Receiver-Device-Independent Quantum Key Distribution Protocols

Marie Ioannou, Pavel Sekatski, Alastair A. Abbott, Denis Rosset, Jean-Daniel Bancal, Nicolas Brunner

Receiver-Device-Independent Quantum Key Distribution Protocols

Marie Ioannou,[1] Pavel Sekatski,[1] Alastair A. Abbott,[1,2] Denis Rosset,[1] Jean-Daniel Bancal,[1,3] and Nicolas Brunner[1]

[1] *Department of Applied Physics University of Geneva, 1211 Geneva, Switzerland*
[2] *Univ. Grenoble Alpes, Inria, 38000 Grenoble, France*
[3] *Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191, Gif-sur-Yvette, France*

We consider a receiver-device-independent (RDI) approach to quantum key distribution. Specifically, we discuss protocols for a prepare-and-measure scenario and present a detailed security analysis. The sender's (Alice's) device is partially characterized, in the sense that we assume bounds on the overlaps of the prepared quantum states. The receiver's (Bob's) device requires no characterisation and can be represented as a black-box. Our protocols are therefore robust to any attack on Bob, such as blinding attacks. In particular, we show that a secret key can be established even when the quantum channel has arbitrarily low transmission by considering RDI protocols exploiting sufficiently many states. Finally, we discuss how the hypothesis of bounded overlaps can be naturally applied to practical devices.

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2] allows two users to establish a secret key via a quantum channel and an authenticated but public classical channel. QKD, together with the one time pad method, provides a secure method of communication with information-theoretical security [3]. Indeed, unlike classical schemes, the security of QKD protocols is physical: it only relies on some knowledge about the functioning of the devices controlled by the communicating parties and the general laws of quantum mechanics. Nevertheless, different approaches require different levels of detail in how the devices are modeled [4–7]. The "standard" approach presumes a full description of different elements in the setup. Such QKD systems are available commercially and can reach high rates over long distances.

However, relying on a detailed quantum model for characterizing the devices may open backdoors that quantum hackers can exploit. Indeed a mathematical model always represents (at best) an idealization of a practical device. For example, the well-known "blinding attacks" exploit the fact that standard models for describing photon detectors typically fail when the intensity of the incoming light falls outside their working range [8, 9]. When a fair-sampling type assumption is used on top of this, the door is open to attacks where an eavesdropper Eve obtains full information about the key, without introducing any detectable level of errors.

This motivates the investigation of the stronger, device-independent (DI) approach. Here, devices are viewed as classically controlled black boxes, and the security of QKD protocols can be demonstrated [10–13] assuming only that (i) the devices can be described accurately within quantum mechanics, and (ii) no information about the secret key leaks out of the laboratories of Alice and Bob (the two communicating parties). While this approach represents, in principle, the perfect solution to counter any hacking attack, its practical implementation is highly challenging, requiring the distribution of high-quality entanglement and notably high detection efficiencies (the best current protocol demands 68.5% [14]). First proof-of-principle experiments have recently been reported [14–16], but any practical implementation of DI QKD is arguably still far out of reach.

Beyond the standard (device-dependent) approach and the DI one, there exists a broad range of models that can be considered, where some of the devices are fully (or partially) characterized, while others are treated as black boxes. These include semi-DI [17–19], one-sided DI [20] and measurement-DI (MDI) [21, 22] protocols. While the last approach has been extensively studied and realized experimentally achieving record distances (see e.g. [23–26]), the former two models have been less explored and, thus far, not experimentally demonstrated.

In this work we propose a new approach, which we call "receiver-device-independent" (RDI). A specific example of such a protocol was recently presented, along with an experimental realisation, in the companion paper [27]. Here, we present a more general class of RDI-QKD protocols and provide a detailed theoretical analysis, investigating the possibilities and limits of QKD in RDI scenarios.

We thereby consider a prepare-and-measure scenario, where the sender (Alice) uses a partially characterized device, while the receiver (Bob) uses an untrusted device. The protocol being black-box on Bob's side, it is therefore inherently secure against attacks on the receiver, notably blinding attacks [8, 9]. On Alice's side, the characterisation we require consists in providing bounds on the (complex) overlaps of the prepared states (given formally by a Gram matrix). We moreover discuss how this hypothesis can be naturally applied to practical devices.

In practice, the RDI scenario can be quite naturally motivated. Consider for instance a large company communicating with an end-user. The latter has essentially no means to test their cryptographic device, which is therefore conveniently treated as a black-box. On the other hand, the company has access to advanced technology and technical expertise, and can therefore regularly test and characterize their cryptographic device. We note that the MDI approach is not applicable to this scenario, as both Alice and Bob require a trusted device (while

trust is then relaxed on an intermediate relay station).

The paper is organized as follows. In Section II we present the scenario of RDI QKD and discuss the key assumptions that are made, before outlining the RDI-QKD themselves in Section III. In Section IV we present a detailed security analysis. In the noiseless case we present an analytical security proof, showing that our protocols can achieve the maximal distance possible in an RDI scenario. Specifically, we show that it is possible to obtain a positive key rate for any transmission $\eta > 1/n$, where n denotes the states prepared by Alice, and corresponds also to the number of measurements performed by Bob. Hence by considering sufficiently many states, our RDI protocol can, in principle, accommodate any amount of losses. When noise is present, the security analysis relies on semidefinite programming, providing lower bounds on the key rate. Then, in Section V, we discuss the practical relevance of our RDI approach, in particular how bounds on the overlaps (Gram matrix) can be estimated and justified in practice. Finally, in Section VI we discuss how our protocol compares to other QKD protocols and scenarios.

II. SCENARIO

We consider a prepare-and-measure scenario as shown in Fig. 1. Alice sends, over a public quantum channel, one state out of a set of n states $\{|\psi_x\rangle\}_{x=0}^{n-1}$. Bob chooses among n measurements labelled by $y = 0, \ldots, n-1$. All measurements have binary outputs $b = 0, 1$. After many rounds, Alice and Bob can estimate the probability distribution $p(b|x, y)$. Bob's measurement device is completely uncharacterized and can be seen as a black box with an input y and an output b. The black box feature is a requirement if we aim to design a protocol robust to attacks where Eve controls Bob's device. The key assumption we make on the setup is about Alice's preparations. Namely, we assume that all inner-products $\gamma_{ij} = \langle\psi_i|\psi_j\rangle$ are bounded. These assumptions do not fix the total dimension of the Hilbert space and only partially characterize Alice's device.

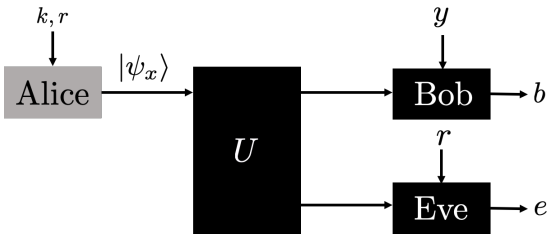

FIG. 1. Scenario: Alice and Bob can establish secret key based on the Gram matrix G of the set of states $\{|\psi_x\rangle\}_x$ prepared by Alice and the observed data $p(b|x, y)$. Eve has a complete control on the quantum channel, and can also have full knowledge of the functioning of the devices of Alice and Bob.

The assumption that Alice prepares pure states with known inner-products γ_{ij} simplifies the presentation and analysis of the protocol, but is evidently impossible to fulfil exactly in practice. In Sec. V we revisit this assumption on Alice's preparation device and show how the presence of noise, unavoidable in experiments, can also be analyzed within our framework in several ways. In particular, we show that the general situation where the preparation device is subject to fluctuating noise, which remains within a certain parameter window, can be analyzed by taking inequality constraints on (the real and imaginary parts of) the values γ_{ij}.

Besides the assumption on Alice's preparation device, specific to our protocol, we also make the standard QKD assumptions, also made in the DI scenario: (i) Alice's input x and Bob's measurement setting y are completely uncorrelated from Eve; (ii) Eve only has access to the classical and quantum communication specified by the protocol, she cannot gather any additional information about x and y; (iii) We assume the validity of quantum physics. In the following, Eve is restricted to collective attacks. She interacts with each round independently and can store her system in a quantum memory.

As we will see, a lower bound on the raw secret key rate, can be computed solely from the observed statistics $p(b|x, y)$, given that the setup satisfies the assumptions detailed above.

III. PROTOCOLS

In this section we describe the general structure of the RDI-QKD protocols we consider and give a family of concrete examples. For simplicity we do not treat the classical steps associated to parameter estimation, error correction, key extraction and authentication. Under the assumption of collective attacks these steps can be included easily following standard techniques [4, 7]. The security analysis under coherent attacks is left out for future work.

A. General structure

We begin by presenting the general structure of our RDI-QKD protocols.

Consider a given ensemble of states $\{|\psi_x\rangle\}_{x=0}^{n-1}$ that Alice is able to prepare and binary measurements $\{B_{0|y}, B_{1|y}\}_{y=0}^{n-1}$ that Bob can perform. We can now define protocols with a general structure as follows.

RDI-protocol Steps to generate a sifted key between Alice and Bob.

Alice and Bob share an authenticated classical channel as well as a quantum channel.

1. **Raw key generation**
   1: Alice randomly chooses a pair of integers $\mathbf{r} = (r_0, r_1)$ with $0 \leq r_0 < r_1 \leq n-1$ and a bit $k = 0, 1$. According to her choice she sends the state $|\psi_{x=r_k}\rangle$ over the quantum channel to Bob.
   2: Bob randomly chooses an integer y with $0 \leq y \leq n-1$ and performs the binary measurement $\{B_{0|y}, B_{1|y}\}$ on the state received from Alice.
2. **Sifting**
   Alice and Bob use the classical channel to communicate.
   1: **if** $b = 1$ **then**
   2: Bob tells Alice to discard the round.
   3: **else if** $b = 0$ **then**
   4: Bob asks Alice to reveal $\mathbf{r}$.
   5: Alice reveals $\mathbf{r}$.
   6: **if** $y = r_0$ **or** $y = r_1$ **then**
   7: Bob tells Alice the round is conclusive.
   8: **else**
   9: Bob tells Alice to discard the round.
   10: **end if**
   11: **end if**

This structure defines a broad class of protocols specified by the choices of n, the states $\{|\psi_x\rangle\}_{x=0}^{n-1}$, and the measurements $\{B_{0|y}, B_{1|y}\}_{y=0}^{n-1}$. In general, the idea is to choose states and measurements such that, in Step 2.7, Bob can readily infer from the observed outcome b what the key bit k of Alice is. Below we will describe in more detail some specific such examples, which will clarify the principles behind the RDI protocols we describe.

B. Ideal qubit protocol

We describe a class of protocols based on qubit states and measurements. These can be considered ideal protocols in the sense of robustness to loss and noise.

Alice prepares states from a set of n single-qubit states $\{|\psi_x\rangle\}_{x=0}^{n-1}$ with

$$|\psi_x\rangle = \cos(\theta/2)\,|0\rangle + e^{\frac{i2\pi}{n}x}\sin(\theta/2)\,|1\rangle \tag{1}$$

for some given θ. Following the general protocol outlined above, to encode the raw key bit Alice chooses a pair of integers $\mathbf{r} = (r_0, r_1)$ with $0 \leq r_0 < r_1 \leq n-1$, among $\binom{n}{2}$ possible pairs. For a key bit k, Alice sets $x = r_k$. Note that every state x can encode the bit value 0 or 1. Alice sends $|\psi_{x=r_k}\rangle$ via the quantum channel to Bob. Bob has $y = 0, \ldots, n-1$ measurements and each measurement has a binary output $b = 0, 1$. The output $b = 1$ corresponds to a projection onto $|\psi_y\rangle$ while $b = 0$ corresponds to the projection on the orthogonal subspace $\mathbb{1} - |\psi_y\rangle\langle\psi_y|$. If Bob observes $b = 0$, he can with certainty exclude the state $x = y$. We refer to the rounds where $b = 0$ as conclusive rounds. If the round is conclusive, Bob asks Alice to reveal $\mathbf{r}$. If $y = r_0$ or $y = r_1$, Bob is able to infer the raw key bit and announces to Alice that the round is successful; otherwise he tells Alice to discard the round. The performance of this protocol, with respect to noise and loss, is described below in Section IV B. Moreover, in Section IV C we show that this protocol is optimal within RDI-QKD protocols in the sense that it yields a positive key rate for any $\eta > \frac{1}{n}$, arbitrarily close to the threshold of $1/n$ beyond which no secret key can be established.

C. Towards practical protocols

While the above ideal qubit protocol is useful to test the limits of model, the RDI approach can also be used quite naturally, and give good protocols, in more realistic setups.

Firstly, the requirement that Alice prepares pure states is not necessary. Indeed, the case of mixed states can naturally be encompassed by considering purifications of the states Alice prepares. We discuss how to take into account the overlap assumption on Alice's device in this case in Section V A.

Secondly, the qubit protocol described above can be adapted quite naturally to an optical setup, where a dimension bound on the states Alice prepares is unrealistic. This is because only the overlaps of the prepared states is required (their Gram matrix), but not their Hilbert space dimension. One can therefore consider a protocol where polarized coherent states of light are prepared, as reported recently in the companion paper [27]. Therein a proof-of-principle implementation of such a protocol was reported, achieving finite-size key over a 4.8km optical fiber.

IV. SECURITY ANALYSIS

Eve's information about the secret bit k is bounded by assuming that the Gram matrix G of the set of encoding states is fully characterized and that the probabilities $p(b|x, y)$ are perfectly estimated by Alice and Bob. The Gram matrix G is a Hermitian matrix whose entries are given by

$$G_{ij} = \langle\psi_i|\psi_j\rangle\,. \tag{2}$$

We do not bound the dimension of the Hilbert space associated to the system sent by Alice. However, under the assumption that Alice prepares pure states the rank of the Gram matrix equals the dimension of the subspace spanned by these states. Recall that this assumption is not indispensable for our analysis, and will be relaxed in Sec. V. Furthermore, no characterization of the exact encoding, transmission channel nor measurement device is needed. Eve can correlate herself to the states prepared by Alice, she can design Bob's measurement device by

the means of an ancilla and a unitary operation, and she can use a quantum memory to keep her ancilla until the end of the classical post-processing (cf. Fig. 1). In fact, she can keep her ancilla until any later time and wait until the reconciliation between Alice and Bob is over in order to perform a measurement allowing her to extract as much information as possible about the secret bit k.

The asymptotic key rate (per round) is lower bounded by [28]

$$[H(k|\text{Eve, succ}) - H(k|\text{Bob, succ})]\, p(\text{succ}), \tag{3}$$

where $H(k|\text{Eve(Bob)}, \text{succ})$ is the entropy of k conditional on Eve(Bob) and the fact that a round is not discarded, and $p(\text{succ})$ is the probability that a round is not discarded. Bob's entropy can be upper-bounded as $H(k|\text{Bob}, \text{succ}) \leq H_2(\text{QBER})$, where $H_2(\cdot)$ is the binary entropy and QBER is the quantum bit error rate. Eve's conditional entropy can be lower-bounded by the conditional min entropy

$$\begin{aligned} H(k|\text{Eve}, \text{succ}) &\geq H_{\min}(k|\text{Eve}, \text{succ}) \\ &= -\log_2 \left(p_g(e = k|\text{succ})\right), \end{aligned}$$

which is in a one-to-one relation with the maximal probability $p_g(e = k|\text{succ})$ that Eve guesses the bit k correctly [29] if the round was not discarded. Combing the two arguments, we can lower bound the key rate by the quantity

$$R = [-\log_2 \left(p_g(e = k|\text{succ})\right) - H_2(\text{QBER})]\, p(\text{succ}). \tag{4}$$

The QBER and $p(\text{succ})$ are extracted from the observed statistics $p(b|x, y)$ while the guessing probability $p_g(e = x|\text{succ})$ needs to be upper bounded in order to give a lower bound on R. Note that $p(\text{succ}) > 0$: if $p(\text{succ}) = 0$ there is no raw key generation and hence nothing for Eve to guess. The guessing probability is given by

$$\begin{aligned} p_g(e = k|\text{succ}) &= \frac{p(e = k, \text{succ})}{p(\text{succ})} \\ &= \frac{\sum_{r=0}^{\binom{n}{2}-1} p_R(r) \sum_{k=0}^{1} p_K(k) \sum_{y=0}^{n-1} p_Y(y) \operatorname{tr}\left(\rho_{r_k}^{BE} M_{1|y} E_{k|r}\right)(\delta_{y,r_0} + \delta_{y,r_1})}{\sum_{r=0}^{\binom{n}{2}-1} p_R(r) \sum_{k=0}^{1} p_K(k) \sum_{y=0}^{n-1} p_Y(y) \operatorname{tr}\left(\rho_{r_k}^{BE} M_{1|y} \mathbb{1}\right)(\delta_{y,r_0} + \delta_{y,r_1})}, \end{aligned} \tag{5}$$

where $M_{b|y}$ are Bob's measurement operators with $b = 0, 1$ and $y = 0, \ldots, n-1$, and $E_{k|r}$ are Eve's measurement operators with $k = 0, 1$ and $r = 0, \ldots, \binom{n}{2} - 1$. $p_R(r)$, $p_Y(y)$ and $p_K(k)$ are the probabilities of choosing the inputs r, y and k. Hence, $\sum_r p_R(r) = \sum_k p_K(k) = \sum_y p_Y(y) = 1$, $p_K(k) \geq 0\ \forall k$, $p_Y(y) \geq 0\ \forall y$ and $p_R(r) \geq 0\ \forall r$. Here we will always we take the input probabilities to be uniformly random over all inputs. As already mentioned, the dimension of the problem is not bounded, so without loss of generality we can, using Naimark's dilation theorem, assume that Bob's and Eve's measurements are projectors satisfying the following properties:

$$\begin{aligned} &M_{b|y} M_{b'|y} = \delta_{b,b'} M_{b|y} && \forall y \\ &\sum_b M_{b|y} = \mathbb{1} && \forall y \\ &E_{e|\mu} E_{e'|\mu} = \delta_{e,e'} E_{e|\mu} && \forall \mu \\ &\sum_e E_{e|\mu} = \mathbb{1} && \forall \mu \\ &[M_{b|y}, E_{e|\mu}] = 0 && \forall b, e, y, \mu. \end{aligned} \tag{6}$$

The last property comes from the fact that Bob and Eve act on two different Hilbert spaces.

A. Semidefinite programming approach

Since $p(\text{succ})$ is extracted from the observed statistics, to upper bound $p_g(e = k|\text{succ})$ we need just to upper bound $p(e = k, \text{succ})$. To do this, we will use the method presented in [30]. In particular, we use the approach described therein which provides a semidefinite programming (SDP) hierarchy giving increasingly tight outer approximations of the set of quantum correlations in discrete prepare-and-measure scenarios compatible with a given Gram matrix. The hierarchy is known to converge to the actual set of quantum correlations, whereas for a fixed level it provides a tractable method of bounding the guessing probability over correlations compatible with the observed statistics. This problem would, without the hierarchy, be computationally intractable since no bound on the Hilbert space dimension is assumed.

Let $\{S_i\}_{i=0}^{s-1}$ be a set of measurement operators and define the moment matrix Γ of size $ns \times ns$ as

$$\Gamma = \sum_{x,x'=0}^{n-1} \Gamma_{xx'} \otimes |\hat{e}_x\rangle\langle\hat{e}_{x'}|, \tag{7}$$

where $\{|\hat{e}_x\rangle\}_{x=0}^{n-1}$ is an orthonormal basis of $\mathbb{R}^n$ and we recall that n is the number of states prepared by Alice.

The sub-blocks $\Gamma_{xx'}$ are defined as

$$\Gamma_{xx'} = \sum_{i,j=0}^{s-1} \langle\psi_x| S_i^\dagger S_j |\psi'_x\rangle \otimes |\hat{\hat{e}}_j\rangle\langle\hat{\hat{e}}_j| \tag{8}$$

where $\{|\hat{\hat{e}}_i\rangle\}_{i=0}^{s-1}$ is an orthonormal basis of $\mathbb{R}^s$. It is easily shown that the moment matrix Γ is positive semidefinite. The elements of the set $\{S_i\}_{i=0}^{s-1}$ are monomials of the operators $B_{b|y}$ and $E_{e|\mu}$. This set of operators can be chosen arbitrarily but the aim is to have as many linearly independent operators as possible in the moment matrix. By taking all monomials of measurement operators up to a given order, we can define different levels of the hierarchy. The first two levels are given, e.g., by the two following sets of operators:

$$\begin{aligned} \mathcal{S}_1 &= \{\mathbb{1}, B_{b|y}, E_{e|\mu}\}, \\ \mathcal{S}_2 &= \mathcal{S}_1 \cup \{B_{b|y}B_{b'|y'}, E_{e|\mu}E_{e'|\mu'}, B_{b|y}E_{e|\mu}\}, \end{aligned} \tag{9}$$

and the levels $\mathcal{S}_n$ for $n > 2$ can likewise be defined inductively. Ref. [30] proved that as n goes to infinity (i.e., in the infinite level limit), the hierarchy converges to the set of quantum correlations.

For the sake of clarity, we define $\Gamma^{ST}_{xx'} := \langle\psi_x| S^\dagger T |\psi_{x'}\rangle$ with $S, T \in \mathcal{S}$ and $x, x' = 0, ..., n-1$. The SDP upper bounding $p(e = x, \text{succ})$ is given by

$$\max_{\Gamma} \quad \frac{1}{(n-1)n^2} \sum_{r=0}^{\binom{n}{2}} \sum_{k=0}^{1} \sum_{y=0}^{n-1} \Gamma^{B_{0|y}E_{r_k|r}}_{r_k r_k} (\delta_{y,r_0} + \delta_{y,r_1}) \tag{10a}$$

$$\text{s.t.} \quad \Gamma^{\mathbb{1}\mathbb{1}}_{xx'} = \langle\psi_x|\psi_{x'}\rangle = \gamma_{xx'} \qquad \forall x, x' \tag{10b}$$

$$\Gamma^{\mathbb{1}B_{b|y}}_{xx} = p(b|x,y) \qquad \forall b, x, y \tag{10c}$$

$$\text{tr}(\Gamma_{xx'} F_k) = f_k \qquad k = 0, \ldots, m, \forall x, x' \tag{10d}$$

$$\Gamma \succeq 0. \tag{10e}$$

The overlap constraint between the set of states is enforced by Eq. (10b). Eq. (10c) enforces the moment matrix Γ to be compatible with the observed correlations $p(b|x,y)$. Eq. (10d) encodes the constraints on Bob's and Eve's operators given by Eq. (6), as well as the constraints between elements of $\Gamma_{xx'}$ implied by the fact that $\Gamma^{ST}_{xx'} = \Gamma^{S'T'}_{xx'}$ whenever $S^\dagger T = S'^\dagger T'$ (cf. Prop. 4 of Ref. [31]).

B. Security analysis of the ideal qubit protocol

Here, we will analyze the security of the idealized qubit protocol presented in Section III B, including in the presence of loss and noise. We will model noise by the means of a depolarizing channel with parameter $\lambda \in [0, 1]$, which replaces the transmitted state with a maximally mixed state with probability λ [32]. Loss is modeled by a binary erasure channel [32] with erasure probability $(1-\eta)$, $\eta \in [0, 1]$. Such a model of loss assumes that loss is orthogonal with respect to the encoding, which is typically the case if one considers, e.g., the polarization of photons for the encoding of the secret bit.

The Gram matrix G corresponding to the set of states (1) prepared by Alice is given by

$$G_{ij} = \cos^2(\theta/2) + e^{i\frac{2\pi(i-j)}{n}} \sin^2(\theta/2) \tag{11}$$

with $i, j = 1, ..., n$. The probability distribution is then given by

$$p(b = 0|x, y) = \eta \left(\frac{\lambda}{2} + (1-\lambda) \sin^2(\theta) \sin^2 \left(\frac{\pi(x-y)}{n} \right) \right). \tag{12}$$

Given the Gram matrix G of (11) and the observed probability distribution one can upper bound the secret key rate as shown previously. Figure 2 shows the raw key rate as a function of the transmission η for different QBER's and values of n. For each η we numerically optimized over θ to obtain the optimal R. We notice that the lower-bound on the key rate goes asymptotically to zero as $\eta \to 1/n$. This is optimal because at $\eta = 1/n$, Eve can break the security by intercepting the states sent by Alice and forcing Bob's detector according to her outcome and Bob's input (see Section IV C). Therefore, for any prepare-and-measure protocol, the key rate is null for $\eta \leq 1/n$.

Interestingly, B92 [33] is a special case of the proposed protocol with $n = 2$ and a fixed $\theta = \frac{\pi}{4}$. Under the same assumptions, our protocol outperforms B92 with respect to the transmission and the noise tolerance, see Fig. 3. Also, BB84 [34] under the same assumptions is outrun by our protocol with 3 states.

C. Analytical bounds

In this section we prove analytically that, if Alice prepares sufficiently many states, the protocol can in principle tolerate arbitrary small transmission η. First, with an explicit attack from Eve we lower bound the transmission η required to have $R > 0$. (Proposition 1). Secondly, we show that this bound is tight as long as G is chosen to obey an additional natural condition (Proposition 2). That is, for any transmission η exceeding the threshold, Eve is unable to guess the secret bit with certainty in all rounds, giving rise to a positive key rate.

Transmission loss in the line (scaling with distance) and finite detection efficiency are the bottlenecks in most QKD protocols. Both effects give rise to a loss channel and contribute to the total transmission η. In this section we assume that this loss is the only imperfection in the setup. This captures the main limiting factor of real QKD setups and allows us to derive relatively simple analytical bounds. We assume that loss is orthogonal with respect to the secret bit encoding, such that with probability η the system sent by Alice is lost and Bob observes a third outcome (e.g., a no-click event $b = \emptyset$). Bob then attributes it the value $b = 1$, such that the rounds

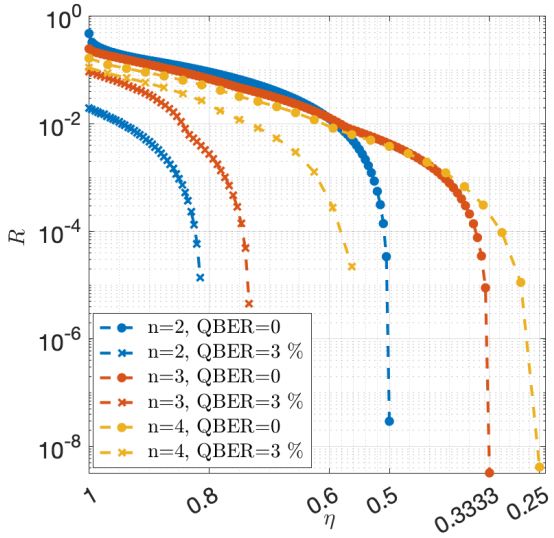

FIG. 2. Raw key rate for our RDI-QKD protocol. The graph shows the lower bound on the raw key rate R as a function of the transmission for different number of states and QBER's. For n states, the noiseless protocol has a positive key rate down to $\eta = 1/n$, which is the minimal transmission for which this is possible in any prepare-and-measure scenario. The protocol is also tolerant to noise in state preparation.

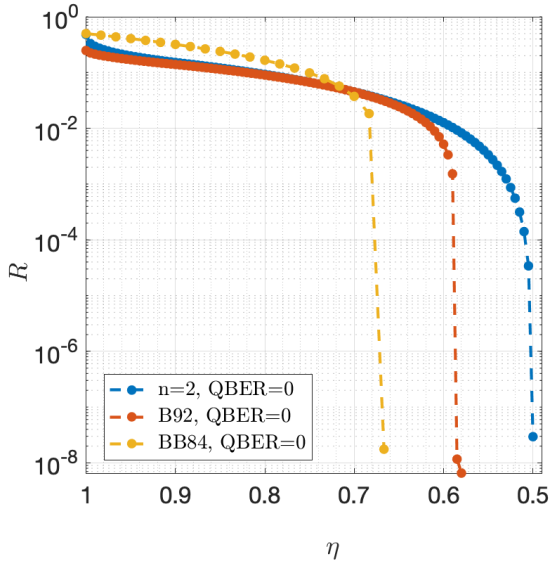

FIG. 3. Comparison of our RDI-QKD protocol with other protocols under the same assumptions. The RDI protocol with $n = 2$ outperforms BB84 and B92.

where the system sent by Alice is lost are rejected in the protocol.

In this case any protocol with a Gram matrix $G_{ij} = \langle\psi_i|\psi_j\rangle$ with $i, j = 0, \ldots, n-1$ and the honest measurements $B_{1|y} = |\psi_y\rangle\langle\psi_y|$ with $B_{0|y} = \mathbb{1} - B_{1|y}$ leads to measurement probabilities

$$\begin{aligned} p(b=0|x,y) &= \eta(1-|G_{xy}|^2), \\ p(b=1|x,y) &= 1 - p(b=0|x,y), \end{aligned} \tag{13}$$

with $x, y = 0, \ldots, n-1$. One notes that with such probabilities $p(0|x=y) = 0$: Bob's bits are perfectly correlated to Alice's after the sifting, i.e. $H_2(\mathrm{QBER}) = 0$. For the following, we define $\lambda_{\min}(G)$ as the minimal non-zero eigenvalue of the Gram matrix G.

Proposition 1. *Given a Gram matrix $G \in \mathbb{C}^{n\times n}$ and measurement probabilities of Eq. (13), a necessary condition for $R > 0$ is that $\eta > \frac{1}{n-\lambda_{\min}(G)}$.*

Proof. Let us assume that with probability q Eve intercepts the state sent by Alice and makes an unambiguous state exclusion measurement $M_i = \mu(\mathbb{1} - |\psi_i\rangle\langle\psi_i|)$ with $i = 0, \ldots, n-1$, $\mu \in [0, 1]$ and $M_n = \mathbb{1} - \sum_{i=0}^{n-1} M_i$.

If Eve obtains an outcome $i < n$, she can exclude with certainty the state $|\psi_i\rangle$, whereas if she gets the outcome n she cannot conclude anything. In order to have as many conclusive outcomes as possible Eve maximizes μ under the constraint $M_n \geq 0$:

$$\begin{aligned} \max_{\mu} \quad & \mu \\ \text{s.t.} \quad & \mathbb{1}\frac{(n\mu-1)}{\mu} \leq \sum_{i=0}^{n-1} |\psi_i\rangle\langle\psi_i|, \\ & \mu \geq 0. \end{aligned} \tag{14}$$

The first constraint in Eq. (14) is satisfied if the eigenvalues of $\sum_{i=0}^{n-1} |\psi_i\rangle\langle\psi_i|$ are all larger than $\frac{(n\mu-1)}{\mu}$. But the eigenvalues of $\sum_i |\psi_i\rangle\langle\psi_i|$ coincide with the nonzero eigenvalues of the Gram matrix G. Hence, the above maximization is satisfied if $\frac{(n\mu-1)}{\mu} \leq \lambda_{\min}(G)$. This leads to an optimal $\mu^* = \frac{1}{n-\lambda_{\min}(G)}$ and $p(i|x) = \mu^*(1-|G_{xi}|^2)$. The result i of Eve's measurement is then sent to Bob's detector which only outputs $b = 0$ if $y = i$, i.e. $p(b = 0|y, i) = \delta_{y,i}$. The resulting probability observed by Bob is

$$\begin{aligned} p(b=0|x,y) &= \sum_{i=0}^{n} p(b=0|i,y)p(i|x) \\ &= \mu^*(1-|G_{xy}|^2). \end{aligned} \tag{15}$$

With probability $(1-q)$ Eve does not intercept the message, and Bob's detector is instructed to perform the ideal measurement $p(b = 0|x, y) = (1 - |G_{xy}|^2)$. Eve wants to remain undetected and hence needs to reproduce the expected statistics of Eq. (13). Her attack must thus satisfy the equality

$$\eta(1-|G_{xy}|^2) = q\mu^*\big(1-|G_{xy}|^2\big)+(1-q)(1-|G_{xy}|^2)\big) \tag{16}$$

for all x, y. This implies that Eve can not intercept the message more often than in a fraction $q = \frac{1-\eta}{1-\mu^*}$ of rounds. In particular, if $q = \frac{1-\eta}{1-\mu^*} \geq 1$ or $\eta \leq \frac{1}{n-\lambda_{\min}(G)}$ she can intercept the message in every round resulting in $p(y = i|\mathrm{succ}) = p_g(e = k|\mathrm{succ}) = 1$ and $R = 0$. □

More generally, this attack gives a lower bound on Eve's guessing probability as

$$p_g(e=k|\text{succ}) \geq q + (1-q)\frac{1}{2} = \frac{1}{2}\left(1 + \frac{1-\eta}{\eta(n-(1+\lambda_{\min}(G))}\right), \tag{17}$$

with equality if $p_g(e=k|\text{succ}) = \frac{1}{2}$ for the honest implementation at $\eta = 1$.

For the considered family of protocols the proposed attack allows Eve to guess the secret bit k of Alice perfectly whenever one has $\eta \leq \frac{1}{n-\lambda_{\min}(G)}$. The converse question is whether, for any transmission exceeding this value, there exists a protocol (with a given n and $\lambda_{\min}(G)$) yielding a strictly positive key rate. We will now show that this is indeed the case by considering a qubit protocol with $\text{rank}(G) = 2$, as discussed in Sec. III B.

Proposition 2. *Consider a Gram matrix G, with $\text{rank}(G) = 2$, leading to measurement probabilities in Eq. (13). If the transmission exceeds $\eta > \frac{1}{n-\lambda_{\min}(G)}$, then one can obtain a positive key rate, i.e., $R > 0$.*

Proof. Since in our case $H_2(\text{QBER}) = 0$, from Eq. (4) one sees that the condition $R > 0$ is equivalent to $p_g(e = k|\text{succ}) < 1$, that is Eve can not always guess the secret bit with certainty. Thus, we want to prove $p_g(e = k|\text{succ}) < 1$. To do so we will proceed by assuming $p_g(e = k|\text{succ}) = 1$ and reach a contradiction.

To start, it is convenient to replace our prepare-and-measure scenario by an equivalent entanglement-based scenario. Alice prepares an entangled state

$$|\Phi\rangle_{AA'} = \frac{1}{\sqrt{n}}\sum_{x=1}^{n} |x\rangle_A |\psi_x\rangle_{A'}, \tag{18}$$

sends out A' and measures A in the computational basis $\{|x\rangle\langle x|\}_{k=0}^{n-1}$ to obtain x. Since the states $\{|\psi_x\rangle\}_x$ span a 2-dimensional space, by the Schmidt theorem the state $|\Phi\rangle_{AA'} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is a two qubit state.

Without loss of generality an attack performed by Eve starts with an isometry U mapping A' onto systems B and E of arbitrary dimension

$$U : |\Phi\rangle_{AA'} \mapsto |\Psi\rangle_{ABE} = \mathbb{1}_A \otimes U_{A'} |\Phi\rangle_{AA'}. \tag{19}$$

In addition Eve chooses a set of binary measurements $\{B_{0|y}, B_{1|y}\}$ acting on B. The combinations of the isometry and the measurements on B define the measurements on the system A' via

$$M_{b|y} = U_{A'}^{\dagger}\left(B_{b|y} \otimes \mathbb{1}_E\right) U_{A'}. \tag{20}$$

Furthermore these measurements are constrained to satisfy $\langle\psi_x| M_{b|y} |\psi_x\rangle = p(b|x,y)$ by the probabilities observed by Alice and Bob in Eq. (13). From $\langle\psi_y| M_{0|y} |\psi_y\rangle = 0$, one concludes that $M_{0|y} \propto \mathbb{1} - |\psi_x\rangle\langle\psi_x|$. Any of the remaining probabilities $\langle\psi_{x\neq y}| M_{0|y} |\psi_{x\neq y}\rangle$ implies

$$M_{0|y} = \eta(\mathbb{1} - |\psi_x\rangle\langle\psi_x|) = \eta\,|\psi_y^{\perp}\rangle\langle\psi_y^{\perp}|. \tag{21}$$

This form of $M_{0|y}$ is very restrictive for Eve. In particular, it projects $|\Phi\rangle_{AA'}$ into a product state

$$\mathbb{1}_A \otimes \sqrt{M_{0|y}}\,|\Phi\rangle_{AA'} = \sqrt{p(b=0|y)}\left|\xi^{(0|y)}\right\rangle_A \left|\phi^{(0|y)}\right\rangle_{A'}, \tag{22}$$

with $p(b=0|y) = \frac{1}{n}\sum_x p(b=0|x,y)$. This identity can be put in the form

$$\sqrt{B_{0|y}}\otimes\mathbb{1}_{AE}\,|\Psi\rangle_{ABE} = \sqrt{p(b=0|y)}\left|\xi^{(0|y)}\right\rangle_A \left|\Psi^{(0|y)}\right\rangle_{BE}. \tag{23}$$

From here we can define the marginal state of Alice and Eve conditional to Bob measuring y and obtaining 0

$$\rho_{AE|B}^{(0|y)} = \left|\xi^{(0|y)}\right\rangle\!\left\langle\xi^{(0|y)}\right|_A \otimes \rho_E^{(0|y)} \quad \text{with} \quad \rho_E^{(0|y)} = \text{tr}_B \left|\Psi^{(0|y)}\right\rangle\!\left\langle\Psi^{(0|y)}\right|_{BE}. \tag{24}$$

Remarkably, Eve's state is no longer influenced by any manipulations done by Alice, and in particular by her measurement result x. That is, conditionally on y Eve's state is independent of x. This means that after the sifting Eve can only guess x perfectly ($p_g(e = k|\text{succ}) = 1$), if she can guess y perfectly. Formally,

$$p_g(e=k|\text{succ}) = 1 \implies \frac{1}{2}\left\|\rho_E^{(0|y)} - \rho_E^{(0|y')}\right\| = 0 \quad \forall\, y \neq y'. \tag{25}$$

Let us now show that this imposes some conditions on the probabilities $p(b = 0|y)$. To do so consider the trivial inequality

$$\rho_E = p(b=0|y)\rho_E^{(0|y)} + (1-p(b=0|y))\rho_E^{(1|y)}, \tag{26}$$

where $\rho_E = \text{tr}_{AB}\,|\Psi\rangle\langle\Psi|_{ABE}$ and $(1-p(b=0|y))\rho_E^{(1|y)} = \text{tr}_{AB}\left[(B_{1|y}\otimes\mathbb{1}_{AE})\,|\Psi\rangle\langle\Psi|_{ABE}\right]$, which implies

$$\rho_E - p(b=0|y=0)\rho_E^{(0|0)} \geq 0. \tag{27}$$

But because the state $\rho_E^{(0|0)}$ and $\rho_E^{(0|1)}$ have orthogonal support, we also obtain

$$\rho_E - p(b=0|y=0)\rho_E^{(0|0)} - p(b=0|y=1)\rho_E^{(0|1)} \geq 0. \tag{28}$$

By recursion we obtain the bound

$$\rho_E - \sum_y p(b=0|y)\rho_E^{(0|y)} \geq 0 \qquad 1 - \sum_y p(b=0|y) \geq 0 \qquad \sum_y p(b=0|y) \leq 1 \tag{29}$$

on the average probability of the $b = 0$ outcome. With the help of Eq. (13) this bound can be written as

$$\eta \leq \frac{1}{\frac{1}{n}\sum_{x,y}(1-|G_{xy}|^2)}. \tag{30}$$

This bound is, however, worse that the one in the statement of the theorem. Let us now show how to match the two. For this we consider a thought experiment where Alice prepares some pure state

$$|\widetilde{\Phi}\rangle_{AA'} \in \mathbb{C}^2 \otimes \mathbb{C}^2. \tag{31}$$

As $M_{0|y} = \eta \left|\psi_y^{\perp}\right\rangle\!\left\langle\psi_y^{\perp}\right|$ is proportional to projector on a state, one has, analogously to Eqs. (22)–(23),

$$\left(\sqrt{B_{0|y}} \otimes \mathbb{1}_{AE}\right) U_{A'} \left|\widetilde{\Phi}\right\rangle_{AA'} = \sqrt{\widetilde{p}(0|y)} \left|\widetilde{\xi}^{(0|y)}\right\rangle_{A} \left|\Psi^{(0|y)}\right\rangle_{BE},$$

with the same state $\left|\Psi^{(0|y)}\right\rangle_{BE}$. Hence the marginal state $\rho_E^{(0|y)}$ are also the same, and satisfy

$$\widetilde{\rho}_E = \widetilde{p}(b|y)\rho_E^{(0|y)} + (1-\widetilde{p}(0|y))\rho_E^{(1|y)} \tag{32}$$

for $\widetilde{\rho}_E = \mathrm{tr}_{AB}[U_{A'} |\widetilde{\Phi}\rangle\!\langle\widetilde{\Phi}|_{AA'} U_{A'}^{\dagger}]$. We can now repeat the arguments of Eqs. (28)–(29) to obtain the bound

$$\sum_y \widetilde{p}(0|y) \leq 1, \tag{33}$$

valid for the sum of probabilities

$$\begin{aligned}\sum_y \widetilde{p}(0|y) &= \mathrm{tr}_{AA'}\left[\left(\mathbb{1}_A \otimes \sum_y M_{0|y}\right) |\widetilde{\Phi}\rangle\!\langle\widetilde{\Phi}|_{AA'}\right] \\ &= \mathrm{tr}_{A'}\left[\left(\sum_y M_{0|y}\right)\rho_{A'}\right]\end{aligned} \tag{34}$$

coming from any state $\rho_{A'}$. Choosing the state which maximizes the bound $\max_{\rho_{A'}} \mathrm{tr}\left[\rho_{A'}(\sum_y M_{0|y})\right] = \|\sum_y M_{0|y}\|$, one obtains

$$\begin{aligned}\left\|\sum_y M_{0|y}\right\| &\leq 1 \\ \eta\left\|\sum_y (\mathbb{1} - |\psi_y\rangle\!\langle\psi_y|)\right\| &\leq 1 \\ \eta\big(n - \lambda_{\min}(G)\big) &\leq 1 \\ \eta &\leq \frac{1}{n-\lambda_{\min}(G)},\end{aligned} \tag{35}$$

where we used the fact that G and $\sum_y |\psi_y\rangle\!\langle\psi_y|$ have the same eigenvalues. Hence, having $p_g(e = k|\mathrm{succ}) = 1$ and $\eta > \frac{1}{n-\lambda_{\min}(G)}$ is impossible, which concludes the proof. □

Propositions 1 and 2 imply that, for any transmission η, there exists a RDI-QKD protocol involving $n > \frac{1}{\eta}$ different measurements performed by Bob which yields a positive key rate. In particular, as follows from the proof of Propostion 2, this is achieved by the ideal qubit protocol of Sec. III B by choosing $\lambda_{\min}(G) < n - \frac{1}{\eta}$. Conversely, in the RDI setting where Bob can do n different measurements labeled by the settings y, Eve can always perform a "blinding" attack and obtain a perfect copy of Bob's registers. To do so she performs one of the possible measurements y' at random, records the outcome e, and sends a copy of e and y' to Bob's detector. When Bob performs his measurement with a setting y, the detector reveals $b = e$ if $y = y'$ and pretends that the system was lost $b = \emptyset$ otherwise. Since $p(y' = y|y) = 1/n$, for $\eta < \frac{1}{n}$ Eve is left with a perfect copy of Bob's registers (b, y) whenever the detection is successful $b \neq \emptyset$.

D. Importance of the choice of the Gram matrix

As we saw in the previous section, if one chooses the n states $\{|\psi_x\rangle\}_x$ well then one can obtain $R > 0$, and thus a positive key rate, whenever $\eta > 1/n$. In this section, we show that it is indeed important to choose the Gram matrix constraining the preparations with some care. In particular, we show that for a seemingly natural choice of Gram matrix the critical transmission, below which no key can be obtained, is significantly worse: Alice and Bob will not be able to provide a nontrivial lower bound on the key rate if there is more than 50% loss, i.e. if $\eta > 1/2$.

We assume thus that Alice prepares a set of n quantum states compatible with the Gram matrix $G_{xx'} = \langle\psi_x|\psi_{x'}\rangle = d$ with $d \in (0, 1)$ for all $x \neq x'$ and that the observed statistics are given by Eq. (13). Since $\mathrm{rank}(G) = n$, the states she prepares are necessarily linearly independent. As a result, there exists an unambiguous state discrimination (USD) measurement [35]. Because of the symmetry, we consider an equiprobable USD and the probability of a conclusive discrimination is given by the smallest eigenvalue of the Gram matrix which is in our case equal to $1 - d$ [36].

We assume that Eve performs an intercept-resend attack such that with a probability $0 \leq q \leq 1$ she performs USD and forces Bob's detection, and with a probability $1 - q$ she leaves the state untouched and guesses at random. Given that $x \neq y$, if Eve attacks the USD is conclusive with a probability $1 - d$ and if she does not intercept the state Bob gets $b = 0$ with a probability $\eta(1-d^2)$. Eve wants her attack to remain unnoticed and this fixes the probability q of intercepting the state to $q = \frac{(1+d)(1-\eta)}{d}$.

The probability that Eve successfully guesses the secret bit is then given by

$$p_g(e = x|\mathrm{succ}) = \frac{1-\eta(1-d)}{2d\eta}. \tag{36}$$

Eve thus has entire knowledge of the secret bit string, i.e., $p_g(e = k|\mathrm{succ}) = 1$, for $\eta = \frac{1}{1+d} > \frac{1}{2}$. Hence, considering identical real overlaps prevents Alice and Bob from obtaining a positive key rate for more than 50% loss.

V. BRIDGING THE GAP BETWEEN THE PROTOCOLS AND PRACTICAL IMPLEMENTATIONS

Our receiver-device independent setting assumes the characterization of Alice's state preparation device, given by the Gram matrix

$$\text{Alice} \simeq G. \tag{37}$$

When Alice prepares pure states, as we have assumed so far, the Gram matrix gives an exhaustive description of the state preparation for our purpose. That is, in the considered RDI setting, additional information on the states does not help restricting Eve further. In particular, any common unitary transformation or isometry on the states can be cancelled by Eve and does not affect the attacks she can perform.

In practice the pure state assumption is always an idealization. Here, we discuss how a more realistic model of Alice's setup can be analysed with our protocols.

A. Mixed state models

Here we consider the setting where Alice's preparation device sends out a mixed state ρ_x for each possible value of x. That is the preparation box is modeled by a set of mixed states

$$\text{Alice} \simeq \{\rho_x\}_{x=0}^{n-1}. \tag{38}$$

An ensemble of mixed states of a system A' can be jointly purified onto a larger system $A' \otimes A_{\text{aux}}$ to obtain a set of pure states $\{|\psi_x\rangle\}_{x=0}^{n-1}$ with $|\psi_x\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{A_{\text{aux}}}$ and

$$\rho_x = \text{tr}_{A_{\text{aux}}} |\psi_x\rangle\langle\psi_x| \;\; \forall\, x.$$

Because the system A_{aux} remains inside Alice's lab by assumption, any security guarantee obtained for a Gram matrix $G_{\{|\psi_x\rangle\}}$ induced by the set of pure states $\{|\psi_x\rangle\}_{x=0}^{n-1}$ is valid for the original mixed states. In this case one is interested in finding the best-case purification maximizing the key rate. This gives a straightforward way to apply our protocols to noisy preparation devices modeled by Eq. (38). The resulting bounds are not necessarily tight, because in the analysis the purifying system A_{aux} is given to the eavesdropper, but are secure.

An interesting open question is whether there exists a compressed representation of the mixed state ensemble $\{\rho_x\}_{x=0}^{n-1}$, analogous to the Gram matrix, that specifies all the relations between the states useful for our purpose. Notably, in the case of two states the fidelity between them $F(\rho_0, \rho_1)$ precisely corresponds to the maximal fidelity between their purifications (see e.g. [37]). However, for larger ensembles the knowledge of pairwise fidelities is known to be insufficient to characterize the joint purification [38]. As a simple example note that even in the case of three pure states the pairwise fidelities disregard the complex phases of the Gram matrix entries, which can be crucial for the security analysis as we have seen in Section IV D.

B. Fully characterized correlated noise models

Next, let us consider the general situation where Alice's preparation device is well described by pure states that are however subject to noise, e.g., coming from drifts and fluctuations of some parameters (laser amplitude, phase noise etc). In such a case the preparation box is modelled by a parametric set of states

$$\text{Alice} \simeq \{|\phi_x(\lambda)\rangle\}_{x=0}^{n-1}, \tag{39}$$

where $p(\lambda)$ is the distribution of the noise parameter λ. In contrast to Eq. (38), this model allows for correlated noise affecting the preparation device for all measurement settings. Notably, the model in Eq. (39) reduces to Eq. (38) when the hidden variable $\lambda = (\lambda_0, \ldots, \lambda_{n-1})$ is composed of random variables λ_x that only influence the preparation for the respective setting x and are distributed independently.

Each set of pure states labeled by λ corresponds to a Gram matrix $G(\lambda)$. Here, it is important to realize that the correlations $p(b|x,y)$ observed by Alice and Bob do not constrain each λ (unless the distribution $p(b|x,y)$ is extremal) but are only respected on average, i.e.

$$p(b|x,y) = \int \mathrm{d}\lambda\, p(\lambda)\, p(b|x,y,\lambda) \tag{40}$$

for some hidden $p(b|x,y,\lambda)$. Hence, one cannot simply verify the security of the protocol for each $G(\lambda)$.

Instead, we recover a pure state situation by explicitly including the hidden noise parameter λ in the state. That is, we consider Alice preparing states of the form

$$|\psi_x\rangle = \int \mathrm{d}\lambda \sqrt{p(\lambda)}\, |\phi_x(\lambda)\rangle\, |\lambda\rangle\,, \tag{41}$$

with the "label" states for the hidden noise parameter respecting $\langle\lambda|\mu\rangle = \delta(\lambda - \mu)$. By doing so we give the noise label λ to Eve who can control it coherently but is bound to respect our noisy model of the device given by $p(\lambda)$. It is straightforward to see that the resulting Gram matrix for the states $\{|\psi_x\rangle\}_{x=0}^{n-1}$ is simply the average

$$\overline{G} = \int \mathrm{d}\lambda\, p(\lambda)\, G(\lambda). \tag{42}$$

Consequently, verifying the security of the protocol for $\overline{G}$ guarantees its security for the original model.

C. Partially characterized correlated noise models

In some situations the full model with the knowledge of the distribution $p(\lambda)$ might not be appropriate, as it requires a complete, precise characterization of the noise

mechanisms present. Instead one can only guarantee (with the desired level of confidence) that in each round the preparation device obeys to the model

$$\text{Alice} \simeq \{|\phi_x(\lambda)\rangle\}_{x=0}^{n-1} \quad \text{with} \quad \lambda \in \Lambda, \tag{43}$$

where Λ specifies the range of possible λ. From there we can recover the previous case by noting that any realization of such model corresponds to the states $\{|\psi_x\rangle\}_{x=0}^{n-1}$ in Eq. (41) for *some* probability density $p(\lambda)$ on Λ. The resulting average Gram matrix then necessarily belongs to the set

$$\begin{aligned} \overline{G} &\in \widehat{G}_\Lambda \\ G_\Lambda &= \{G(\lambda)|\lambda \in \Lambda\}, \end{aligned} \tag{44}$$

where the hat $\widehat{G}_\Lambda$ denotes the convex hull of the set G_Λ. In principle, it remains to determine the worst case $\overline{G}$ inside the set, with respect to the key rate it implies, in order to guarantee the security for the noise model.

Practically, this problem is however computationally hard. And instead of solving it directly it is convenient to further relax the constraints on $\overline{G}$ to a form that one can easily include in the security analysis described in Section IV. This can be done by constraining each entry of the Gram matrix $\overline{G}_{ij}$ *independently*. Concretely, the set G_Λ can be relaxed to a collection of constraints

$$\begin{aligned} r_{ij} \leq \text{Re}[G_{ij}] &\leq R_{ij} \\ i_{ij} \leq \text{Im}[G_{ij}] &\leq I_{ij}, \end{aligned} \tag{45}$$

on the real and imaginary parts of each entry of the matrices $G \in G_\Lambda$. Being linear these constraints remain valid for the convex hull set $\widehat{G}_\Lambda$. Most importantly, they are very simple to include in the SDP. The equality constraint $\Gamma_{ij}^{11} = G_{ij}$ in Eq. (10b) translates in two inequalities on the real and imaginary part of Γ for $i \neq j$

$$\begin{aligned} r_{ij} \leq \text{Re}[\Gamma_{ij}^{\mathbb{1}\mathbb{1}}] &\leq R_{ij} \\ i_{ij} \leq \text{Im}[\Gamma_{ij}^{\mathbb{1}\mathbb{1}}] &\leq I_{ij}. \end{aligned} \tag{46}$$

Through the SDP the Gram matrix is constraint to be positive semidefinite. Hence, the set of states described by the Gram matrix which maximizes $p_g(e = k|\text{succ})$ remains physical.

VI. COMPARISON TO OTHER QKD MODELS

In this section we present a brief comparison of our RDI approach with other models for partially DI QKD.

A first semi-DI (SDI) approach bearing some resemblances to our RDI approach was proposed in Ref. [39]. There, Alice's device is taken to be fully characterized, while Bob's device is, at least in principle, black-box and requires no characterisation. While this holds true in the ideal (lossless) case, it is unclear how their protocol would perform when losses and noise are taken into account. Indeed, the analysis of Ref. [39] in the presence of losses and noise relies on a fair-sampling type assumption, and hence the protocol can no longer be considered fully black-box on Bob's side. In particular, blinding attacks already mean that, as for our RDI protocol, no secret key can be obtained for a transmission $\eta \leq 1/n$.

Another SDI approach presented in Ref. [17, 18] shares more similarities with our approach. The authors consider prepare-and-measure scenario where Alice's device is assumed to prepare quantum states of bounded Hilbert space dimension (for instance qubits), while Bob's device is completely black-box. This represents a very different type of assumption on the preparations, which is however arguably difficult to justify in practice; indeed a photon is not a qubit, and has many other degrees of freedom than (say) polarisation [40]. In this sense, we believe that our RDI approach is more naturally tailored to experiments, as it can deal with systems of arbitrary (possibly infinite) dimension. Another important advantage in practice, is the robustness to losses. Indeed, dimension-based SDI protocols are also sensitive to detection-loophole-type attacks and thus require detection efficiencies comparable to Bell tests [41]. This renders their practical implementation challenging. To the best of our knowledge, no experiment has been reported so far. Another related approach was developed in Ref. [19], considering an entanglement-based QDK setup assuming only the dimension of the entangled state prepared by the source. Again, practical implementation is challenging due to high detection efficiency requirements.

Insofar as our model considers a black-box on Bob's side it is similar also to the model of one-sided DI QKD [20]. The latter is based on quantum steering, and therefore relies on entanglement. Moreover, a full characterisation of Alice's device is required. In practice one-sided QKD has never been implemented, most likely due to the requirement of a high detection efficiency ($\eta > 65.9\%$ [20]). We believe our RDI protocols provide a number of advantages over the one-sided DI approach. The experimental realisation is greatly simplified, as no source of entanglement is necessary, and much lower detection efficiencies can be tolerated. Moreover, in our case, the characterized party (Alice) acts as a sender, while in the one-sided model Alice holds a measurement device. Having to trust a preparation device instead of a measurement device is arguably an advantage.

Finally, we compare our RDI model to the MDI approach [21, 22]. Both approaches aim at relaxing trust on the measurement device. While we do this in the prepare-and-measure scenario, the MDI model considers an additional party (Charlie), located in between Alice and Bob and who acts as a relay. Charlie's (measurement) device is then fully untrusted, while Alice's and Bob's (preparation) devices must be well characterized. In practice, a strong advantage of the MDI approach is its robustness to losses, leading to record-distance experiments [23–26]. In a scenario where both end parties, Alice and Bob, have means to characterize and test their devices (or good reasons to believe the devices function

correctly), the MDI approach is a good choice. However, in a scenario where one of the parties does not have the resources (or the expertise) for testing and characterizing their device (or reasons not to trust their devices, for instance a possible malfunctioning due to ageing), the RDI approach provides a good solution. In contrast, the MDI approach cannot be used here, as Bob's (nor Alice's) device can be described by a black-box; some level of trust on both Alice and Bob will always be required in the MDI case.

VII. CONCLUSION

We have discussed a receiver-device-independent (RDI) approach to QKD. We presented protocols for this model and discussed their security analysis. We also provided a more detailed discussion concerning the relevance of our approach in a practical context, in particular discussing how the overlap assumption can be justified. These results complement a recent (companion) paper, where a proof-of-principle RDI QKD experiment has been reported [27].

To conclude, we discuss a number of open questions. A first interesting question is to derive stronger bounds on the secret key rate. This may be possible using techniques recently developed in Ref. [42] providing lower bounds on the conditional von Neumann entropy (instead of the conditional min-entropy, as we consider here) from observed data. Elements from the approach used in Ref. [43] might also be useful here.

Another question is to turn our asymptotic key rate into a finite key length when a finite number of systems are exchanges between Alice and Bob. A natural route towards this goal consists in using the entropy accumulation theorem [44], although it is still unclear whether this approach can be adapted to the prepare-and-measure scenario.

An important direction to pursue is to look for RDI protocols that can achieve long distance and are practical. Here we presented protocols that can tolerate the minimum possible transmission (depending on the number of measurements n made by Bob) in the RDI model. In practice, the drawback of our protocols is the sifting, which, for large n, renders the protocols inefficient. Developing more efficient protocols would represent significant progress.

Finally, we note our approach shares similarities with the recent work of Ref. [45], where the author investigates correlations in a prepare-and-measure scenario with bounded distrust in the preparations. Specifically, the fidelity of the prepared states with respect to some reference state is lower bounded. Hence the distance between the actual and ideal states is bounded. In our approach we bound the distance between the prepared states via their pairwise overlaps.

Acknowledgements.—We thank Jonathan Brask, Davide Rusca and Hugo Zbinden for discussions. We acknowledge financial support from the EU Quantum Flagship project QRANGE, and the Swiss National Science Foundation (BRIDGE, project 2000021_192244/1 and NCCR QSIT).

[1] 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* (IEEE, 1984) pp. 175–179.
[2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).
[3] G. S. Vernam, Cipher printing telegraph systems: For secret wire and radio telegraphic communications, J. AIEE **45**, 109 (1926).
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).
[5] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nature Photonics **8**, 595 (2014).
[6] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. **2**, 1 (2016).
[7] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).
[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics **4**, 686 (2010).
[9] 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 Commun. **2**, 349 (2011).
[10] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Phys. Rev. Lett. **98**, 230501 (2007).
[11] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).
[12] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, Phys. Rev. Lett. **113**, 140501 (2014).
[13] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nature Commun. **9**, 459 (2018).
[14] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, High-speed device-independent quantum key distribution against collective attacks (2021), arXiv:2110.01480 [quant-ph].

[15] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Device-independent quantum key distribution (2021), arXiv:2109.14600 [quant-ph].

[16] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, V. Scarani, C. C. W. Lim, and H. Weinfurter, Experimental device-independent quantum key distribution between distant users (2021), arXiv:2110.00575 [quant-ph].

[17] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302 (2011).

[18] E. Woodhead and S. Pironio, Secrecy in prepare-and-measure Clauser-Horne-Shimony-Holt tests with a qubit bound, Phys. Rev. Lett. **115**, 150501 (2015).

[19] K. T. Goh, J.-D. Bancal, and V. Scarani, Measurement-device-independent quantification of entanglement for given Hilbert space dimension, New J. Phys. **18**, 045022 (2016).

[20] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering, Phys. Rev. A **85**, 010301 (2012).

[21] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[22] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[23] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[24] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nature Photonics **15**, 530 (2021).

[25] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, *et al.*, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nature Photonics **15**, 570 (2021).

[26] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum key distribution over 658 km fiber with distributed vibration sensing (2021), arXiv:2110.11671 [quant-ph].

[27] M. Ioannou, M. A. Pereira, D. Rusca, F. Grünenfelder, A. Boaron, M. Perrenoud, A. A. Abbott, P. Sekatski, J.-D. Bancal, N. Maring, H. Zbinden, and N. Brunner, Receiver-device-independent quantum key distribution (2021), arXiv:2104.14574 [quant-ph].

[28] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. Roy. Soc. **A461**, 207 (2005).

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

[30] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, Characterising the correlations of prepare-and-measure quantum networks, npj Quantum Inf. **5**, 1 (2019).

[31] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, USA, 2011).

[33] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

[34] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Science **560**, 7 (2014).

[35] A. Chefles, Unambiguous discrimination between linearly independent quantum states, Phys. Lett. A **239**, 339 (1998).

[36] D. W. Horoshko, M. M. Eskandari, and S. Y. Kilin, Equiprobable unambiguous discrimination of quantum states by symmetric orthogonalisation, Phys. Lett. A **383**, 1728 (2019).

[37] M. A. Nielsen and I. Chuang, Quantum computation and quantum information (2002).

[38] M. Fannes, F. De Melo, W. Roga, and K. Zyczkowski, Matrices of fidelities for ensembles of quantum states and the Holevo quantity, Quantum Inf. Comput. **12**, 472 (2011), arXiv:1104.2271 [quant-ph].

[39] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nature Commun. **3**, 1 (2012).

[40] More generally, practical systems are usually described as infinite dimensional systems, for instance when considering optical implementations based on coherent states.

[41] M. Dall'Arno, E. Passaro, R. Gallego, M. Pawlowski, and A. Acin, Detection loophole attacks on semi-device-independent quantum and classical protocols, Quantum Inf. Comput. **15**, 37 (2015), arXiv:1210.1272 [quant-ph].

[42] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy (2021), arXiv:2106.13692 [quant-ph].

[43] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, npj Quantum Inf. **7**, 158 (2021).

[44] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, Commun. Math. Phys. **379**, 867 (2020).

[45] A. Tavakoli, Semi-device-independent framework based on restricted distrust in prepare-and-measure experiments, Phys. Rev. Lett. **126**, 210503 (2021).