Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds

M. K. Bochkov¹ and A. S. Trushechkin¹,²,³,⁴

¹National Research Nuclear University MEPhI, Moscow 115409, Russia
²Steklov Mathematical Institute of Russian Academy of Sciences, Moscow 119991, Russia
³Russian Quantum Center, Skolkovo, Moscow 143025, Russia
⁴National University of Science and Technology MISiS, Moscow 119049, Russia

(Dated: November 6, 2018)

One of the challenges in practical quantum key distribution is dealing with efficiency mismatch between different threshold single-photon detectors. There are known bounds for the secret key rate for the BB84 protocol with detection-efficiency mismatch provided that the eavesdropper sends exactly one photon to the legitimate receiver. Here we improve these bounds and give tight bounds for the secret key rate with a constant detection-efficiency mismatch provided that the eavesdropper cannot send more than one photon to the receiver. We propose a method based on the analytical minimization of the relative entropy of coherence, which can be used in other problems in quantum key distribution.

I. INTRODUCTION

Quantum key distribution (QKD) is a way for two distant parties (Alice and Bob, the legitimate parties) to establish a common secret key for confidential messaging. Theoretically, the security of QKD is based solely on the laws of quantum mechanics, i.e., does not depend on the computational power or technical devices of an eavesdropper (Eve). However, in practice QKD faces certain challenges caused by imperfect devices [1–3]. One of such imperfections is efficiency mismatch between different threshold single-photon detectors.

In the most common QKD protocol BB84 as well as in other discrete-variable QKD protocols, information is typically encoded in the polarization or phase of weak coherent pulses simulating true single-photon states. Hence, the corresponding implementations employ single-photon detection techniques. Ideally, a detector should click whenever it is hit by at least one photon. However, a realistic detector is triggered by a photon only with a certain probability \(0 < \eta < 1\), which is referred to as the efficiency of a detector. Typical value of \(\eta\) for the detectors used in practical QKD systems (based on avalanche photodiodes) is 0.1. The detectors based on superconductors have \(\eta \approx 0.9\), but they are more expensive and require cryogenic temperatures.

In this paper we will consider the BB84 protocol with the active basis choice. In this case Bob uses two detectors: one for the signals encoding bit 0 and one for the signals encoding bit 1, respectively. If both detectors have the same efficiency \(\eta\), then the loss in the detection rate can be treated as a part of transmission loss followed by ideal detectors with perfect efficiency. However, in practice, it is hard to build two detectors with exactly the same efficiencies. So, the problem of detector-efficiency mismatch arises. In this case we cannot anymore treat the detection loss as a part of the transmission loss since the detection loss is different for different detectors. Also, in general, usual proofs of security of QKD [4–7] are not applicable to this case.

For example, if detection-efficiency mismatch takes place, then the frequency of, for example, zeros is greater than the frequency of ones in the raw key. This increases the Eve’s a priori information on the raw key and, hence, requires larger key contraction on the privacy amplification step.

The situation becomes even more complicated if Eve has the ability to control the efficiencies in some way (for example, by manipulation with spatial modes) [8]. Such attacks are described and employed experimentally [9, 10]. Under some conditions, Eve can completely control the Bob’s measurements and obtain full information on the secret key.

The security of the BB84 protocol with detection-efficiency mismatch is proved in [8], but the proof is restricted to the case when exactly one photon may arrive at the Bob’s side. Here we improve the bounds and give tight bounds for the secret key rate with a constant detection-efficiency mismatch provided that Eve cannot send more than one photon to Bob. In particular, the last condition means that the zero-photon case on the receiver’s side, which is not obvious in the case of detection-efficiency mismatch, is explicitly included in the analysis. This means that Eve has the ability not to send photons to Bob in some positions. Here we do not address the case when Eve can control the efficiencies of the detectors and consider only the case of a constant detection-efficiency mismatch.

We adopt the approach introduced in [11, 12] based on the minimization of the relative entropy of coherence for the purpose of numerical determination of the secret key rate. We show that the analytical (rather than numerical) minimization of the relative entropy of coherence also can be used as a method of solving QKD problems.

The text is organized as follows. In Sec. II we formulate a prepare&measure version of the BB84 protocol and specify the Bob’s POVM for the case of detection-efficiency mismatch. In Sec. III we give an equiva-
lent entanglement-based formulation of the protocol. In Sec. IV we review the approach of [11, 12], which reduces the calculation of the secret key rate to a convex optimization problem, and state a theorem with the analytic formula for the secret key rate (28). A slight modification of this formula (34), which outperforms (28) if the detection-efficiency mismatch or quantum bit error rate (QBER) is large, is given after the theorem. The proof of the theorem is given in Appendix A, and the leakage of information in the error correction procedure for the case of detection-efficiency mismatch is analyzed in Appendix B.

II. PREPARE&MEASURE FORMULATION OF THE BB84 PROTOCOL WITH DETECTION-EFFICIENCY MISMATCH

We start with the description of a mathematical model of the BB84 protocol with detection-efficiency mismatch. Most practical implementations of the BB84 protocol are prepare&measure based, in which Alice sends quantum states to Bob. We assume that Alice sends true qubits to Bob, i.e., single-photon pulses with information encoded in some two-dimensional variable. Hence, the Alice’s Hilbert space is $H_A = \mathbb{C}^2$. We will use two bases of $\mathbb{C}^2$: the standard one ($z$-basis) $\{|0\rangle, |1\rangle\}$ and the Hadamard one ($x$-basis) $\{|+, \rangle, |−\rangle\}$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. In each basis, the first element encodes the bit 0, and the second element encodes the bit 1.

Remark 1. In most implementations, Alice sends not true single-photon states, but weak coherent pulses, which make QKD vulnerable to the photon number splitting attack [13, 14]. However, this problem can be fixed by the decoy-state method, which allows effectively to bound the number of multiphoton pulses from above [15–19]. These pulses are treated as insecure, i.e., the information encoded in such pulses is assumed to be known to Eve. The decoy state method for the detector-efficiency mismatch case is considered in [20]. After the estimation of the number of multiphoton pulses, it suffices to bound the Eve’s information on the key bits originated from the single-photon pulses. So, here we consider only single-photon Alice’s pulses.

Bob measures the signals in an infinite-dimensional mode space with no limit on the number of photons. Eve can use this fact for her advantage: she can send to Bob as many photons as she wishes. The security proof for QKD with detection-efficiency mismatch in [8] is based on the assumption that Eve sends exactly one photon to Bob. Here we use a slightly weakened assumption: Eve cannot send more than one photon to Bob. In particular, Eve is allowed not to send photons in some positions. The issues with the number of photons can be avoided in QKD with perfect detectors due to the squashing model method [22]. However, there is no squashing model for the detection-efficiency mismatch case, hence, zero-photon and multiphoton cases should be analyzed explicitly. Another approach to these issues based on the entanglement verification is proposed in [23]. Note that a possible way to assure that Eve does not send more than one photon to Bob is the use of the detector-decoy idea [21].

Thus, the Bob’s Hilbert space is $H_B = \mathbb{C}^3$ and is spanned by three vectors: $|0\rangle$, $|1\rangle$, and $|\text{vac}\rangle$ (a vacuum vector).

Remark 2. We restrict our analysis to the case of a constant detection-efficiency mismatch. In contrast, in [8] Eve is allowed to control the efficiencies of the detectors. Setting the efficiency to zero in some position is equivalent to not sending a photon to Bob. However, there is an additional assumption in [8] that the information-carrying qubit sent by Eve is not coupled to an auxiliary system, which controls the efficiencies. In our analysis Eve may send to Bob an arbitrary state from $\mathbb{C}^3$, i.e., the information-carrying subsystem $\mathbb{C}^2$ may be coupled to the vacuum component.

Let us describe the Bob’s POVM. Bob chooses the $z$ measurement basis with the probability $p_z$ and the $x$ basis with the probability $p_x = 1 - p_z$. We consider the BB84 protocol with single-photon detectors and the active basis choice. In this case Bob uses two single-photon detectors: one for the signals encoding bit 0 and one for the signals encoding bit 1.

Let the efficiencies of the Bob’s detectors be $\eta_0$ and $\eta_1 \neq \eta_0$, respectively. Let, for definiteness, $1 \geq \eta_0 > \eta_1 > 0$. Then the efficiencies of the detectors can be renormalized as $\eta_0' = 1$ and $\eta_1' = \eta = \eta_1/\eta_0$, and the common loss $\eta_0$ in both detectors can be treated as additional transmission loss [23].

As shown in [22], without loss of generality, we can think that the actual measurement is preceded by a quantum non-demolition (QND) measurement of the number of photons (POVM $\{|\text{vac}\rangle \langle \text{vac}|, |I_2\rangle\}$, where $I_2$ is a unity operator in the two-dimensional single-photon subspace, which is spanned by $|0\rangle$ and $|1\rangle$). Then, the Bob’s POVM is as follows:

$$P^B_{z,0} = p_z |0\rangle \langle 0|, \quad P^A_{z,1} = p_z \eta |1\rangle \langle 1|, \quad (1a)$$

$$P^B_{x,0} = p_x |+\rangle \langle +|, \quad P^A_{x,1} = p_x \eta |−\rangle \langle −|, \quad (1b)$$

$$P^B_{\phi} = 1 - P^B_{z,0} - P^B_{x,0} - P^B_{x,1}, \quad (1c)$$

where $\phi$ corresponds to the outcome “no click”. It happens whenever either the outcome of the QND is vac or a photon hits the detector 1, but the no-click event is activated with the probability $1 - \eta$.

Now we describe the protocol.

1. Alice randomly, with the probabilities $(1/2, 1/2)$, chooses a bit value $\overline{p} \in \{0, 1\}$;

2. Alice randomly, with the probabilities $(p_z, p_x = 1 - p_z)$, chooses a basis: either the $z$-basis or $x$-basis. It is assumed that $p_z \approx 1$. Only $z$-basis is used for the key generation, while the $x$-basis is used only for the detection of eavesdropping (see below).
3. Bob also chooses a measurement basis: either the $z$-basis or $x$-basis, with the same probabilities.

4. Alice generates a photon in the state depending on the basis and the bit value and send it to Bob. For example, if Alice has chosen the bit value 0 and the $x$-basis, she sends a photon in the state $|+\rangle$. Bob measures this photon according to POVM (1) and, if at least one detector clicks, obtain the bit value $b$.

5. Alice and Bob repeat steps 1–3 a large number of times $n$. As a result, they have their own bit strings $\overline{a}$ and $\overline{b}$, which are referred to as the raw keys.

6. Announcements: Bob announces the numbers of positions where he has obtained a click over a public authentic classical channel. Alice and Bob announce the bases they used and the bit values for positions where both used the $x$ basis.

7. Sifting: Alice and Bob keep the states where they both chose the $z$-basis and Bob obtained a click. The other positions are dropped from the raw keys. The resulting keys are referred to as the sifted keys.

8. Parameter estimation: Alice and Bob analyze the announced data and estimate the amount of information on the Alice’s sifted key that can be known to Eve. If this amount is not too large, they continue. Otherwise, they abort the protocol.

9. Error correction: the mismatches between the bit values of Alice’s and Bob's sifted keys are treated as the errors in the Bob’s key. Alice sends to Bob a syndrome of her sifted key over the classical authentic channel. Using the syndrome, Bob corrects the errors in his key. Now the Bob’s corrected key coincides with the Alice’s sifted key.

10. Privacy amplification: Alice sends to Bob a hash function, both apply this function to their (identical) keys. The hash function maps the key to a shorter key about which Eve has only negligible amount of information. This is the final key, or secret key.

Remark 3. In this paper we consider only asymptotic case $n \to \infty$ and do not address the finite-key effects [5, 6]. By this reason we also do not address some practical peculiarities like the verification after the error-correction step [24, 25] or the use of both bases for the key generation since they do not matter in the asymptotic case.

III. ENTAILMENT-BASED FORMULATION OF THE PROTOCOL

We have described the prepare&measure implementation of the BB84 protocol, which is the most common in practice. However, a common mathematical trick is to reformulate the protocol in an equivalent entanglement-based version. In the entanglement-based version of the protocol, an entangled state $\rho_{AB}$ is distributed among the legitimate parties. The Alice’s measurement result encodes the information about which state she prepared. Let us describe the entanglement-based version of the BB84 protocol.

The steps 1, 2, and 4 of the protocol given above are replaced by:

1. A source of entangled states generates a two-qubit entangled state
   \[ \rho_{AB} = |\Phi\rangle_{AB} \langle\Phi|, \]  
   where
   \[ |\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B), \]  
   and sends the first qubit to Alice and the second qubit to Bob.

2. Alice perform a measurement of her part according to the POVM
   \[ P_{x,0}^A = p_x |0\rangle \langle 0|, \quad P_{x,1}^A = p_x |1\rangle \langle 1|, \quad P_{x,0}^B = p_x |+\rangle \langle +|, \quad P_{x,1}^B = p_x |\rangle \langle \rangle. \]  
   The probabilities of obtaining these results provided that the state is $\rho_{AB} = \mathbb{I}_A \otimes \rho_{AB} = I_2/2$ are: $p_x/2, p_x/2, p_x/2$, and $p_x/2$, respectively. If Alice obtains the result, say $(x,1)$, then the state is changed to
   \[ \rho_{AB} \to |\rangle_A \langle \rangle_{AB}, \]  
i.e., is equivalent to sending the state $|\rangle$ to Bob. In this sense, the entanglement-based formulation is mathematically equivalent to the prepare&measure one. Note that since Alice’s measurement is virtual, it corresponds to detectors with the perfect efficiency.

In the prepare&measure formulation of the protocol, Eve controls the transmission channel between Alice and Bob. In the equivalent entanglement-based formulation this is modeled by the Eve’s ability to replace (2) by her own density operator $\rho_{AB}$ acting on the space $\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^3$ under the restriction of the fixed $\rho_A = \mathbb{I}_B \rho_{AB}$. This means that the subsystem $A$ is inaccessible for Eve. One may think about the source of entangled states placed inside the Alice’s laboratory, so, Eve has access only to the subsystem $B$ transmitting over the channel. In our case (2) we have $\rho_A = I_2/2$.

IV. SECRET KEY RATE

We define the secret key rate as the ratio of the length of the final key to the number of channel uses $n$. To derive the formula for it, we need to formalize the steps of the
QKD protocol given above. We adopt the mathematical model developed in [11, 12].

The Alice’s and Bob’s measurements with the announcements are described by the following quantum channel:

\[
\rho_{AB} \mapsto \sum_{\alpha \in \{0,1\}} \sum_{\beta \in \{0,1\}} K^A_{\alpha} \otimes K^B_{\beta} \rho_{AB}(K^A_{\alpha} \otimes K^B_{\beta})^\dagger
\]
\[
+ \sum_{\alpha \in \{0,1\}} K^A_{\alpha} \otimes \rho_{AB}(K^A_{\alpha} \otimes K^B_{\beta})^\dagger
\]
\[
= \mathcal{M}(\rho_{AB}) = \rho^{(2)}_{AABB\tilde{B}B} \]
\[
\text{where}
\]
\[
K^A_{\alpha} = \sum_{\alpha \in \{0,1\}} \sqrt{p_{\alpha,a}} |a\rangle \tilde{A} \otimes |\alpha\rangle_A,
\]
\[
K^B_{\beta} = \sum_{\beta \in \{0,1\}} \sqrt{p_{\beta,b}} |b\rangle \tilde{B} \otimes |\beta\rangle_B,
\]
\[
K^B_{\beta} = \sqrt{p_{\beta,b}} |\varnothing\rangle \tilde{B} \otimes |0\rangle_B.
\]

Here the registers \(\tilde{A}\) (two-dimensional) and \(\tilde{B}\) (three-dimensional) store the information that is announced in the public channel: bases choices and the result \(\varnothing\) for Bob. The two-dimensional registers \(\tilde{A}\) and \(\tilde{B}\) store the key bit, which is not announced.

The sifting step is described by the projector

\[
\Pi = |z\rangle \tilde{A} \langle z| \otimes |z\rangle \tilde{B} \langle z|,
\]

\[
\rho^{(2)}_{AABB\tilde{B}B} \mapsto \frac{1}{p_{\text{pass}}} \Pi \rho^{(2)}_{AABB\tilde{B}B} \Pi = \rho^{(3)}_{AABB\tilde{B}B}
\]
\[
\text{where}
\]
\[
p_{\text{pass}} = \text{Tr} \Pi \rho^{(2)}_{AABB\tilde{B}B}
\]

is the probability of passing the sifting stage.

In the general scheme given in [11], an additional key map \(g(a, b, \alpha)\) is used to form the Alice’s key bit in an additional register. In this particular protocol we do not need this since the Alice’s and Bob’s key bits are already given in the registers \(\tilde{A}\) and \(\tilde{B}\). Let us also define a pinching (partially dephasing) quantum channel

\[
\mathcal{Z}(\sigma) = \sum_{\alpha \in \{0,1\}} (|\alpha\rangle \tilde{A} \langle \alpha| \otimes I) \sigma (|\alpha\rangle \tilde{A} \langle \alpha| \otimes I),
\]
\[
\mathcal{Z}(\rho^{(3)}_{AABB\tilde{B}B}) = \rho^{(4)}_{A\tilde{A}B\tilde{B}B}.
\]

As we said in the end of Sec. III, Eve can choose the state \(\rho_{AB}\) under the restriction \(\rho_{A} = \text{Tr}_{B} \rho_{AB} = I_2/2\).

Also, according to the purification theorem, \(\rho_{AB}\) can be expressed as \(\rho_{AB} = \text{Tr}_{E} \rho_{ABE}\), where \(\rho_{ABE}\) is a pure state in a larger Hilbert space \(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E\), and all such representations are unitary equivalent [29]. Eve is assumed to own the additional register \(E\) (the purification of \(\rho_{AB}\)).

In this paper we restrict our analysis to the case when Eve performs a collective attack: she prepares \(n\) equal copies of \(\rho_{ABE}\) and then perform a collective measurement on her parts \(E\) in all copies. According to Devetak and Winter theorem [30], the asymptotic \((n \to \infty)\) secret key rate is given by

\[
K = p_{\text{pass}} \left[ H(\overline{A}|E\overline{A}\overline{B})_{\rho^{(3)}} - H(\overline{A}|\overline{B}\overline{A}\overline{B})_{\rho^{(3)}} \right],
\]

(12)

where \(H\) is the conditional von Neumann entropy. Here the first and the second terms in the brackets characterize the Eve’s and Bob’s ignorances on an Alice’s key bit, respectively. Here we assume that the length of the error-correcting syndrome is given by the Shannon theoretical limit. Otherwise, a factor \(f > 1\) should be added to the second term. The present-day error-correcting codes allow for \(f \approx 1.22\). A novel method of the use of the low-density parity-check codes in QKD, which allows to decrease the factor \(f\), is given in [26, 27]. A new syndrome-based QBER estimation algorithm, which also can decrease \(f\), is proposed in [28].

The second term in the right-hand side of (12) is bounded from above by \(h(Q)\), where \(h\) is the binary entropy and \(Q\) is the QBER in the \(z\)-basis. Note that, due to detection-efficiency mismatch, the channel from \(\tilde{A}\) to \(\tilde{B}\) is not a binary symmetric channel. However, in our case the second term can be taken to be equal to \(h(Q)\), see Appendix B for details. The QBER is a value observed by Alice and Bob.

The Eve’s ignorance should be estimated from below. By Theorem 1 from [31],

\[
H(\overline{A}|E\overline{A}\overline{B})_{\rho^{(3)}} = D(\rho^{(3)}_{A\tilde{A}B\tilde{B}B}\|[4]_{A\tilde{A}B\tilde{B}B})
\]
\[
= p_{\text{pass}}^{-1} D(\mathcal{G}(\rho_{AB})\|[4]_{A\tilde{A}B\tilde{B}B}),
\]

(13)

where

\[
\mathcal{G}(\rho_{AB}) = \Pi \mathcal{M}(\rho_{AB}) \Pi
\]

and \(D(\sigma||\tau) = \text{Tr} \sigma \log \sigma - \text{Tr} \sigma \log \tau\) is the quantum relative entropy. The advantage of formula (13) is that the right-hand side does not involve the additional register \(E\).

Note that, since \(\mathcal{Z}\) is a partially dephasing channel, (13) is a generalization of a coherence measure proposed in [32] called the relative entropy of coherence. Its operational meaning in QKD is investigated in [33]. It is the distance between the quantum state \(\mathcal{G}(\rho_{AB})\), emerging as a result of a QKD protocol, and its partially dephased (“partially classical”) counterpart. Thus, the eavesdropper’s ignorance in quantum key distribution is equal to a measure of quantumness of the distributed bipartite state.

The state \(\rho_{AB}\) is chosen by Eve and, hence, is unknown to Alice and Bob. So, to make a reliable estimate of the secret key rate, they should minimize quantity (13) over
The most "strong" set of restrictions is
\[
K = \min_{\rho_{AB}} D(G(\rho_{AB})||Z(G(\rho_{AB}))) - p_{\text{pass}}h(Q),
\] (15a)
\[
S = \{\rho \geq 0 \text{ on } H_A \otimes H_B \mid \text{Tr} \Gamma_i \rho = \gamma_i, \forall i\}. \tag{15b}
\]

Here the operators \(\Gamma_i\) specify the restrictions:

- Weighted mean detection rate in the \(z\) basis:
  \[
  \Gamma_1 = I_2 \otimes (\eta P_{z,0}^B + P_{z,1}^B) = \eta I_2 \otimes I_2; \tag{16}
  \]

- Weighted mean error detection rate in the \(x\) basis:
  \[
  \Gamma_2 = P_{x,0}^A \otimes P_{x,1}^B + \eta P_{x,1}^A \otimes P_{x,0}^B; \tag{17}
  \]

- Fixation of \(p_{\text{pass}}\), or, in other words, the sifted key rate:
  \[
  \Gamma_3 = I_2 \otimes (P_{z,0}^B + P_{z,1}^B). \tag{18}
  \]

We have \(p_{\text{pass}} = p_z^2 \text{Tr} \Gamma_3 \rho_{AB}\). Recall that we consider the asymptotic case of infinitely many pulses sent by Alice, \(n \to \infty\). In this case, \(p_z\) can be made arbitrarily small. The \(x\) basis does not participate in the secret key generation, it is used only to estimate \(\gamma_2\). In the limit of infinitely many pulses, an arbitrarily small fraction of them is sufficient to collect a reliable statistics. So, we put \(p_x = 0\) in (15a), but still use the \(x\) basis statistics in (17). Then \(p_{\text{pass}} = \text{Tr} \Gamma_3 \rho_{AB}\).

Let us discuss the first restriction \(\Gamma_1\). Denote \(t = \text{Tr} \rho_{AB}(I_2 \otimes I_2) \leq 1\). In the no-eavesdropping case this corresponds to the transparency of the transmission line (so that \(1 - t\) is the trace of the vacuum component of the Bob’s space). Then \(\text{Tr} \Gamma_1 \rho_{AB} = t\eta\). So, \(\Gamma_1\) fixes the transparency for a constant known \(\eta\).

Together with the restriction \(\Gamma_3\), the restriction \(\Gamma_1\) additionally fixes the ratio of zeros and ones in the Bob’s sifted key. If the probability of error in the channel in the no-eavesdropping case does not depend on the bit value, then the ratio of the number of zeros to the number of zeros is \(\eta\). The restrictions \(\Gamma_1\) and \(\Gamma_3\) prevent Eve from changing this ratio. As can be seen from Appendix A (see (A9) and (A10)), the restriction \(\Gamma_1\) can be equivalently replaced by the detection rate of either only zeros or only ones: \(\Gamma'_1 = I_2 \otimes P_{z,\beta}\), where either \(\beta = 0\) or \(\beta = 1\).

Finally, let us denote \(Q_x = \text{Tr} \Gamma_2 \rho_{AB}/(t\eta)\). In the case of no detection-efficiency mismatch \(\eta = 1\), this is the QBER in the \(x\) basis. Thus,
\[
\text{Tr} \Gamma_1 \rho_{AB} = t\eta, \tag{19a}
\]
\[
\text{Tr} \Gamma_2 \rho_{AB} = t\eta Q_x, \tag{19b}
\]
\[
\text{Tr} \Gamma_3 \rho_{AB} = p_{\text{pass}}, \tag{19c}
\]

where \(t\) and \(p_{\text{pass}}\) are in the range \((0, 1]\) and \(Q_x\) is in the range \([0, 1]\).

Remark 4. The most “strong” set of restrictions is \(\{\Gamma_{jk} = P_{jk}^A \otimes P_{jk}^B\}\) along with the unit trace condition and the fixation of \(\rho_A = \text{Tr} \rho_{AB}\) (by means of the Pauli matrices [11]). The natural noise in the transmission line is often described by the depolarizing channel acting in the qubit space:
\[
E_Q(p_2) = (1 - 2Q)p_2 + 2QI_2/2, \tag{20}
\]
where \(Q\) is a QBER in both bases. So, the entangled stated distributed to Alice and Bob in the no-eavesdropping case is:
\[
\rho_0^{AB} = (\text{Id}_A \otimes E_Q)(|\Phi\rangle_{AB} \langle \Phi|) \oplus 0 + (1 - t)(I_2/2) \otimes |\text{vac}\rangle \langle \text{vac}|, \tag{21}
\]
where \(\text{Id}_A\) is the identity channel in the Alice’s space, \(E_Q\) acts in the single-photon subspace of the Bob’s space and \(\oplus 0\) denotes the embedding of the 4-dimensional space into the 6-dimensional one (with the vacuum component of the Bob’s space). Then one can take
\[
\gamma_i = \text{Tr} \rho_0^{AB} \Gamma_i, \tag{22}
\]
for all \(i\), i.e., \(\gamma_1 = t, \gamma_2 = t\eta Q\), and \(\gamma_3 = t(1 + \eta)/2\). In this case, additional restrictions in comparison to (16)–(18) does not alter the solution of the optimization problem (15) and, hence, do not increase the secret key rate. In some other cases, additional restrictions may increase the secret key rate [12, 33, 34].

Now we are ready to formulate the main theorem.

Theorem 1. Optimization problem (15)–(19) has feasible solutions if and only if
\[
2Q_x \geq 1 - \sqrt{1 - \delta^2}, \tag{23}
\]
where
\[
\delta = \frac{2p_{\text{pass}} - t(1 + \eta)}{t(1 - \eta)}. \tag{24}
\]
In this case, the optimal value of the objective function is given by
\[
K(Q_x, Q_x, \eta, t, p_{\text{pass}}) = p_{\text{pass}} \left[ h \left( \frac{1 + \delta}{2p_{\text{pass}}} \right) - h(\lambda(Q_x, \eta, t, p_{\text{pass}})) - h(Q_x) \right], \tag{25}
\]
where
\[
\lambda(Q, \eta, t, p_{\text{pass}}) = \frac{1}{2} \left[ 1 - \frac{t}{4p_{\text{pass}}} \sqrt{[1 - \eta + \delta(1 + \eta)]^2 + 4\eta(1 - 2Q)^2} \right]. \tag{26}
\]

Corollary 1. If
\[
p_{\text{pass}} = t(1 + \eta)/2, \tag{27}
\]
then the optimal value of the objective function in optimization problem (15)–(19) is given by

\[ K(Q_z, Q_x, \eta) = p_{\text{pass}} \left[ h\left(\frac{1}{1 + \eta}\right) - h(Q_x) - h(Q_z) \right], \quad (28) \]

where

\[ \lambda(Q, \eta) = \frac{1}{2} + \frac{1}{2} \sqrt{\frac{1 - 16\eta Q(1 - Q)}{(1 + \eta)^2}}. \quad (29) \]

The proof of the theorem is provided in Appendix A.

Formulas (25) and (28) are the desired formulas for the secret key rate. They are tight for the proposed protocol since the optimization problem is solved exactly.

Condition (23) means that there is no positive semi-definite operator \( \rho_{AB} \) satisfying (19) if (23) is not satisfied. Hence, the values of \( t, Q_x, \) and \( p_{\text{pass}} \) not satisfying (23) cannot be obtained.

Let us discuss the difference between formulas (25) and (28). Suppose that the transmission loss and the probability of error in the channel in the no-eavesdropping case are independent on the bit value (i.e., are the same for the states \([0]\) and \([1]\)). Then, in the no-eavesdropping case, (27) is satisfied: \( p_{\text{pass}} \) equals the average between the efficiencies of the detectors multiplied by the transparency \( t \). In the asymptotic case \( n \to \infty \), Eve cannot violate equality (27) because, otherwise, Alice and Bob will detect the eavesdropping precisely by observing the violation of (27). Hence, Eve is restricted to attacks that do not violate (27), and the secret key rate is given by (28).

However, formula (28) itself cannot be used in practice because in the finite-key scenario, even in the no-eavesdropping case, the statistical fluctuations lead to deviations of \( p_{\text{pass}} \) from its mean value \( t(1 + \eta)/2 \). Since we cannot distinguish the statistical deviations from a small \( \delta \) introduced by Eve, we must be able to bound the Eve’s knowledge on the sifted key for an arbitrary \( \delta \) in some neighborhood of zero. Formula (25) do this and can be used as a starting point in the finite-key analysis. But in the rest of the paper we will be interested in the actual secret-key rate in the asymptotic case and, so, will consider only formula (28).

For perfect detection \( \eta = 1 \), formula (28) gives the well-known result [4]:

\[ K = t[1 - h(Q_z) - h(Q_z)] \]

In another particular case of \( Q_x = Q_z = 0 \) (noiseless case), formula (28) gives another known result, which was obtained in [8]:

\[ K = p_{\text{pass}}h\left(\frac{1}{1 + \eta}\right). \quad (31) \]

Figure 1. Secret key rate \( K(Q, Q, \eta) \) of the BB84 protocol vs the efficiency of one of the detectors \( \eta \). Another detector and the transmission line are assumed to be perfect, otherwise the secret key rate is reduced by a constant factor. Red: the noiseless case \( Q = 0 \), blue: the case \( Q = 0.05 \). Solid line: formula (28) (deviates from the previous one only for the noisy case and small \( \eta \), dashed line: formula (32), dotted line: formula (33) (coincides with (32) for the noiseless case)).

Let us compare formula (28) to the two formulas obtained in [8]:

\[ K_1 = p_{\text{pass}} \left\{ \frac{2\eta}{1 + \eta}[1 - h(Q_z) - h(Q_z)] \right\}, \quad (32) \]

\[ K_2 = p_{\text{pass}} \frac{2\eta}{1 + \eta}[1 - h(Q_z) - h(Q_z)]. \quad (33) \]

The first formula is obtained as a result of a more general analysis, which includes the cases when \( \eta \) is under Eve’s control, applied to the particular case of a constant \( \eta \). The second formula is obtained by the simple discarding argument. Of course, the simplest solution to the detection-efficiency mismatch problem is to discard every zero from the Bob’s raw key (to turn it into the no-click event) with the probability \( 1 - \eta \). This allows to artificially adjust the efficiencies of the two detectors so that both cases of 0 and 1 bit values are “detected” with the probability \( \eta \). Thus, the secret key rate is equal to the right-hand side of (30) multiplied by \( \eta \), which gives exactly (33).

The comparison of these formulas are given on Fig. 1. We see that formula (28) gives definitely higher secret key rates than (32). Also it gives higher secret key rates than (33) for the most of range of \( \eta \). Only in the case of small \( \eta \), which corresponds to a large efficiency mismatch, the discarding provides higher rates. This does not contradict the tightness of bound (28) since the possibility of discarding (a kind of preprocessing of the observation data) immediately after the transmission of quantum states is not provided in our description of the protocol. Also the calculations according to formula (28) coincide with the numerical results of [11].

We can modify our protocol to overcome this limitation of formula (28). Namely, we can combine the discard-
Very recently, during the preparation of this paper, another paper [33] was published with the derivation of formula (28) by a similar method (also based on the analytical minimization of the relative entropy of coherence). The differences of our result are as follows. Firstly, in [33], a closed analytic formula (28) is derived under an additional assumption that the Eve’s attack is symmetric. In contrast, we prove the validity of (28) for arbitrary Eve’s collective attacks, but with a weaker assumption (27) on the transmission line in the no-eavesdropping case. Formula (25) is valid without this assumption and can be used as a starting point for the

![Secret key rate vs detector efficiency](image1)

**Figure 2.** Secret key rate $K(Q, Q, \eta)$ of the BB84 protocol vs the efficiency of one of the detectors $\eta$. The lines are the same as on Fig. 1, except that the thick solid line has been added. It corresponds to formula (34) and outperforms (34) (thin solid line) one only for the noisy case and small $\eta$.

![Secret key rate vs detector efficiency](image2)

**Figure 3.** Secret key rate $K(Q, Q, \eta)$ of the BB84 protocol vs the efficiency of one of the detectors $\eta$, for $Q = 0.10$. The lines are the same as on Fig. 2. Formula (34) outperforms (34) for the most range of $\eta$.

The main remaining problem is the proof of the security of QKD with detection-efficiency mismatch for the case when Eve is allowed to send an arbitrary number of photons to Bob. She can do it, for example, to artificially increase the efficiency of one of the detectors. Also the analysis of the case when the efficiencies of the detectors are under partial Eve’s control is important due to experimental realizations of such attacks [9, 10].

Preliminary results of this paper (including formula (28)) were presented at the International conference “Quantum information, statistics, probability” with a special session dedicated to A. S. Holevo’s 75th birthday [36].

**Remark 5.** Very recently, during the preparation of this paper, another paper [33] was published with the derivation of formula (28) by a similar method (also based on the analytical minimization of the relative entropy of coherence). The differences of our result are as follows. Firstly, in [33], a closed analytic formula (28) is derived under an additional assumption that the Eve’s attack is symmetric. In contrast, we prove the validity of (28) for arbitrary Eve’s collective attacks, but with a weaker assumption (27) on the transmission line in the no-eavesdropping case. Formula (25) is valid without this assumption and can be used as a starting point for the

V. DISCUSSIONS AND CONCLUSIONS

We have proved the security of the BB84 QKD protocol with detection-efficiency mismatch and have derived tight bounds on the secret key rate: formulas (25), (28) and (34). We used the approach of [11, 12] based on a reduction of the determination of the secret key rate to a convex optimization problem: the minimization of the relative entropy of coherence. We have demonstrated that the analytical (rather than numerical) minimization of the relative entropy of coherence also can be used as a method of solving QKD problems.

The finite-key analysis can be developed starting from formula (25) using the conservative (pessimistic) statistical estimations of parameters and the entropy accumulation technique [35]. Also recall that the Devetak and Winter formula for the secret key rate (12) is valid only for collective Eve’s attacks. Using the entropy accumulation technique, the security against the most general, coherent attacks can be proved.

Finally, let us recall, that, if both detectors are not perfect and have efficiencies $\eta_0$ and $\eta_1$, then $\eta = \min(\eta_0, \eta_1)/\max(\eta_0, \eta_1)$, and the secret key rate is

$$K(Q_z, Q_x, \eta) = \max\left((1 + \eta_2)\frac{\eta_1(1 + \eta_2)}{1 + \eta_2}, \frac{\eta_1(1 + \eta_2)}{1 + \eta_2}, \frac{\eta_1(1 + \eta_2)}{1 + \eta_2} - h(\lambda(Q_x, \eta_2)) - h(Q_z)\right).$$

In the limiting cases ($\eta_1 = 1, \eta_2 = \eta$) and ($\eta_1 = \eta, \eta_2 = 1$) we obtain formulas (28) and (33), respectively. The results of calculations according to formula (34) is shown on Figs. 2 and 3. We see that (34) outperforms (32) and (33) and also outperforms (28) if the detection-efficiency mismatch or QBER is large.

Finally, let us recall, that, if both detectors are not perfect and have efficiencies $\eta_0$ and $\eta_1$, then $\eta = \min(\eta_0, \eta_1)/\max(\eta_0, \eta_1)$, and the secret key rate is

$$K(Q_z, Q_x, \eta_0, \eta_1) = \max(\eta_0, \eta_1)K(Q_z, Q_x, \eta)$$

with $K(Q_z, Q_x, \eta)$ given by either (25), (28) or (34).
finite-key analysis. Secondly, we additionally analyze the case when Eve can use the vacuum component of the Bob’s space. We prove that this does not give an advantage to Eve, but, a priori, this was not obvious in the case of detection-efficiency mismatch (see the discussion in the beginning of Sec. II). Thirdly, we have derived a slightly modified formula (34), which outperforms (28) if the detection-efficiency mismatch or QBER is large.

Acknowledgments. We are grateful to A.K. Fedorov, N. Lütkenhaus, X. Ma, D. V. Sych, I. V. Volovich, and Y. Zhou for fruitful discussions and comments. This work was supported by the Russian Science Foundation (project 17-11-01388).

APPENDIX A. PROOF OF THEOREM 1

1. Preliminaries. Define

\[ D\left( \mathcal{G}(\rho_{AB})\| \mathcal{Z}(\mathcal{G}(\rho_{AB})) \right) = f(\rho_{AB}). \] (A1)

Sometimes we will omit the subindexes \( AB \) of \( \rho_{AB} \). The gradient of this function is given by [11]

\[ \nabla f(\rho) = \mathcal{G}(\rho) \left( \log \mathcal{G}(\rho) - \log \mathcal{Z}(\mathcal{G}(\rho)) \right)^T, \] (A2)

where \( \mathcal{G}^i \) is the dual quantum channel to \( \mathcal{G} \). Since \( \rho \) can be specified by a finite number of real numbers, the gradient can be understood as the usual gradient of a function of several real variables.

Let \( \{\Gamma_i\} \) be a Gram-Schmidt orthogonalization of the restriction operators \( \{\Gamma_i\} \) in (15) with respect to the scalar product \( \langle A, B \rangle = \text{Tr} A^\dagger B \), and \( \pi_i \) be the corresponding mean values: \( \text{Tr} \pi_i \rho = \pi_i \). Hence, \( \rho \) can be expressed as \( \rho = \sum_i \pi_i \Gamma_i \). Let also \( \{\Omega_j\} \) be an orthogonal complement of \( \{\Gamma_i\} \) in the real linear space of Hermitian matrices, i.e., \( \{\Gamma_i\} \cup \{\Omega_j\} \) is an orthonormal basis in this space. The set of unit real vectors \( \tilde{\omega} = (\omega_1, \ldots, \omega_m) \) such that

\[ \sum_i \pi_i \Gamma_i + \mu \sum_j \omega_j \Omega_j \geq 0 \] (A3)

for some \( \mu > 0 \) compose a set of allowable directions of movement away from \( \rho \) in the optimization problem (15).

If the projections of the gradient (A2) to all allowable directions are non-negative, then \( \rho \) yields a local minimum to the objective function (A1). Due to the well-known property of the joint convexity of the quantum relative entropy [37] and due to the convexity of the set \( S \) in (15), a local minimum is a global one. Hence, the non-negativity of the projections of the gradient to all allowable directions is a sufficient condition for the global minimum of the secret key rate.

However, this is not a necessary condition since the gradient (A2) may be ill-defined. Firstly, if \( \rho \) belongs to the boundary of the set \( S \), then the gradient is ill-defined by definition. Secondly, the operator \( \mathcal{G}(\rho_{AB}) \) is typically degenerate. This is not a problem for the relative entropy expression (13) due to the rule \( 0 \log 0 = 0 \) and the fact that the kernel subspace of \( \mathcal{Z}(\mathcal{G}(\rho)) \) is a subspace of the kernel subspace of \( \mathcal{G}(\rho) \). But the degeneracy may be a problem for the gradient expression (A2) if the kernel subspace of \( \mathcal{G}(\rho) \) is not a subspace of the kernel subspace of \( \mathcal{G}(\rho + \Delta \rho) \) for an arbitrarily small \( \Delta \rho \). In this case the gradient may be infinite (since the derivative of \( x \log x \) is infinite for \( x = 0 \)).

Let us consider this problem. The general form of \( \rho_{AB} \)

\[ \rho_{AB} = \sum_{i,k\in\{0,1\}} \sum_{j,l\in\{0,1,\text{vac}\}} \rho_{ij,kl} |ij\rangle \langle kl|. \] (A4)

Let us show that, if the operator

\[ \rho'_{AB} = \sum_{i,j,k,l=0}^{1} \rho_{ij,kl} |ij\rangle \langle kl| \] (A5)

is non-degenerate, then the gradient (A2) is well-defined by continuity. We have

\[ \mathcal{G}(\rho_{AB}) = |zz\rangle \tilde{A}_B \langle zz| \otimes \sum_{i,j,k,l=0}^{1} \eta^{(j+l)/2} \rho_{ij,kl} |ij\rangle_{AB} \langle kl| \otimes |ij\rangle_{\tilde{A}B} \langle kl|. \]

We see that \( \mathcal{G}(\rho_{AB}) \) is degenerate on the space \( A\bar{A}B\bar{B} \). Namely,

\[ \mathcal{G}(\rho_{AB}) |ij\rangle_{\tilde{A}B} |i'j'\rangle_{\tilde{A}B} |ab\rangle \bar{A}_B = 0 \] (A6)

whenever \( i \neq i', j \neq j', a \neq z, \text{ or } b \neq z \). Denote \( P_0 \) the projector onto the kernel subspace of \( \mathcal{G}(\rho_{AB}) \). The dual channel \( \mathcal{G}^i \) acts on an arbitrary operator \( A \) in the space \( A\bar{A}B\bar{B} \) as:

\[ \mathcal{G}^i(A) = \sum_{i,j,k,l=0}^{1} \eta^{(j+l)/2} a_{ij,kl} |ij\rangle_{AB} \langle kl|, \] (A7)

where

\[ a_{ij,kl} = A_B \bar{A}_B \bar{A}_B \langle ij, ij, zz|A|kl, kl, zz\rangle_{AB\bar{A}_B \bar{A}_B}. \] (A8)

So, \( \mathcal{G}^i(P_0) = 0 \) and, due to the rule \( 0 \log 0 = 0 \), the expressions \( \mathcal{G}^i(\log \mathcal{G}(\rho)) \) and \( \mathcal{G}^i(\log \mathcal{Z}(\mathcal{G}(\rho))) \) are well-defined.

Also, the elements \( \rho_{i,\text{vac},k,\text{vac}} \) do not contribute neither to the objective function (A1) nor to the right-hand of (A2). Hence, even if all these elements are zero, the gradient is still well-defined by continuity (despite that \( \rho \) belongs to the boundary of \( S \)). Formally, one can impose some regularization onto the channel \( \mathcal{G} \) (see (12)–(15) in [11]) and then pass to the limit of infinitesimal regularization parameter.

We see that the support of \( \mathcal{G}(\rho_{AB}) \) is isomorphic to \( C^2 \otimes C^2 \). We can consider \( \mathcal{G}(\rho_{AB}) \) to be defined only on
the two registers $AB$: the registers $\overline{AB}$ are just copies of $AB$, and the registers $\overline{AB}$ contain the fixed value $z$.

For simplicity and graduality, the further proof of Theorem 1 will consist of two parts. In the first part we restrict the Bob’s Hilbert space to a single-photon subspace spanned by the states $|0\rangle$ and $|1\rangle$. Also we put $t = 1$ in this case. In the second part we will show that the use of the vacuum component does not give an advantage to Eve.

2. The case of two-dimensional Bob’s space: $\mathcal{H}_B = \mathbb{C}^2$, $t = 1$. The matrices $\Gamma_i$ are:

$$\Gamma_1 = \eta \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \Gamma_2 = \frac{\eta}{2} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix},$$

$$\Gamma_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \eta & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \eta \end{pmatrix}$$

(A9)

(the order of rows and columns are as follows: $AB = 00, 01, 10, 11$). Note that

$$\text{Tr} \Gamma_i \rho = \sum_{j,k=1}^4 \Gamma_i^{jk} \rho_{jk} = \sum_{j,k=1}^4 (\Gamma_i^{jk})^* \rho_{jk},$$

(A10)

where $\Gamma_i^{jk}$ and $\rho_{jk}$ are the elements of the corresponding matrices. So, each $\Gamma_i$ fixes a weighted sum of the elements of $\rho$.

Let us prove the necessity of condition (23) for the existence of feasible solutions of the optimization problem. Positive-semidefiniteness of $\rho$ imply

$$|\rho_{00,11}| \leq \sqrt{\rho_{00,00}\rho_{11,11}},$$

(A11a)

$$|\rho_{01,10}| \leq \sqrt{\rho_{01,01}\rho_{10,10}}.$$  \hspace{1cm} (A11b)

Denote

$$\rho_{00,00} = (1 - Q_z)(1 + \delta_0)/2,$$  \hspace{1cm} (A12a)

$$\rho_{01,11} = (1 - Q_z)(1 - \delta_0)/2,$$  \hspace{1cm} (A12b)

$$\rho_{01,01} = Q_z(1 - \delta_1)/2,$$  \hspace{1cm} (A12c)

$$\rho_{10,10} = Q_z(1 + \delta_1)/2.$$  \hspace{1cm} (A12d)

Then, from (19), (A9), (A11), and (A12) (recall that now $t = 1$),

$$2Q_z = 1 - 2\Re \rho_{00,11} - 2\Re \rho_{01,10}$$

$$\geq 1 - (1 - Q_z)\sqrt{1 - \delta_0^2} - Q_z\sqrt{1 - \delta_1^2},$$

(A13)

and

$$p_{\text{pass}} = \frac{1 + \eta}{2} + \frac{1 - \eta}{2}[(1 - Q_z)\delta_0 + Q_z\delta_1].$$

(A14)

The right-hand side of (A13) with the restriction (A14) for a fixed $p_{\text{pass}}$ takes its minimum for $\delta_0 = \delta_1 = \delta$. The minimum is equal to the right-hand side of (23), and equality (24) takes place. Hence, (23) is a necessary condition for the existence of a positive semi-definite operator $\rho_{AB}$ satisfying (19).

Consider the following operator:

$$\rho_{AB} = \frac{1 - Q_z}{2} \begin{pmatrix} 1 + \delta & 0 & 0 & 1 - 2Q_z \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 - \delta \\ 1 - 2Q_z & 0 & 0 & 0 \end{pmatrix} + \frac{Q_z}{2} \begin{pmatrix} 0 & 1 - \delta & 0 & 1 - 2Q_z \\ 0 & 0 & 0 & 0 \\ 0 & 1 - 2Q_z & 1 + \delta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$  \hspace{1cm} (A15)

If (23) is true, then this operator is positive semi-definite and satisfies (19) (for $t = 1$). This proves the sufficiency of condition (23) for the existence of a solution. As we will see, (A15) is an optimal solution.

Recall that we consider $\mathcal{G}(\mathcal{P}_{AB})$ to be defined only on the registers $AB$. Then,

$$\mathcal{G}(\mathcal{P}_{AB}) = \frac{1 - Q_z}{2} \begin{pmatrix} 1 + \delta & 0 & 0 & (1 - 2Q_z)\sqrt{\eta} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & (1 - \delta)\eta \\ (1 - 2Q_z)\sqrt{\eta} & 0 & 0 & 0 \end{pmatrix} + \frac{Q_z}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & (1 - \delta)\eta & (1 - 2Q_z)\sqrt{\eta} & 0 \\ 0 & (1 - 2Q_z)\sqrt{\eta} & 1 + \delta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

(A16)

and $\mathcal{Z}(\mathcal{G}(\mathcal{P}_{AB}))$ is the diagonal part of $\mathcal{G}(\mathcal{P}_{AB})$. The eigenvalues of $\mathcal{G}(\mathcal{P}_{AB})$ are:

$$\lambda_{1,2} = (1 - Q_z)\lambda_{\pm}, \quad \lambda_{3,4} = Q_z\lambda_{\pm},$$

(A17)

where $\lambda_{\pm} = p_{\text{pass}}\lambda(Q_z, \eta, t, p_{\text{pass}})$ (see (26)) and $\lambda_{\pm} = p_{\text{pass}} - \lambda_{\pm}$. Then the straightforward calculation of (13) yields (25).

2. The proof of optimality of $\mathcal{P}_{AB}$. We have obtained the desired formula (25). It remains to show that $\mathcal{P}_{AB}$ is optimal. We will show that the gradient $\nabla f(\mathcal{P}_{AB})$ is orthogonal to all allowable directions of movement away from $\mathcal{P}_{AB}$. This will mean that $\mathcal{P}_{AB}$ provides an optimal value to (15a).

Let (23) be satisfied as a strict inequality. In this case operator (A15) is non-degenerate and the gradient, as we concluded above, is well-defined. The case when (23) is satisfied as an equality can be obtained as a limiting case. The continuity of the objective function in $\rho_{AB}$ is proved in [11].

Consider the eigenvectors $(\cos \theta, \sin \theta)$ and $(-\sin \theta, \cos \theta)$, $\theta = \frac{1}{2} \arctan \frac{2\sqrt{1 - 2Q_z}}{1 - \eta + 2Q_z(1 + \eta)}$, of the matrix

$$\begin{pmatrix} 1 + \delta & (1 - 2Q_z)\sqrt{\eta} \\ (1 - 2Q_z)\sqrt{\eta} & (1 - \delta)\eta \end{pmatrix}$$

(A18)

corresponding to the eigenvalues $2\lambda_{\pm}$. Then the direct
calculation according to (A2) and (A7) gives
\[
\nabla f(\overline{\rho}_{AB}) = \begin{pmatrix}
  d_0 & 0 & 0 & 0 \\
  0 & \eta d_1 & 0 & 0 \\
  0 & 0 & d_0 & 0 \\
  0 & 0 & 0 & \eta d_1
\end{pmatrix}
+ \sqrt{\eta} \sin \theta \cos \theta \log \frac{\lambda_+}{\lambda_-} \begin{pmatrix}
  0 & 0 & 1 & 0 \\
  0 & 1 & 0 & 0 \\
  1 & 0 & 0 & 0
\end{pmatrix},
\]
where
\[
d_0 = \cos^2 \theta \log \lambda_+ + \sin^2 \theta \log \lambda_-,
\]
\[
d_1 = \sin^2 \theta \log \lambda_+ + \cos^2 \theta \log \lambda_- - \log \eta.
\]

We see that the gradient is orthogonal to all directions except the changes in the diagonal of \(\rho_{AB}\) and directions that change the sum of the secondary diagonal. However, the sum of the secondary diagonal is fixed by the restrictions \(\Gamma_1\) and \(\Gamma_2\). According to the restrictions \(\Gamma_1\) and \(\Gamma_3\), the allowable directions of changes in the diagonal \((\Delta \rho_{00}, \Delta \rho_{01}, \Delta \rho_{10}, \Delta \rho_{11})\) satisfy the relations \(\Delta \rho_{00} = -\Delta \rho_{10}\) and \(\Delta \rho_{01} = -\Delta \rho_{11}\). Hence,
\[
\text{Tr} \nabla f(\overline{\rho}_{AB}) \text{diag}(\Delta \rho_{00}, \ldots, \Delta \rho_{11})
= d_0(\Delta \rho_{00} + \Delta \rho_{10}) + \eta d_1(\Delta \rho_{01} + \Delta \rho_{11}) = 0,
\]
and the gradient is thus orthogonal to all allowable directions. This means that \(\overline{\rho}_{AB}\) provides a minimum to the secret key rate (15a) for the case of two-dimensional Bob’s space.

3. The case of three-dimensional Bob’s space.

Now we return to the case of three-dimensional Bob’s space and arbitrary \(t \leq 1\). Since \(t\) is a common factor in all restrictions (19), if we multiply (A15) by \(t\), then the restrictions will be satisfied for this value of \(t\). We can also see the vacuum component of \(\rho_{AB}\) does not contribute directly (i.e., besides the factor \(t\)) neither to the secret key rate nor to the gradient (see (A2) and (A7)) nor to the restrictions. So, the state \(\overline{\rho}_{AB} \oplus 0 + (1 - t)I_2/2 \otimes \langle\text{vac}|\langle\text{vac}\rangle\) where \(\overline{\rho}_{AB}\) is a matrix defined by (A15) on the 4-dimensional subspace and \(\oplus 0\) denotes its embedding into the 6-dimensional space \(\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^3\), is an optimal state and the secret key is given by (25). In other words, the use of the vacuum component and transmission loss do not give an advantage to Eve: her knowledge per sifted key bit remains the same.

APPENDIX B. INFORMATION LEAKAGE IN THE ERROR CORRECTION FOR THE CASE OF DETECTION-EFFICIENCY MISMATCH

Our aim is to calculate the quantity \(H(\overline{\mathcal{X}}|B\overline{A}B)_{\rho^{(3)}}\) in (12). Since the registers \(A\overline{B}\) are the copies of \(AB\) and the registers \(\overline{A}\overline{B}\) store the fixed value \(z\) in \(\rho^{(3)}\) (see the beginning of Appendix A for details), we can consider \(\rho^{(3)}\) to be defined only on the two registers \(A\) and \(B\): \(\rho_{A\overline{B}}^{(3)}\). Further, \(H(A|B)_{\rho^{(3)}}\) is a classical conditional entropy with the two binary random variables \(A\) and \(B\). It is well-known to be upper bounded by \(h(Q_z)\), where \(Q_z\) is the probability of error \((A \neq B)\).

However, in our case, for \(\overline{\rho}_{AB}\) given by (A15), which corresponds to an optimal Eve’s attack, \(H(A|B)\) is exactly \(h(Q_z)\) whenever \(\delta = 0\). Indeed the diagonal part of \(\overline{\rho}_{AB}\) takes the form \((1 - Q_z, Q_z, 1 - Q_z)/2\) in this case (the order of the values of the registers is the same as in Appendix A: \(AB = 00, 01, 10, 11\)). Further, \(\rho_{A\overline{B}}^{(3)} = p_{\text{pass}}G(\rho_{AB})\). The diagonal part of \(\rho_{A\overline{B}}^{(3)}\) is then \((1 - Q_z, Q_z\eta, Q_z, (1 - Q_z)\eta)/(1 + \eta)\). This is the joint distribution of \(A\). It is straightforward to show that \(H(A|B) = h(Q_z)\). So, the state \(\overline{\rho}_{AB}\) simultaneously minimizes the first term in the right-hand side of (12) and maximizes the second term there. Thus, it minimizes the whole expression (12). Hence, we can substitute the second term by its maximal value \(h(Q_z)\) without loss of tightness of the bound.

If \(\delta \neq 0\), then, strictly speaking, \(H(A|B)\) is smaller than \(h(Q_z)\). However, in this paper we assume that a non-zero value of \(\delta\) is caused by the statistical fluctuations or by the Eve’s interference of the same order (see the discussion after Theorem 1 and Corollary 1) and, hence, \(\delta\) is infinitesimal in the limit \(n \to \infty\). Hence, the difference between \(H(A|B)\) and \(h(Q_z)\) is also infinitesimal.

[1] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quant. Inf. **2**, 16025 (2016).
[2] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] P.W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] R. Renner, arXiv:quant-ph/0512258 (2005).
[6] M. Tomamichel, C.C.W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[7] M. Tomamichel and A. Leverrier, Quantum **1**, 14 (2017).
[8] C.-H.F. Fung, K. Tamaki, B. Qi, H.-K. Lo, X. Ma, Quant. Inf. Comput. **9**, 131 (2009).
[9] Y. Zhao, C.-H.F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[10] S. Sajeev, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).
[11] A. Winick, N. Lütkenhaus, and P.J. Coles, Quantum **2**, 77 (2018).
[12] P.J. Coles, E.M. Metodiev, and N. Lütkenhaus, Nat. Commun. **7**, 11712 (2016).
[13] M. Dušek, M. Jahma, and N. Lütkenhaus Phys. Rev. A 62, 022306 (2000).
[14] N. Lütkenhaus and M. Jahma, New J. Phys. 4, 44 (2002).
[15] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[16] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[17] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A 72, 012326 (2005).
[18] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Phys. Rev. A 95, 012333 (2017).
[19] A. S. Trushechkin, E. O. Kiktenko, and A. K. Fedorov, Phys. Rev. A 96, 022316 (2017).
[20] Y. Fei, X. Meng, M. Gao, Z. Ma, and H. Wang, Eur. Phys. J. D 72, 107 (2018)
[21] T. Moroder, M. Curty, and N. Lütkenhaus, New J. Phys. 11, 045008 (2009).
[22] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. Romero Alvarez, T. Moroder, and N. Lütkenhaus, Phys. Rev. A 89, 012325 (2014).
[23] Y. Zhang and N. Lütkenhaus, Phys. Rev. A 95, 042319 (2017).
[24] N. Walenta et al. New J. Phys. 16 013047 (2014).
[25] E. O. Kiktenko, A. S. Trushechkin, Y. V. Kurochkin, and A. K. Fedorov, J. Phys. Conf. Ser. 741, 012081 (2016).
[26] E. O. Kiktenko, A. S. Trushechkin, C. W. Lim, Y. V. Kurochkin, A. K. Fedorov, Phys. Rev. Applied 8, 044017 (2017).
[27] E. O. Kiktenko, A. S. Trushechkin, A. K. Fedorov, Lobachevskii J. Math. 39, 992 (2018).
[28] E. O. Kiktenko, A. O. Malyshev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, A. K. Fedorov, arXiv:1810.05841 (2018).
[29] A. S. Holevo, Quantum systems, channels, information. A mathematical introduction (De Gruyter, Berlin–Boston, 2012).
[30] I. Devetak and A. Winter, Proc. R. Soc. Lond. A, 461, 207 (2005)
[31] P. J. Coles, Phys. Rev. A 85, 042103 (2012).
[32] T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. 113, 140401 (2014).
[33] J. Ma, Y. Zhou, X. Yuan, X. Ma, arXiv:1810.03267 (2018).
[34] S. Watanabe, R. Matsumoto, and T. Uyematsu, Phys. Rev. A 78, 042316 (2008).
[35] F. Dupuis, O. Fawzi, and R. Renner, arXiv:1607.01796 (2005).
[36] A. S. Trushechkin, Presentation at the International conference “Quantum information, statistics, probability” with a special session dedicated to A. S. Holevo’s 75-th birthday, Moscow, Russia, 12th September, 2018, http://www.mathnet.ru/eng/present19544 (video).
[37] E. H. Lieb, Adv. Math. 11, 267 (1973).