protocols.* Lower bounds on the asymptotic key rate r for routed (solid curves) and non-routed (dashed curves) protocols. In all protocols, Bob does not bin and visibility $\nu = 1$. The bounds for CHSH and rCHSH protocols were obtained at NPA level $2 + ABZ + AZB + AABZ + AAZB$, whereas the bounds for CHSH-BB84 and rCHSH-BB84 were obtained at level $2 + ABZ + AZB$

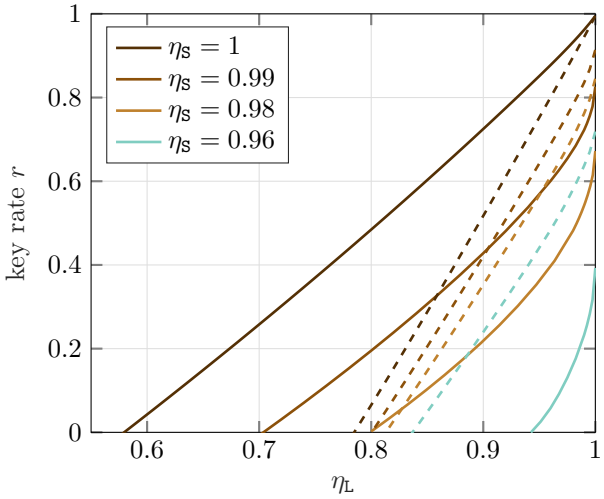
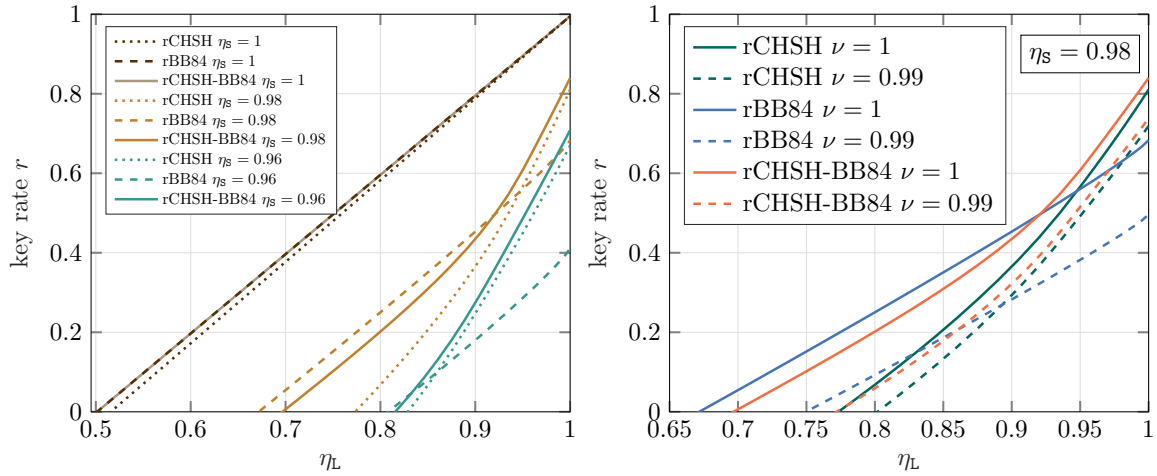


Figure 8: *Comparison of the standard CHSH-BB84 protocol to rBB84.* Lower bounds on the asymptotic key rate r as a function of η_{L} for different values of η_{S} for rBB84 and CHSH-BB84 with binning of the outcomes of B and visibility $\nu = 1$. Bounds are obtained at NPA level $2 + ABZ + AZB + AABZ + AAZB$.

protocol, we see that there exist regions of the parameter (when η_{L} is low), where our rBB84 bounds are higher than the rCHSH-BB84 bounds. This is due to the fact that the rCHSH-BB84 bounds were computed at a lower level of the NPA hierarchy than the other protocols due to the bigger SDP size. We thus expect that the key rates for the rCHSH-BB84 protocol could be greatly improved by computing them at a higher level of the NPA hierarchy.

We showcase the effect of finite visibility ν in Fig. 9b for $\eta_{\mathsf{S}} = 0.98$. We see that the key rate is very sensitive to finite visibility, but the effect is more pronounced for the rBB84 protocol. This is consistent with our previous observations: the rBB84 protocol performs best when the A/T test is of high quality ($\nu = 1$), while the rCHSH protocol is more robust to noise ($\nu = 0.99$).



(a) Plot for different values of η_{S} and visibility $\nu = 1$. **(b)** Plot for $\eta_{\mathsf{S}} = 0.98$ and visibility $\nu = 1$ and $\nu = 0.99$.

Figure 9: *Comparison of different protocols.* Lower bounds on the asymptotic key rate r as a function of η_{L} for the different routed protocols in Table 1 in the case where Bob does not bin. Bounds for rCHSH-BB84 (rCHSH and rBB84) are obtained at NPA level $2 + ABZ + AZB(+AABZ + AAZB)$.

Additional remarks

We finish with several additional remarks on the results obtained. First, as we explained earlier, in the limiting case where $\eta_{\mathsf{S}} = 1$, the A/T correlations effectively self-test the BB84 preparations. The rBB84 protocol is then equivalent to the one-sided PM BB84 protocol where Bob's measurement is fully untrusted. If the only information used in parameter estimation, assuming Bob bins his outcomes, is the standard quantum bit-error rate (QBER) q_x in the σ_x basis (the σ_z basis is used for key generation) then the asymptotic key rate is given by the Shor-Preskill rate [SP00, Woo16] $r = 1 - h(q_x) - H(A|B)$, where $h(\cdot)$ is the binary entropy. A simple calculation gives $q_x = \frac{1-\eta_{\mathsf{L}}}{2}$ and $H(A|B) = 1 - \eta_{\mathsf{L}}$, implying $r = 1 - h\left(\frac{1-\eta_{\mathsf{L}}}{2}\right) - (1 - \eta_{\mathsf{L}})$. We verified numerically that we recover this rate if we impose in the BBF method, besides the ideal CHSH A/T correlations, only the QBER value for the A/B correlations. We then find that the key rate is positive as long as $\eta_{\mathsf{L}} \geq 65.9\%$.

Interestingly, when we compute the key rate by fixing the full set of A/B correlations and not only the QBER in the σ_x basis, we find as illustrated in Fig. 6b that for $\eta_{\mathsf{S}} = 1$, the key rate in the rBB84 protocol is positive for $\eta_{\mathsf{L}} \gtrsim 58.5\%$ when binning B outcomes and $\eta_{\mathsf{L}} \gtrsim 50\%$ when non-binning B outcomes. These results, due to the equivalence mentioned above, also apply to one-sided PM BB84 protocols and imply that the Shor-Preskill rate can be significantly improved by taking into account the full set of A/B correlations. This is consistent with the recent results of [MS24].

We also observe that the thresholds of $\eta_{\mathsf{L}} \gtrsim 58.5\%$ (binning) and $\eta_{\mathsf{L}} \gtrsim 50\%$ (non-binning) at which the key rate of the rBB84 vanished correspond precisely to the point where the rBB84 correlations become SQR [LPP23]. This is to be contrasted with DIQKD protocols in which the key rate typically vanishes well before the underlying correlations become local.

Finally, the $\eta_{\mathsf{L}} \gtrsim 50\%$ threshold for rBB84 obtained in the case of non-binning is optimal according to the upper bound (3) and the general attacks of [MIB+24]. Though the same upper bound applies to DIQKD protocols, it is not clear if it can be achieved with a simple qubit-based protocol as in the routed case.

4 Conclusion and outlook

We considered routed DIQKD protocols based on the recently introduced routed Bell configuration [LPP23, CVP24]. Our work is motivated by the finding that introducing an additional measurement device close to the source, allowing for improved testing of quantum correlations at short distance, effectively lowers the visibility and detection efficiency requirements for certifying

long-range quantum correlations [LPP23], which are a prerequisite for DI security.

We outlined how the GEAT applies to rDIQKD protocols, essentially in the same way the EAT applies to DIQKD protocols, enabling reducing the security analysis to a single-round. We then applied the Brown-Fawzi-Fawzi method [BFF21a] combined with semidefinite relaxation hierarchies [NPA07, NPA08, PNA10] to numerically compute lower bounds on the asymptotic key rate for several routed DIQKD protocols.

We focused on a simple family of two-qubit rDIQKD protocols, in which Alice's device A and Bob's device B establish CHSH correlations, BB84 correlations, or a combination of both. In all cases, the additional short-range testing device T is used to generate CHSH correlations with A, thus enabling in the ideal case a perfect self-test of the source and Alice's measurements. Consistent with the previous study on quantum correlations in routed Bell scenarios [LPP23], we find that for low noise A/T correlations (i.e., high detection efficiencies at short distance), rDIQKD protocols based on BB84 correlations between A and B, whose nonlocality can be certified in routed setups, tolerate the lowest detection efficiency for the long-range device B. When the short-range devices are ideal, rBB84 protocols can be secure up to the theoretical limit [LPP23, MIB+24] of $\eta_{\mathrm{L}} \gtrsim 50\%$ for the long-range device B. On the other hand, rCHSH protocols have absolute higher detection efficiency requirements for B, but they are more robust to imperfections in the A/T correlations. A combined CHSH-BB84 protocol is expected to perform best in both regimes, though clearly establishing this would likely require computing the key rates at a higher level of the SDP hierarchy.

While the advantages of routed protocols are significant, enabling to lower the detection efficiency of Bob's device B up to $\sim 30\%$ compared to non-routed protocols, they crucially depend on the ability to generate high-quality short-range correlations between Alice's device A and the additional testing device T. This is further complicated by the need for a switch to implement routing to either the testing device T or Bob's device B, which can be actively controlled at a sufficiently high rate, leading to additional noise and inefficiencies. Nevertheless, given that routed protocols can be implemented modularly in existing DIQKD setups at relatively minimal experimental overhead, they may facilitate the prospects of a full photonic implementation of DIQKD.

Our work suggests several interesting directions for future work. First, it would be interesting to study more general rDQIKD protocols, particularly with more inputs/outputs, to overcome the ultimate limitations implied by convex-combination attacks based on joint-measurability [MIB+24]. Second, it would be interesting to consider more complicated topologies, featuring multiple switches and testing devices, which could potentially provide more robust certification of the device B. Along this line, we note that the DIQKD protocol introduced in [LPT+13] can be seen as a routed protocol with an additional Bell-state measurement between Alice and Bob to further limit the effect of losses in the channel. The numerical methods used in this work could possibly be improved to provide better bounds on the key rate of this protocol or study variants of it. Finally, it would be interesting to explicitly model imperfections in the switch and explore the experimental feasibility of routed DIQKD protocols with current technology.

On a more conceptual level, the link between rDIQKD protocols and one-sided PM protocols is particularly interesting and deserves to be further explored. In particular, we note that the threshold $\eta_{\mathrm{L}} \gtrsim 50\%$ for the rBB84 protocol when the A/T correlations perfectly self-test the BB84 preparations imply that the traditional BB84 protocol can be secure up to this threshold in a one-sided setting where Bob's device is fully untrusted [May01, BCC+10, Woo16]. This finding, consistent with a similar observation in [MS24], shows that the Shor-Preskill rate for the one-sided PM BB84 protocol can be significantly improved by taking into account the full set of A/B correlations and keeping non-detection events as a separate outcome.

Note added: While completing this work, we were made aware of similar work by E. Tan and R. Wolf [TW24].

Acknowledgments. S.P. acknowledges funding from the VERIqTAS project within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 101017733 and the F.R.S-FNRS Pint-Multi program under Grant Agreement R.8014.21, from the European Union's Horizon Europe research and innovation program under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043), from the F.R.S-FNRS through the PDR T.0171.22, from the FWO and

F.R.S.-FNRS under the Excellence of Science (EOS) program project 40007526, from the FWO through the BeQuNet SBO project S008323N, from the Belgian Federal Science Policy through the contract RT/22/BE-QCI and the EU "BE-QCI" program. S.P. is a Research Director of the Fonds de la Recherche Scientifique – FNRS. E.P.L. acknowledges support from the Fonds de la Recherche Scientifique – FNRS through a FRIA grant. J.P. acknowledges support from NCCR-SwissMAP. T.L.D. benefited from a government grant managed by the Agence Nationale de la Recherche under the Plan France 2030 with the reference ANR-22-PETQ-0009. This project was funded within the QuantERA II Programme which has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 101017733.

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

A Explicit formulation of BFF-NPO for lower bounding the conditional entropy $H(A|XE)$

The Brown-Fawzi-Fawzi (BFF) method [BFF21b] provides a hierarchy of successively tighter approximations to the von Neumann entropy. As explained in the main text, we can use it in the context of rDIQKD in the same way it is used in DIQDK, modulo the introduction of operators $\hat{\mathsf{T}}_{c|z}$ that act on the joint systems BE, and hence do not commute with the BFF operators Z_a acting on Eve's system E. Explicitly, the BFF-NPO formulation for lower-bounding the conditional entropy $H(A|XE)$ is as follows. For simplicity, we only present it in the case where the raw key of Alice is composed of the outcome of a single input $x = x^*$.

Let V_i be the solutions to the following NPO problems, where t_i and w_i are the nodes and weights of an m-point Gauss-Radau quadrature on $[0, 1]$ with an endpoint at $t_m = 1$, and $\alpha_i = \frac{3}{2}\max\{\frac{1}{t_i}, \frac{1}{1-t_i}\}$:

$$
\begin{aligned}
V_i = \inf \sum_a \langle\psi|\, \mathsf{A}_{a|x^*}(Z_a + Z_a^* + (1-t_i)Z_a^* Z_a) + t_i Z_a Z_a^*\, |\psi\rangle \\
\text{s.t. } \langle\psi|\, \mathsf{A}_{a|x}\mathsf{B}_{b|y}\, |\psi\rangle = p(a,b|x,y), \quad \forall a,b,x,y, \\
\langle\psi|\, \mathsf{A}_{a|x}\mathsf{T}_{c|z}\, |\psi\rangle = p(a,c|x,z), \quad \forall a,c,x,z, \\
\mathsf{A}_{a|x}\mathsf{A}_{a'|x} = \delta_{aa'}\mathsf{A}_{a|x}, \quad \forall a,a',x, \\
\mathsf{B}_{b|y}\mathsf{B}_{b'|y} = \delta_{bb'}\mathsf{B}_{b|y}, \quad \forall b,b',y, \\
\mathsf{T}_{c|z}\mathsf{T}_{c'|z} = \delta_{cc'}\mathsf{T}_{c|z}, \quad \forall c,c',z, \\
[\mathsf{A}_{a|x}, \mathsf{B}_{b,y}] = [\mathsf{A}_{a|x}, \mathsf{T}_{c,z}] = 0, \quad \forall a,b,c,x,y,z, \\
[\mathsf{A}_{a|x}, Z_{a'}^{(*)}] = [\mathsf{B}_{b|y}, Z_a^{(*)}] = 0, \quad \forall a,a',b,x,y, \\
Z_a^* Z_a \leq \alpha_i, \quad \forall a, \\
Z_a Z_a^* \leq \alpha_i, \quad \forall a,,
\end{aligned}
$$

where the minimization is over the state $|\psi\rangle$ and the Hermitian operators $\mathsf{A}_{a|x}$, $\mathsf{B}_{b|y}$, $\mathsf{T}_{c|z}$, and non-Hermitian operators Z_a. The von Neumann entropy is then lower bounded by [BFF21b],

$$
H(A|E, X = x^*) \geq \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln 2}(1 + V_i)\,.
$$

We can compute a lower bound on the NPO optimums V_i, hence on $H(A|E, X = x^*)$, by relaxing them to semidefinite programs [NPA07, NPA08, PNA10]. The numerical results presented in this work have been computed using $m = 12$ points in Gauss-Radau quadrature and SDP relaxations corresponding to level 2 and some additional monomials, as detailed in the main text.

References

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2007.

[AEE+23] Koji Azuma, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin. Quantum repeaters: From quantum networks to the quantum internet. *Reviews of Modern Physics*, 95(4):045006, 2023.

[AFDF+18] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature communications*, 9(1):459, 2018.

[AFRV19] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *SIAM Journal on Computing*, 48(1):181–225, 2019.

[BA04] J. S. Bell and Alain Aspect. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*. Cambridge University Press, 2 edition, 2004.

[BCC+10] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6(9):659–662, 2010.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Review of Modern Physics*, 86(2):419–478, 2014.

[BFF21a] Peter Brown, Hamza Fawzi, and Omar Fawzi. Computing conditional entropies for quantum correlations. *Nature Communications*, 12(1), 2021.

[BFF21b] Peter Brown, Hamza Fawzi, and Omar Fawzi. Device-independent lower bounds on the conditional von Neumann entropy. *arXiv:2106.13692 [quant-ph]*, 2021.

[CH74] John F. Clauser and Michael A. Horne. Experimental consequences of objective local theories. *Physical Review D*, 10:526–535, 1974.

[CM11] Marcos Curty and Tobias Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Physical Review A*, 84(1):010304, 2011.

[CS12] Adán Cabello and Fabio Sciarrino. Loophole-free bell test based on local precertification of photon's presence. *Physical Review X*, 2(2):021010, 2012.

[CVP24] Anubhav Chaturvedi, Giuseppe Viola, and Marcin Pawłowski. Extending loophole-free nonlocal correlations to arbitrarily large distances. *npj Quantum Information*, 10(1), 2024.

[DFR20] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, 2020.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[Git] https://github.com/tristan-le-roy/Routed-DIQKD.

[GM87] Anupam Garg and N David Mermin. Detector inefficiencies in the einstein-podolsky-rosen experiment. *Physical Review D*, 35(12):3831, 1987.

[GPS10] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Physical Review Letters*, 105(7):070501, 2010.

[LLR+21] Wen-Zhao Liu, Ming-Han Li, Sammy Ragy, Si-Ran Zhao, Bing Bai, Yang Liu, Peter J. Brown, Jun Zhang, Roger Colbeck, Jingyun Fan, Qiang Zhang, and Jian-Wei Pan. Device-independent randomness expansion against quantum side information. *Nature Physics*, 17(4):448–451, 2021.

[LPP23] Edwin Peter Lobo, Jef Pauwels, and Stefano Pironio. Certifying long-range quantum correlations through routed bell tests. *arXiv:2310.07484 [quant-ph]*, 2023.

[LPT+13] Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin. Device-independent quantum key distribution with local bell test. *Physical Review X*, 3(3):031006, 2013.

[LZL+21] Ming-Han Li, Xingjian Zhang, Wen-Zhao Liu, Si-Ran Zhao, Bing Bai, Yang Liu, Qi Zhao, Yuxiang Peng, Jun Zhang, Yanbao Zhang, W. J. Munro, Xiongfeng Ma, Qiang Zhang, Jingyun Fan, and Jian-Wei Pan. Experimental realization of device-independent quantum randomness expansion. *Physical Review Letters*, 126(5):050503, 2021.

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, 2001.

[MFSR22] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. Generalised entropy accumulation. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 844–850, 2022.

[MIB+24] Michele Masini, Marie Ioannou, Nicolas Brunner, Stefano Pironio, and Pavel Sekatski. Joint-measurability and quantum communication with untrusted devices. *arXiv preprint arXiv:2403.14785*, 2024.

[MP03] Serge Massar and Stefano Pironio. Violation of local realism versus detection efficiency. *Physical Review A*, 68:062109, 2003.

[MS24] Michele Masini and Shubhayan Sarkar. One-sided di-qkd secure against coherent attacks over long distances. *arXiv preprint arXiv:2403.11850*, 2024.

[MW99] Ueli M Maurer and Stefan Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2):499–514, 1999.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Physical Review Letters*, 98:010401, 2007.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[PAM+10] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[Pea70] Philip M. Pearle. Hidden-variable example based upon data rejection. *Physical Review D*, 2:1418–1425, 1970.

[PNA10] Stefano Pironio, Miguel Navascués, and Antonio Acin. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIOPT*, 20(5):2157–2180, 2010.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000.

[SSC+11] Nicolas Sangouard, Bruno Sanguinetti, Noé Curtz, Nicolas Gisin, Rob Thew, and Hugo Zbinden. Faithful entanglement swapping based on sum-frequency generation. *Physical Review Letters*, 106(12):120403, 2011.

[SZB+21] Lynden K. Shalm, Yanbao Zhang, Joshua C. Bienfang, Collin Schlager, Martin J. Stevens, Michael D. Mazurek, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Mohammad A. Alhejji, Honghao Fu, Joel Ornstein, Richard P. Mirin, Sae Woo Nam, and Emanuel Knill. Device-independent randomness expansion with entangled photons. *Nature Physics*, 17(4):452–456, 2021.

[TW24] Ernest Tan and Ramona Wolf. Entropy bounds for device-independent quantum key distribution with local bell test, 2024.

[WLP12] Erik Woodhead, Charles Ci Wen Lim, and Stefano Pironio. Semi-device-independent qkd based on bb84 and a chsh-type estimation. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 107–115. Springer, 2012.

[Woo16] Erik Woodhead. Semi device independence of the bb84 protocol. *New Journal of Physics*, 18(5):055010, 2016.

[WP15] Erik Woodhead and Stefano Pironio. Secrecy in prepare-and-measure clauser-horne-shimony-holt tests with a qubit bound. *Physical Review Letters*, 115(15):150501, 2015.

[ZZHE93] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "“event-ready-detectors”" bell experiment via entanglement swapping. *Physical Review Letters*, 71(26):4287–4290, 1993.