Effects of preparation and measurement misalignments on the security of the Bennett-Brassard 1984 quantum-key-distribution protocol

Erik Woodhead[*] and Stefano Pironio

Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium

(Received 23 September 2012; published 11 March 2013)

The ideal Bennett-Brassard 1984 (BB84) quantum-key-distribution protocol is based on the preparation and measurement of qubits in two alternative bases differing by an angle of $\pi/2$. Any real implementation of the protocol, though, will inevitably introduce misalignments in the preparation of the states and in the alignment of the measurement bases with respect to this ideal situation. Various security proofs take into account (at least partially) such errors, i.e., show how Alice and Bob can still distill a secure key in the presence of these imperfections. Here, we consider the complementary problem: How can Eve exploit misalignments to obtain more information about the key than would be possible in an ideal implementation? Specifically, we investigate the effects of misalignment errors on the security of the BB84 protocol in the case of individual attacks, where necessary and sufficient conditions for security are known. Though the effects of these errors are small for expected deviations from the perfect situation, our results nevertheless show that Alice and Bob can incorrectly conclude that they have established a secure key if the inevitable experimental errors in the state preparation and in the alignment of the measurements are not taken into account. This gives further weight to the idea that the formulation and security analysis of any quantum cryptography protocol should be based on realistic assumptions about the properties of the apparatus used. Additionally, we note that BB84 seems more robust against alignment imperfections if both the x and z bases are used to generate the key.

DOI: 10.1103/PhysRevA.87.032315 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

The use of quantum systems to accomplish cryptographic tasks promises levels of security unachievable with any classical system. With these benefits, however, comes an added difficulty. Unlike classical protocols intended for execution on a digital computing device and whose security is purely based on the *mathematical* properties of the device's outputs, quantum protocols make use of analog systems and their security is intrinsically *physical*: it depends on the fact that device's output was obtained by measuring, e.g., the polarization of a single photon along well defined orientations. Deviations from the ideal situation, which are an all-or-nothing affair in a digital algorithm and can typically be eliminated with some very large probability, therefore become inevitable to some degree in quantum protocols.

The Bennett-Brassard 1984 (BB84) protocol [1] for quantum key distribution (QKD) [2,3], for instance, requires that one party ("Alice") prepares and sends a sequence of random qubits taken from the set $\{|\psi_{bm}\rangle\}$, where the indices $b,m \in \{0,1\}$ can be interpreted as a choice of basis and bit, respectively. The other party ("Bob") then randomly measures each qubit he receives in one of two bases $\{|\phi_{00}\rangle,|\phi_{01}\rangle\}$ or $\{|\phi_{10}\rangle,|\phi_{11}\rangle\}$. In its ideal formulation, the states $\{|\psi_{b0}\rangle,|\psi_{b1}\rangle\}$ prepared by Alice are supposed to form a basis and therefore to be orthogonal,

$$\langle\psi_{b0}|\psi_{b1}\rangle = 0 \quad \text{for} \quad b = 0,1. \tag{1}$$

Furthermore, the two bases on Alice's and on Bob's sides are supposed to differ exactly by an angle of $\pi/2$, i.e., to satisfy the relations[1]

$$|\psi_{10}\rangle = \tfrac{1}{\sqrt{2}}[|\psi_{00}\rangle + |\psi_{01}\rangle], \tag{2a}$$

$$|\psi_{11}\rangle = \tfrac{1}{\sqrt{2}}[|\psi_{01}\rangle - |\psi_{00}\rangle], \tag{2b}$$

and

$$|\phi_{10}\rangle = \tfrac{1}{\sqrt{2}}[|\phi_{00}\rangle + |\phi_{01}\rangle], \tag{3a}$$

$$|\phi_{11}\rangle = \tfrac{1}{\sqrt{2}}[|\phi_{01}\rangle - |\phi_{00}\rangle]. \tag{3b}$$

While existing security proofs for BB84 can deal with an arbitrary noise in the quantum channel from Alice to Bob, they usually assume that the states prepared by Alice and that the measurements performed by Bob satisfy precisely the conditions (1), (2), and (3). In a realistic execution of the protocol, however, experimental errors are inevitable. For instance, the measurement of a polarization qubit cannot be more precise than 2° or 4° (on the Bloch sphere) due to the intrinsic uncertainty of the polarization rotator used. Such imperfections may allow an eavesdropper to gain more information about the shared key than existing security proofs would imply.

Here we illustrate the effects that imperfections in the preparation of the states and in the alignment of the measurement bases could have on the performance of quantum cryptography protocols, using the BB84 protocol as our example.

[*] Erik.Woodhead@ulb.ac.be

[1] In addition, in the ideal formulation of the BB84 protocol, the bases on Alice's and Bob's sides are usually taken to be perfectly aligned, i.e., $|\psi_{bm}\rangle = |\phi_{bm}\rangle$. But any misalignment between the two bases can always be absorbed in the unitary transformation performed by Eve on the states emitted by Alice and thus has no incidence on the security of the protocol.

We note that proofs of security of BB84 have been proposed that relax conditions (1) and (2) [4,5], conditions (3) [6], conditions (2) and (3) [7], and also that take into account certain particular modifications of all three conditions (1), (2), and (3) in the context of collective attacks [8]. A proof of security in the asymptotic limit valid against arbitrary deviations from the three conditions (1), (2), (3) has also been reported in [9]. These types of analyses, however, are not routinely considered and scarcely used in practical implementations of BB84 [10]. The main objective of this paper is to draw attention to this issue.

Rather than deriving a new security proof, our aim is to demonstrate an explicit advantage gained by an eavesdropper. We therefore restrict our analysis to individual attacks—where, contrarily to more general types of attacks, necessary and sufficient conditions for security are known—and optimize over all possible attacks of this type in the presence of imperfections. We emphasize that, though security proofs against more general types of attacks, such as those mentioned above, do report keyrates that are lower than in the ideal case, it is not *a priori* clear that these observed reductions in security are genuine and not an artifact of a suboptimal security proof. In the case of individual attacks, however, optimal criteria for security are known, and thus any reduction in the keyrate that we observe illustrates some genuine advantage gained by the eavesdropper. Furthermore, general security proofs bound security "from below," ruling out possible successful attacks by an eavesdropper below a certain threshold. In optimizing explicitly over individual attacks, we bound security "from above." Our results can thus also be viewed as representing an *upper* bound on security: we strictly prove that non-ideal BB84 implementations of the type we consider are *insecure* above a certain threshold.

For simplicity, we consider the case where the states emitted by Alice still form two orthonormal bases as in (1). (Any deviation from (1) can only reinforce the effects of imperfections that we illustrate here.) We suppose, however, that Alice's preparation and Bob's measurement bases are not exactly mutually unbiased, but that they differ by angles α and β, respectively, different from $\pi/2$. That is, we suppose instead of (2) and (3) that

$$|\psi_{10}\rangle = \cos\left(\tfrac{\alpha}{2}\right)|\psi_{00}\rangle + \sin\left(\tfrac{\alpha}{2}\right)|\psi_{01}\rangle, \tag{4a}$$

$$|\psi_{11}\rangle = \cos\left(\tfrac{\alpha}{2}\right)|\psi_{01}\rangle - \sin\left(\tfrac{\alpha}{2}\right)|\psi_{00}\rangle, \tag{4b}$$

and

$$|\phi_{10}\rangle = \cos\left(\tfrac{\beta}{2}\right)|\phi_{00}\rangle + \sin\left(\tfrac{\beta}{2}\right)|\phi_{01}\rangle, \tag{5a}$$

$$|\phi_{11}\rangle = \cos\left(\tfrac{\beta}{2}\right)|\phi_{01}\rangle - \sin\left(\tfrac{\beta}{2}\right)|\phi_{00}\rangle. \tag{5b}$$

It is clear that such errors will in general reduce the security of BB84. For example, in the extreme case where the two bases accidentally coincide ($\alpha,\beta = 0$), an eavesdropper could perfectly clone the states sent by Alice without revealing her presence. Using a combination of analytical techniques and numerical optimization, we demonstrate here more generally a reduction in the extractable secret keyrate of the BB84 protocol against individual attacks, for a given quantum bit error rate (QBER), when $\alpha,\beta \neq \pi/2$.

Though the reduction in the keyrate that we observe is small for deviations from the ideal situation expected in realistic implementations, our results nevertheless show that Alice and Bob can erroneously conclude that they have established a secure key if the inevitable experimental errors in the alignment of the bases are not taken into account. Though our findings are restricted to individual attacks, it is reasonable to expect that similar results hold in full generality. This gives further weight to the idea that the formulation and security analysis of any quantum cryptography protocol should be based on realistic assumptions about the properties of the apparatus used.

This conclusion goes in a similar direction as that which can be drawn from the recent weaknesses discovered in certain QKD implementations, such as those in Refs. [11,12]. Note though that our work has a very different perspective. Indeed, contrary to Refs. [11,12], our results do not uncover an implementation flaw in an otherwise theoretically secure scheme—a flaw which could therefore be fixed purely at the implementation level. The message that we want to convey here is rather that in any trusted and "secure" QKD implementation, uncertainties in the preparation of the quantum states and in the alignment of the measurement bases will inevitably be present and may affect the security. These uncertainties must therefore be accounted for at a *theoretical* level either by adapting the security proof or by moving to device-independent [13,14] or semi-device-independent schemes [15–17].

The present work originates from a loose collaboration with the authors of Refs. [18,19], who along similar lines have explored the effect of imperfections in the alignment of measurement bases on the characterization of quantum resources through quantum state tomography and entanglement witnesses.

Our results are presented in more detail in Sec. II; technical details are deferred to Sec. III.

II. RESULTS

A. Problem definition

We begin by briefly recounting the BB84 protocol. As recalled above, one party (Alice) prepares random qubits from the set $\{|\psi_{bm}\rangle\}$, and transmits them to a second party (Bob). Bob then measures each qubit that he receives in one of two bases $\{|\phi_{b0}\rangle, |\phi_{b1}\rangle\}$, randomly choosing between $b = 0$ and $b = 1$ each time, and stores the results. After discarding the cases where the choices of basis do not match, Alice and Bob share a so-called sifted key, with Bob's version of the key likely containing errors compared with Alice's. By sacrificing a part of the sifted key, Alice and Bob can estimate the quantum bit error rate (QBER) Q, which is defined in terms of the observed coincidence rates $p^{(b)}(m,n)$ of Alice sending a state encoding bit m and Bob measuring n, given basis b. Assuming that the QBER is the same in both bases, it can be defined as

$$Q = \frac{1}{2} \sum_{b \in \{0,1\}} [p^{(b)}(0,1) + p^{(b)}(1,0)]. \tag{6}$$

Following this, error correction and privacy amplification are applied. In the case of one-way communication from Alice to Bob, the asymptotic keyrate secure against individual attacks is given by the Csiszár-Körner bound [20]:

$$r = I(A:B) - I(A:E), \tag{7}$$

where $I(A:B)$ denotes the mutual information between Alice and Bob and $I(A:E)$ between Alice and Eve. We recall that, in the case of individual attacks, Eve performs the same unitary attack on each of Alice's qubits, but is allowed to possess a quantum memory and can delay her measurements on the states in her possession until after the bases are revealed. Fuchs *et al.* show in Ref. [21] that the highest secure asymptotic keyrate under conditions (1), (2), and (3) is given in terms of Q by

$$r = h\left(\tfrac{1}{2} - \sqrt{Q(1-Q)}\right) - h(Q), \tag{8}$$

where h is the binary entropy function.

Our task is to minimize the expression (7) for a given QBER Q using the preparation and measurement bases defined by (4) and (5) rather than the ideal ones. To simplify the analysis we will assume that the errors observed between Alice and Bob are symmetric, i.e.,

$$p^{(0)}(0,1) = p^{(0)}(1,0) = p^{(1)}(0,1) = p^{(1)}(1,0). \tag{9}$$

Given our assumptions about the symmetries in the errors observed by Alice and Bob, $I(A:B)$ is a simple function of Q:

$$I(A:B) = 2 - h(Q). \tag{10}$$

In general there need not be such symmetries in the joint probabilities $p_{\mathrm{AE}}^{(b)}(m,q)$ shared between Alice and Eve, and $I(A:E)$ is accordingly more complicated. In each basis it will be convenient to parameterize these quantities in terms of an error $Q_{\mathrm{AE}}^{(b)}$ analogous to the QBER, and an offset $\delta^{(b)}$:

$$p_{\mathrm{AE}}^{(b)}(0,0) = \tfrac{1}{2}\left(1 - Q_{\mathrm{AE}}^{(b)} - \delta^{(b)}\right), \tag{11a}$$

$$p_{\mathrm{AE}}^{(b)}(0,1) = \tfrac{1}{2}\left(Q_{\mathrm{AE}}^{(b)} + \delta^{(b)}\right), \tag{11b}$$

$$p_{\mathrm{AE}}^{(b)}(1,0) = \tfrac{1}{2}\left(Q_{\mathrm{AE}}^{(b)} - \delta^{(b)}\right), \tag{11c}$$

$$p_{\mathrm{AE}}^{(b)}(1,1) = \tfrac{1}{2}\left(1 - Q_{\mathrm{AE}}^{(b)} + \delta^{(b)}\right). \tag{11d}$$

The inverse relations are $Q_{\mathrm{AE}}^{(b)} = p_{\mathrm{AE}}^{(b)}(0,1) + p_{\mathrm{AE}}^{(b)}(1,0)$ and $\delta^{(b)} = p_{\mathrm{AE}}^{(b)}(0,1) - p_{\mathrm{AE}}^{(b)}(1,0)$. The mutual information between Alice and Eve is given by

$$I(A:E) = 1 + \tfrac{1}{2}[I^{(0)}(A:E) + I^{(1)}(A:E)], \tag{12}$$

where $I^{(b)}(A:E)$ is the mutual information in a single basis, determined by the joint probabilities $p_{\mathrm{AE}}^{(b)}(m,n)$.

We present results for the numerical optimization of this problem in the next subsection. Details of the parametrization and techniques employed are deferred to Sec. III.

B. Optimization results

In numerically evaluating the keyrate, it generally seems to be the case, as one might expect, that the minimal keyrate is found for a unitary interaction that gives Eve symmetric information about the bits in Alice's possession. In terms of the parametrization introduced at the end of the previous section, this is the case where $\delta^{(0)} = \delta^{(1)} = 0$ and $Q_{\mathrm{AE}}^{(0)} = Q_{\mathrm{AE}}^{(1)} \equiv Q_{\mathrm{AE}}$. The keyrate is then a simple function of Q and Q_{AE}:

$$r = h(Q_{\mathrm{AE}}) - h(Q). \tag{13}$$

Supported by a few test cases, this simplification was applied in the results we now present. (Note that even if Eve's optimal attack does not generally satisfy this symmetry, our results still represent an upper bound on the secure keyrate, which conclusively shows that Eve can gain information by exploiting preparation and measurement imperfections with respect to the ideal case.)

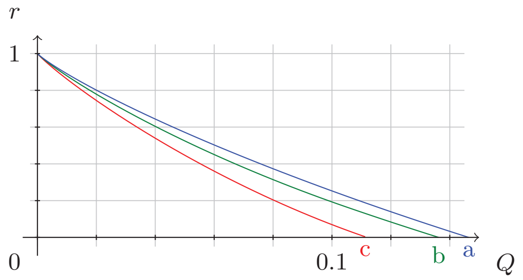

FIG. 1. (Color online) Variation of keyrate with QBER for $\theta = 90°$ [blue (a)], $80°$ [green (b)], and $70°$ [red (c)], corresponding to the worst-case scenarios for errors of $0°$, $5°$, and $10°$ respectively.

Figure 1 is a plot of the optimized keyrate as a function of Q for a few fixed values of $\alpha = \beta = \theta$. The values of θ used are 90° (the ideal case), 80°, and 70°. The latter two are the worst-case scenarios if there are absolute experimental errors of respectively 5° and 10° on the orientations of the bases both used by Alice and measured by Bob. That is, if Alice and Bob know, say, that their devices are accurate to within five degrees, i.e., $80° \leqslant \alpha,\beta \leqslant 90°$, then the worst keyrate that we have found corresponds to the situation $\alpha = \beta = \theta = 80°$. The worst-case scenario is thus that the largest possible error on the orientation of the devices is systematic.

Figure 2 is a plot of the minimized keyrate as a function of the deviation $\delta_\theta = \pi/2 - \theta$ from the ideal case, for QBERs of $\frac{1}{4}Q_0$, $\frac{1}{2}Q_0$, and $\frac{3}{4}Q_0$, where $Q_0 = \frac{1}{2} - \frac{1}{4}\sqrt{2} \approx 0.1464$ is the maximum tolerable QBER in the ideal case.

Finally, Fig. 3 is a plot of the upper secure bound on the QBER as a function of the deviation $\delta_\theta = \pi/2 - \theta$. The Shor-Preskill bound of 0.11 [22], representing the best known threshold QBER below which an ideal BB84 implementation is known to be secure against arbitrary attacks, is added for comparison.

C. Discussion

Assuming that Alice and Bob observe errors that are symmetric, according to (9), using a combination of analytical

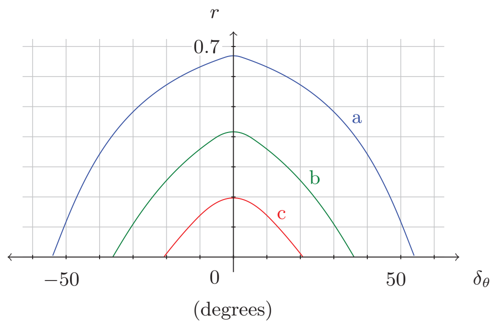

FIG. 2. (Color online) Variation of keyrate with angle $\delta_\theta = 90° - \theta$, for $Q = \frac{1}{4}Q_0$ [blue (a)], $\frac{1}{2}Q_0$ [green (b)], and $\frac{3}{4}Q_0$ [red (c)], where $Q_0 \approx 0.1464$ is the upper secure bound on the QBER.

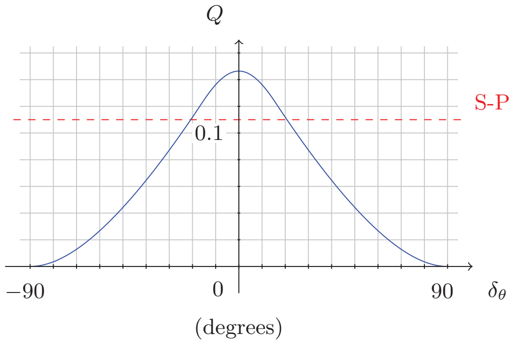

FIG. 3. (Color online) Maximum secure QBER as a function of $\delta_\theta = 90^\circ - \theta$. The horizontal dashed (red) line (S-P) corresponds to the Shor-Preskill bound of about 0.11.

and numerical techniques we have determined upper bounds on the keyrate for preparation and measurement devices characterized by the misalignment angles α and β defined in (4) and (5). As soon as $\alpha,\beta \neq \pi/2$, we find that these upper bounds are lower than the optimal keyrate (8) for a given QBER, therefore showing that imperfections in the preparation and measurement devices can be exploited by an eavesdropper if they are not taken into account in the security proof. We also draw attention to the fact that the threshold QBER illustrated in Fig. 3 drops below the Shor-Preskill bound of about 0.11 for deviation angles larger than about 20.7°, demonstrating that the Shor-Preskill keyrate is certainly insecure in this case.

The upper bounds that we have obtained correspond to the best individual attack that is symmetric, i.e., that satisfies $\delta^{(0)} = \delta^{(1)} = 0$ and $Q_{\mathrm{AE}}^{(0)} = Q_{\mathrm{AE}}^{(1)} \equiv Q_{\mathrm{AE}}$. We have numerically verified in a few test cases that the best overall individual attack satisfies this symmetry condition. We thus expect our upper bounds on the keyrate to actually correspond to the *optimal* keyrates in the presence of imperfections of the type we consider.

If Alice and Bob know that their devices are accurate to within a given precision δ_θ, they should assume, for the purpose of proving security, that their devices are characterized by the angles α and β compatible with this precision that yield the worst-case keyrate. We verified in a few test cases that this happens for the smallest angles α and β consistent with the set error, at least in the case where the set error is the same on Alice's and Bob's devices. It is for this reason that the above figures are plotted for values of the angles satisfying $\alpha = \beta = \theta = \pi/2 - \delta_\theta$.

All the results that we have presented here were obtained for the case where both bases are used to establish the secret key. One may also consider the variant of BB84 in which only one basis is used to generate the key [23]. In the ideal case, this results in a keyrate that is asymptotically twice as high, as the sifting step, where half of the results are discarded, is no longer necessary. We have also adapted our analysis to this situation and have found that for high QBERs the two-basis protocol results in a higher keyrate than the single-basis one, suggesting that the former is more robust against alignment errors.

Finally, we remind the reader that throughout our analysis, we have assumed that the states prepared by Alice define a basis, i.e., satisfy (1). Relaxing this condition could only strengthen the effects of imperfections observed here.

III. TECHNICAL DETAILS

A. Eve's interaction

The model applied here is a straightforward adaptation of the one considered in [21]. In the worst-case scenario the eavesdropper (Eve) has replaced the quantum channel between Alice and Bob with a lossless channel, before appending an ancilla to the state sent by Alice and applying a unitary operation with the intent of cloning the communication. We express the interaction as

$$|\psi_{00}\rangle|0\rangle \mapsto |\Psi_{00}\rangle, \tag{14a}$$
$$|\psi_{01}\rangle|0\rangle \mapsto |\Psi_{01}\rangle, \tag{14b}$$

in the basis $b = 0$, and similarly

$$|\psi_{10}\rangle|0\rangle \mapsto |\Psi_{10}\rangle, \tag{15a}$$
$$|\psi_{11}\rangle|0\rangle \mapsto |\Psi_{11}\rangle, \tag{15b}$$

in the basis $b = 1$, where the states $\{|\Psi_{bx}\rangle\}$ are states in the Hilbert space $\mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{E}}$ accessible to Bob and Eve. Linearity of the unitary interaction implies that these states obey the same relations as $\{|\psi_{bx}\rangle\}$. Specifically,

$$|\Psi_{10}\rangle = \cos\left(\tfrac{\alpha}{2}\right)|\Psi_{00}\rangle + \sin\left(\tfrac{\alpha}{2}\right)|\Psi_{01}\rangle, \tag{16a}$$
$$|\Psi_{11}\rangle = \cos\left(\tfrac{\alpha}{2}\right)|\Psi_{01}\rangle - \sin\left(\tfrac{\alpha}{2}\right)|\Psi_{00}\rangle. \tag{16b}$$

In order to parametrize the interaction, we set

$$|\Psi_{00}\rangle = |\phi_{00}\rangle(|a\rangle + |b\rangle) + |\phi_{01}\rangle(|c\rangle + |d\rangle), \tag{17a}$$
$$|\Psi_{01}\rangle = |\phi_{01}\rangle(|a\rangle - |b\rangle) + |\phi_{00}\rangle(|c\rangle - |d\rangle), \tag{17b}$$

and

$$|\Psi_{10}\rangle = |\phi_{10}\rangle(|a'\rangle + |b'\rangle) + |\phi_{11}\rangle(|c'\rangle + |d'\rangle), \tag{18a}$$
$$|\Psi_{11}\rangle = |\phi_{11}\rangle(|a'\rangle - |b'\rangle) + |\phi_{10}\rangle(|c'\rangle - |d'\rangle), \tag{18b}$$

where $|a\rangle,|b\rangle,|c\rangle,|d\rangle \in \mathcal{H}_{\mathrm{E}}$ are (not necessarily normalized) states accessible to Eve whose "metric" $\gamma_{ij} = \langle i|j\rangle$, $i,j \in \{a,b,c,d\}$ completely defines Eve's interaction. Combining (17) and (18) with (16) and (5), we extract the relations

$$|a'\rangle = \cos(\Delta)|a\rangle + \sin(\Delta)|d\rangle, \tag{19a}$$
$$|d'\rangle = \cos(\Delta)|d\rangle - \sin(\Delta)|a\rangle, \tag{19b}$$

and

$$|b'\rangle = \cos(\theta)|b\rangle + \sin(\theta)|c\rangle, \tag{20a}$$
$$|c'\rangle = \cos(\theta)|c\rangle - \sin(\theta)|b\rangle, \tag{20b}$$

where we have set

$$\Delta = \frac{\beta - \alpha}{2}, \tag{21a}$$
$$\theta = \frac{\beta + \alpha}{2}. \tag{21b}$$

The problem now is to identify the metric γ_{ij} which will maximize the information Eve is able to gain about Alice's raw key. Note that this information also depends on the measurements Eve performs on her part of the states she shares with Bob. In general these will be positive operator-valued measures (POVMs) which are allowed to depend on the basis (since we allow Eve to possess a quantum memory). We call the POVM elements F_{b0} and F_{b1}, where $b \in \{0,1\}$ and $F_{b0} + F_{b1} = \mathbb{1}$. As will be explained in the next subsection, we will be able to eliminate the explicit appearance of the POVM elements in our optimization problem.

B. Eve's quantum error

As stated in the introduction to this section, we wish to minimize the extractable secret keyrate, which involves maximizing the mutual information $I(A:E)$. As a stepping stone to optimizing this quantity we will consider the QBER in Eve's inference of Alice's bits, Q_{AE}, first introduced in Sec. I, in (11). Working in a single basis b for now, this quantity is given by

$$Q_{\mathrm{AE}}^{(b)} = p_{\mathrm{AE}}^{(b)}(0,1) + p_{\mathrm{AE}}^{(b)}(1,0). \tag{22}$$

In general $I^{(b)}(A:E)$ depends on both this error $Q_{\mathrm{AE}}^{(b)}$ and the asymmetry $\delta^{(b)}$ also introduced in (11), and is an increasing function as $Q_{\mathrm{AE}}^{(b)}$ approaches $1/2$ for fixed $\delta^{(b)}$. Rather than attempting to *directly* optimize the mutual information in terms of $Q_{\mathrm{AE}}^{(b)}$ and $\delta^{(b)}$, we instead turn our attention to the combination

$$Q_{\mathrm{AE}}^{(b)}(\varepsilon) = (1+\varepsilon)p_{\mathrm{AE}}^{(b)}(0,1) + (1-\varepsilon)p_{\mathrm{AE}}^{(b)}(1,0). \tag{23}$$

In terms of $Q_{\mathrm{AE}}^{(b)}$ and $\delta^{(b)}$ this is

$$Q_{\mathrm{AE}}^{(b)}(\varepsilon) = Q_{\mathrm{AE}}^{(b)} + \varepsilon\delta^{(b)}. \tag{24}$$

Optimizing this quantity yields a $\delta^{(b)}$, dependent on the weighting parameter ε, and an optimal $Q_{\mathrm{AE}}^{(b)}$ given $\delta^{(b)}$. By varying ε one may hope to sweep the range of values of $\delta^{(b)}$ and obtain a profile of minimized $Q_{\mathrm{AE}}^{(b)}$ as a function of $\delta^{(b)}$. The motivation for this approach becomes apparent when we express $Q_{\mathrm{AE}}^{(b)}(\varepsilon)$ in terms of Eve's probe and POVM elements.

In terms of Eve's interaction and measurement,

$$p_{\mathrm{AE}}^{(b)}(0,1) = \tfrac{1}{2}\mathrm{Tr}[\rho_{b0}F_{b1}], \tag{25a}$$

$$p_{\mathrm{AE}}^{(b)}(1,0) = \tfrac{1}{2}\mathrm{Tr}[\rho_{b1}F_{b0}], \tag{25b}$$

where $\rho_{bx} = \mathrm{Tr}_{\mathrm{B}}[|\Psi_{bx}\rangle\langle\Psi_{bx}|]$, Tr_{B} is the partial trace over $\mathcal{H}_{\mathrm{B}}$, and F_{bz} are POVM elements which sum to unity for each basis. Substituting into (23) and using that $F_{b1} = \mathbb{1} - F_{b0}$, we obtain

$$Q_{\mathrm{AE}}^{(b)}(\varepsilon) = \tfrac{1}{2}(1+\varepsilon) - \tfrac{1}{2}\mathrm{Tr}\{[(\rho_{b0}-\rho_{b1}) + \varepsilon(\rho_{b0}+\rho_{b1})]F_{b0}\}. \tag{26}$$

This expression is minimized by taking for F_{b0} a projector which selects the positive eigenvalue part of the operator in the trace (the Helström bound). The result of optimizing over Eve's measurement is

$$Q_{\mathrm{AE}}^{(b)}(\varepsilon) = \tfrac{1}{2} - \tfrac{1}{4}\|(\rho_{b0}-\rho_{b1}) + \varepsilon(\rho_{b0}+\rho_{b1})\|_1, \tag{27}$$

where for an arbitrary matrix $\|M\|_1 = \mathrm{Tr}[(M^\dagger M)^{1/2}]$. This replaces the explicit appearance of Eve's POVM with an eigenvalue problem, leaving only an optimization over Eve's interaction. Note that this would not be possible if we instead attempted to optimize $Q_{\mathrm{AE}}^{(b)}$ for fixed $\delta^{(b)}$, since in that case the POVM element F_{b0} would appear explicitly in the constraint as well as in the expression to optimize.

Using $b=0$ as an example, we now describe how we approach the problem of maximizing $Q_{\mathrm{AE}}^{(0)}$ and how we extract the corresponding values of $Q_{\mathrm{AE}}^{(0)}$ and $\delta^{(0)}$. In terms of the four states $|a\rangle$, $|b\rangle$, $|c\rangle$, and $|d\rangle$ introduced earlier in order to parametrize the probe,

$$\tfrac{1}{2}(\rho_{00}-\rho_{01}) = |a\rangle\langle b| + |b\rangle\langle a| + |c\rangle\langle d| + |d\rangle\langle c|, \tag{28a}$$

$$\tfrac{1}{2}(\rho_{00}+\rho_{01}) = |a\rangle\langle a| + |b\rangle\langle b| + |c\rangle\langle c| + |d\rangle\langle d|. \tag{28b}$$

In general our problem is to extract the eigenvalues of an operator $\hat{A}$ given its decomposition

$$\hat{A} = A^{ij}|i\rangle\langle j| \tag{29}$$

in terms of the states $\{|i\rangle \mid i \in \{a,b,c,d\}\}$ (where we adopt the convention of summing over repeated indices). Explicitly decomposing a vector $|u\rangle$ on the same basis as $|u\rangle = u^i|i\rangle$, the action of $\hat{A}$ on $|u\rangle$ is

$$\hat{A}|u\rangle = A^{ij}|i\rangle\langle j|u^k|k\rangle = A^{ij}\gamma_{jk}u^k|i\rangle. \tag{30}$$

It is not difficult to see that determining the eigenvalues and eigenstates of $\hat{A}$ is equivalent to determining the eigenvalues and eigenvectors of the matrix $A\Gamma$, where $A = (A_{ij})$ and $\Gamma = (\gamma_{ij})$. (This remains true even in the case where the vectors $\{|i\rangle\}$ are not linearly independent.) The matrix whose eigenvalues we wish to determine may be expressed as $D + \varepsilon\Gamma$, where

$$D = \begin{bmatrix} \gamma_{ba} & b^2 & \gamma_{bc} & \gamma_{dc} \\ a^2 & \gamma_{ab} & \gamma_{ac} & \gamma_{ad} \\ \gamma_{da} & \gamma_{db} & \gamma_{dc} & d^2 \\ \gamma_{ca} & \gamma_{cb} & c^2 & \gamma_{cd} \end{bmatrix}, \tag{31}$$

$$\Gamma = \begin{bmatrix} a^2 & \gamma_{ab} & \gamma_{ac} & \gamma_{ad} \\ \gamma_{ba} & b^2 & \gamma_{bc} & \gamma_{dc} \\ \gamma_{ca} & \gamma_{cb} & c^2 & \gamma_{cd} \\ \gamma_{da} & \gamma_{db} & \gamma_{dc} & d^2 \end{bmatrix}, \tag{32}$$

and $a^2 = \gamma_{aa}$, and so on. Let the eigenvalues of this matrix be $\{\lambda_p\}$ and the corresponding (not necessarily normalized) eigenvectors be $\{v_p\}$, such that

$$(D + \varepsilon\Gamma)v_p = \lambda_p v_p. \tag{33}$$

In terms of the set of eigenvectors, the operator F_{00} has the expression

$$F_{00} = \sum_{\lambda_p>0} \frac{|v_p\rangle\langle v_p|}{\langle v_p|v_p\rangle}, \tag{34}$$

where $|v_p\rangle = v_p^i|i\rangle$, $i \in \{a,b,c,d\}$ and the sum is over the indices p for which $\lambda_p > 0$. Using this, and the fact that the $|v_p\rangle$ are orthogonal, we obtain a matrix expression for the trace of an arbitrary operator $\hat{A}$ multiplied by F_{00}:

$$\mathrm{Tr}[\hat{A}F_{00}] = \sum_{\lambda_p>0} \frac{\langle v_p|\hat{A}|v_p\rangle}{\langle v_p|v_p\rangle} = \sum_{\lambda_p>0} \frac{v_p^\dagger \Gamma A \Gamma v_p}{v_p^\dagger \Gamma v_p}, \tag{35}$$

The explicit expressions for $Q_{\mathrm{AE}}^{(0)}$ and $\delta^{(0)}$ are

$$Q_{\mathrm{AE}}^{(0)} = \frac{1}{2} - \sum_{\lambda_p>0} \frac{v_p^\dagger \Gamma D v_p}{v_p^\dagger \Gamma v_p}, \tag{36}$$

$$\delta^{(0)} = \frac{1}{2} - \sum_{\lambda_p>0} \frac{v_p^\dagger \Gamma^2 v_p}{v_p^\dagger \Gamma v_p}. \tag{37}$$

With $Q_{\mathrm{AE}}^{(0)}$ and $\delta^{(0)}$ determined, we have an optimized value of $I^{(0)}(A:E)$ for fixed $\delta^{(0)}$, and all that remains is to optimize $I^{(0)}(A:E)$ over ε.

Finally, the generalization when we consider two bases is straightforward: we will approach the optimization of $I(A:E)$ by introducing three weighting parameters ε_0, ε_1, and ε, instead of one, optimizing the quantity

$$Q_{\mathrm{AE}}(\varepsilon_0,\varepsilon_1,\varepsilon) = \tfrac{1}{2}(1+\varepsilon)Q_{\mathrm{AE}}^{(0)}(\varepsilon_0) + \tfrac{1}{2}(1-\varepsilon)Q_{\mathrm{AE}}^{(1)}(\varepsilon_1), \quad (38)$$

and then optimizing $I(A:E)$ over $(\varepsilon_0,\varepsilon_1,\varepsilon)$.

C. Inherent QBER

All that remains now, before being able to optimize (38) over all of Eve's possible unitary interactions, is to determine the full set of constraints on the metric γ_{ij}, since not all metrics will represent a unitary interaction, and to determine the relationship between the metrics γ_{ij} and γ'_{ij} in the two bases (which depends only on the angles θ and Δ). This is done in the next subsection. Before this, we demonstrate that there is a minimum nonzero QBER if $\alpha \neq \beta$ (in which case Alice and Bob's bases cannot be perfectly aligned). This is easily verified by expressing the QBER Q in terms of a basis $\{|0'\rangle,|1'\rangle\}$ intermediate between $\{|\Psi_{00}\rangle,|\Psi_{01}\rangle\}$ and $\{|\Psi_{10}\rangle,|\Psi_{11}\rangle\}$, and a basis $\{|0\rangle,|1\rangle\}$ midway between $\{|\phi_{00}\rangle,|\phi_{01}\rangle\}$ and $\{|\phi_{10}\rangle,|\phi_{11}\rangle\}$. Specifically,

$$|0'\rangle = \cos\left(\tfrac{\alpha}{4}\right)|\Psi_{00}\rangle + \sin\left(\tfrac{\alpha}{4}\right)|\Psi_{01}\rangle, \quad (39a)$$
$$|1'\rangle = \cos\left(\tfrac{\alpha}{4}\right)|\Psi_{01}\rangle - \sin\left(\tfrac{\alpha}{4}\right)|\Psi_{00}\rangle, \quad (39b)$$

and

$$|0\rangle = \cos\left(\tfrac{\beta}{4}\right)|\phi_{00}\rangle + \sin\left(\tfrac{\beta}{4}\right)|\phi_{01}\rangle, \quad (40a)$$
$$|1\rangle = \cos\left(\tfrac{\beta}{4}\right)|\phi_{01}\rangle - \sin\left(\tfrac{\beta}{4}\right)|\phi_{00}\rangle. \quad (40b)$$

Setting

$$\Sigma_z = |0'\rangle\langle 0'| - |1'\rangle\langle 1'|, \quad (41a)$$
$$\Sigma_x = |0'\rangle\langle 1'| + |1'\rangle\langle 0'|, \quad (41b)$$

and

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad (42a)$$
$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad (42b)$$

then with this choice of basis the expression we find for the quantum error is

$$Q = \tfrac{1}{2} - \tfrac{1}{4}\cos\left(\tfrac{\alpha}{2}\right)\cos\left(\tfrac{\beta}{2}\right)\mathrm{Tr}[\Sigma_z(\sigma_z\otimes\mathbb{1}_{\mathrm{E}})] - \tfrac{1}{4}\sin\left(\tfrac{\alpha}{2}\right)\sin\left(\tfrac{\beta}{2}\right)\mathrm{Tr}[\Sigma_x(\sigma_x\otimes\mathbb{1}_{\mathrm{E}})]. \quad (43)$$

Clearly, $-2 \leqslant \mathrm{Tr}[\Sigma_z(\sigma_z\otimes\mathbb{1}_{\mathrm{E}})] \leqslant 2$ and $-2 \leqslant \mathrm{Tr}[\Sigma_x(\sigma_x\otimes\mathbb{1}_{\mathrm{E}})] \leqslant 2$, and we find the bound

$$Q \geqslant \tfrac{1}{2} - \tfrac{1}{2}\max\{|\cos(\Delta)|,|\cos(\theta)|\}, \quad (44)$$

with Δ and θ defined as in (21) (this bound is also saturated, e.g., if Eve does not interfere with the channel, in which case $\Sigma_{z,x} = \sigma_{z,x}$). The corresponding upper bound is

$$Q \leqslant \tfrac{1}{2} + \tfrac{1}{2}\max\{|\cos(\Delta)|,|\cos(\theta)|\}. \quad (45)$$

D. Transformation and constraints

We now determine the full set of constraints on the metric elements γ_{ij}. First, we impose that the QBER is fixed at Q. This, combined with $\langle\Psi_{00}|\Psi_{00}\rangle = \langle\Psi_{01}|\Psi_{01}\rangle = 1$, imposes

$$a^2 + b^2 = 1 - Q, \quad (46a)$$
$$c^2 + d^2 = Q, \quad (46b)$$

and $\mathrm{Re}[\gamma_{ab}] = \mathrm{Re}[\gamma_{cd}] = 0$, with analogous constraints for the basis $b = 1$. The components γ_{ab}, γ_{ac}, γ_{bd}, and γ_{cd} transform between the two bases according to

$$\gamma'_{ab} = \cos(\Delta)\cos(\theta)\gamma_{ab} + \cos(\Delta)\sin(\theta)\gamma_{ac} + \sin(\Delta)\cos(\theta)\gamma_{db} + \sin(\Delta)\cos(\theta)\gamma_{dc}, \quad (47a)$$
$$\gamma'_{ac} = \cos(\Delta)\cos(\theta)\gamma_{ac} - \cos(\Delta)\sin(\theta)\gamma_{ab} + \sin(\Delta)\cos(\theta)\gamma_{dc} - \sin(\Delta)\sin(\theta)\gamma_{db}, \quad (47b)$$
$$\gamma'_{db} = \cos(\Delta)\cos(\theta)\gamma_{db} + \cos(\Delta)\sin(\theta)\gamma_{dc} - \sin(\Delta)\cos(\theta)\gamma_{ab} - \sin(\Delta)\sin(\theta)\gamma_{ac}, \quad (47c)$$
$$\gamma'_{dc} = \cos(\Delta)\cos(\theta)\gamma_{dc} - \cos(\Delta)\sin(\theta)\gamma_{db} - \sin(\Delta)\cos(\theta)\gamma_{ac} + \sin(\Delta)\sin(\theta)\gamma_{ab}. \quad (47d)$$

For a more compact representation, the transformation matrix from $[\gamma_{ab},\gamma_{ac},\gamma_{db},\gamma_{dc}]^T$ to $[\gamma'_{ab},\gamma'_{ac},\gamma'_{db},\gamma'_{dc}]^T$ can be expressed as

$$\begin{bmatrix} \cos(\Delta) & \sin(\Delta) \\ -\sin(\Delta) & \cos(\Delta) \end{bmatrix} \otimes \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}. \quad (48)$$

Equations (47a) and (47d) together with the constraint $\mathrm{Re}[\gamma_{ab}] = \mathrm{Re}[\gamma_{cd}] = 0$ imply $\mathrm{Re}[\gamma_{ac}] = \mathrm{Re}[\gamma_{bd}] = 0$.

For a' and d', we find

$$a'^2 = \cos(\Delta)^2a^2 + \sin(\Delta)^2d^2 + \sin(2\Delta)\,\mathrm{Re}[\gamma_{ad}], \quad (49a)$$
$$d'^2 = \cos(\Delta)^2d^2 + \sin(\Delta)^2a^2 - \sin(2\Delta)\,\mathrm{Re}[\gamma_{ad}], \quad (49b)$$

from which we immediately see that $a'^2 + d'^2 = a^2 + d^2$. From (49), and taking the real and imaginary parts of

$$\gamma'_{ad} = -\tfrac{1}{2}\sin(2\Delta)(a^2 - d^2) + \cos(\Delta)^2\gamma_{ad} - \sin(\Delta)^2\gamma_{da}, \quad (50)$$

we find

$$\delta'_{ad} = \cos(2\Delta)\delta_{ad} + \sin(2\Delta)\,\mathrm{Re}[\gamma_{ad}], \quad (51a)$$
$$\mathrm{Re}[\gamma'_{ad}] = \cos(2\Delta)\,\mathrm{Re}[\gamma_{ad}] - \sin(2\Delta)\delta_{ad}, \quad (51b)$$
$$\mathrm{Im}[\gamma'_{ad}] = \mathrm{Im}[\gamma_{ad}], \quad (51c)$$

where $\delta_{ad} = \frac{a^2-d^2}{2}$. Similarly, $b'^2 + c'^2 = b^2 + c^2$ and

$$\delta'_{bc} = \cos(2\theta)\delta_{bc} + \sin(2\theta)\,\mathrm{Re}[\gamma_{bc}], \quad (52a)$$
$$\mathrm{Re}[\gamma'_{bc}] = \cos(2\theta)\,\mathrm{Re}[\gamma_{bc}] - \sin(2\theta)\delta_{bc}, \quad (52b)$$
$$\mathrm{Im}[\gamma'_{bc}] = \mathrm{Im}[\gamma_{bc}], \quad (52c)$$

with $\delta_{bc} = \frac{b^2-c^2}{2}$. Orthogonality of $|\Psi_{00}\rangle$ and $|\Psi_{01}\rangle$ implies $\mathrm{Im}[\gamma_{bc}] = \mathrm{Im}[\gamma_{ad}]$.

We still require $a'^2 \leqslant 1 - Q$ and $d'^2 \leqslant Q$ individually, which impose

$$\cos(\Delta)^2a^2 + \sin(\Delta)^2d^2 + \sin(2\Delta)\,\mathrm{Re}\,\gamma_{ad}] \leqslant 1 - Q, \quad (53a)$$
$$\cos(\Delta)^2d^2 + \sin(\Delta)^2a^2 - \sin(2\Delta)\,\mathrm{Re}[\gamma_{ad}] \leqslant Q. \quad (53b)$$

Equation (53a) is automatically satisfied, in the sense that there are no new restrictions on a^2, d^2, or $\mathrm{Re}[\gamma_{ad}]$, if $Q \geqslant \frac{1}{2} - \frac{1}{2}|\cos(\Delta)|$. Equation (53b) is automatically satisfied if $Q \leqslant \frac{1}{2} + \frac{1}{2}|\cos(\Delta)|$. Similarly, we automatically have $b'^2 \leqslant 1 - Q$ and $c'^2 \leqslant Q$ as long as $\frac{1}{2} - \frac{1}{2}|\cos(\theta)| \leqslant Q \leqslant \frac{1}{2} + \frac{1}{2}|\cos(\theta)|$.

Finally, using $a'^2 + b'^2 = a^2 + b^2$ and $c'^2 + d'^2 = c^2 + d^2$, we obtain the constraint

$$\begin{aligned}\sin(2\Delta)\,\mathrm{Re}[\gamma_{ad}] + \sin(2\theta)\,\mathrm{Re}[\gamma_{bc}] \\ = \sin(\Delta)^2(a^2 - d^2) + \sin(\theta)^2(b^2 - c^2).\end{aligned} \tag{54}$$

E. Optimization

The plots given in Figs. 1 and 2 were generated by numerically maximizing $Q_{\mathrm{AE}} = Q_{\mathrm{AE}}(\varepsilon_0 = \varepsilon_1 = \varepsilon = 0)$, defined by Eq. (38), using MATLAB's `fmincon` routine, over all metrics γ_{ij} respecting the constraints derived in the preceding subsection for the reported angles θ and values of Q_{AB} and with $\Delta = 0$, and calculating the corresponding value of $I(A:E)$. For simplicity, we performed no systematic optimization over $(\varepsilon_0,\varepsilon_1,\varepsilon)$. Optimizing over $(\varepsilon_0,\varepsilon_1,\varepsilon)$ in a few test cases generally supported our expectation that the minimal keyrate would be obtained for the maximal value of Q_{AE} with a symmetric attack ($\delta^{(0)} = \delta^{(1)} = 0$ and $Q_{\mathrm{AE}}^{(0)} = Q_{\mathrm{AE}}^{(1)}$). Similarly, investigating test cases generally found that the minimal keyrate, given a common error bound on the deviation of α and β from 90°, was obtained by setting both to the worst case such that $\alpha = \beta = \theta$ and $\Delta = 0$. As a result, the keyrates given in Sec. II B are an upper bound on the secure keyrate (which is sufficient to demonstrate a degradation in performance) which we believe are very likely the optimal keyrates.

The maximum tolerable QBERs reported in Fig. 3 are those for which $Q = Q_{\mathrm{AE}}$ for the angles θ considered, again with $\Delta = 0$.

In addition to the keyrates reported in Sec. II B, we also similarly investigated the case in which only one basis is used to generate the key, by maximizing only $Q_{\mathrm{AE}}^{(0)}$. In this case, the resulting keyrates (not accounting for sifting) are lower than those obtained for the case in which both bases are used, for the same parameters. This suggests that implementations of BB84 in which both bases are used to generate the key are likely to be more robust against implementation errors, as we alluded to in Sec. II C.

ACKNOWLEDGMENTS

This work was supported by the European EU QCS project, the CHIST-ERA DIQIP project, the Interuniversity Attraction Poles Photonics@be Programme (Belgian Science Policy), and the Brussels-Capital Region through a BB2B Grant. E.W. acknowledges support from the Belgian Fonds pour la Formation à la Recherche dans l'Industrie et dans l'Agriculture (F.R.I.A.).

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, Vol. 11 (IEEE, New York, 1984), pp. 175–179.

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

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[4] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[5] M. Koashi, New J. Phys. **11**, 045018 (2009).

[6] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, CA, 1998* (IEEE Computer Society, Los Alamitos, CA, 1998), pp. 503–509.

[7] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[9] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[10] N. Gisin (private communication).

[11] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[13] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[15] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).

[16] E. Woodhead, C. C. W. Lim, and S. Pironio, Theory of Quantum Computation, Communication, and Cryptography, Lecture Notes in Computer Science **7582**, 107 (2013).

[17] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[18] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).

[19] D. Rosset, R. Ferretti-Schöbitz, J.-D. Bancal, N. Gisin, and Y.-C. Liang, Phys. Rev. A **86**, 062325 (2012).

[20] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[21] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[22] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[23] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).