METHODOLOGICAL NOTES

Security of the decoy state method for quantum key distribution

A S Trushechkin, E O Kiktenko, D A Kronberg, A K Fedorov

Contents

Abstract. Quantum cryptography or, more precisely, quantum key distribution (QKD), is one of the advanced areas in the field of quantum technologies. The confidentiality of keys distributed with the use of QKD protocols is guaranteed by the fundamental laws of quantum mechanics. This paper is devoted to the decoy state method, a countermeasure against vulnerabilities caused by the use of coherent states of light for QKD protocols whose security is proved under the assumption of single-photon states. We give a formal security proof of the decoy state method against all possible attacks. We compare two widely known attacks on multiphoton pulses: photon-number splitting and beam splitting. Finally, we discuss the equivalence of polarization and phase coding.

Keywords: quantum cryptography, quantum key distribution, BB84, decoy states

A S Trushechkin [(1, 2, †)], **E O Kiktenko** [(1, 2, 3, 4)],
D A Kronberg [(1, 3, 4)], **A K Fedorov** [(3, 4, ‡)]
[(1)] Steklov Mathematical Institute, Russian Academy of Sciences,
  ul. Gubkina 8, 119991 Moscow, Russian Federation
[(2)] National University of Science and Technology MISIS,
  Competence Center of the Quantum Communications
  National Technology Initiative,
  Leninskii prosp. 4, 119049 Moscow, Russian Federation
[(3)] International Center for Quantum Optics and Quantum Technologies
  (Russian Quantum Center),
  ul. Novaya 100, 143025 Skolkovo, Moscow region, Russian Federation
[(4)] Moscow Institute of Physics and Technology (National Research
  University), Institutskii per. 9, 141701 Dolgoprudny,
  Moscow region, Russian Federation
E-mail: [(†)] trushechkin@mi-ras.ru, [(‡)] akf@rqc.ru

1. Introduction

Information protection is one of the key demands of modern society. In most cases, information security is ensured by using cryptographic techniques, such as encryption. Encryption is commonly understood as the transformation of information that is needed to be secured (plaintext) into an encrypted message (ciphertext) with the use of a certain algorithm [1]. At the same time, to realize encryption, the legitimate parties of the communication need a so-called cryptographic key, which is a secret parameter (usually a binary string of a certain length), which determines the choice of a specific transformation of information when performing encryption. The key distribution problem is one of the most important in cryptography [1, 2]. For example, Ref. [2] emphasizes: "Keys are as valuable as all the messages they encrypt, since knowledge of the key gives knowledge of all the messages. For encryption systems that span the world, the key distribution problem can be a daunting task."

Several approaches to the distribution of cryptographic keys can be used. First, the keys can be delivered using trusted couriers. The main disadvantage of this method is the presence of the human factor. Furthermore, with the increasing amount of transmitted data keys every year, physical transfer is becoming more difficult. An alternative approach is public-key cryptography. It is based on the use of so-called one-way functions, i.e., functions that are easy to compute but for which it is difficult to find an argument for a given function value. Examples include the Diffie–Hellman and RSA (abbreviation from the surnames Rivest, Shamir, and Adleman) algorithms (which were developed for encrypting messages, but are also used for key distribution), which use the complexity of solving discrete logarithm and integer factorization problems, respectively. The majority of data transmitted on the Internet is protected with the use of public-key algorithms, which are included in the HTTPS (HyperText Transfer Protocol Secure) protocol.

Today, efficient (of polynomial complexity) classical algorithms for solving factorization and discrete logarithm problems are unknown, but there is the efficient quantum Shor algorithm [3]. Therefore, when a quantum computer becomes available for an adversary, the widely used algorithms for key distribution would no longer provide information security. Besides, the impossibility of the existence of efficient classical algorithms for solving these problems has also not been proven, and it is only a conjecture. There are currently no quantum computers capable of implementing Shor's quantum algorithm for fairly large numbers, but such devices may appear in the near future. Also, alternative approaches to solving the factorization problem are being developed, for example, using variational quantum algorithms [4]. Thus, ensuring the confidentiality of data requires an early transition to cryptographic methods that would be resistant to attacks using a quantum computer [5].

One possible solution for key distribution in the 'post-quantum era' is to use quantum key distribution (QKD), which was proposed by C Bennett and G Brassard in 1984 [6], and also independently by A Ekert in 1991 [7]. Quantum key distribution is based on the idea of encoding information into the quantum states of individual quantum systems. For example, the most common QKD protocol BB84 [6] uses photon states (for example, polarization) in two mutually unbiased bases [8]. The idea of using mutually unbiased bases was introduced by S Wiesner in the 1970s (his paper [9] was published later, in 1983) within the concept of 'quantum money'. Fundamental limitations of quantum mechanics, such as the no-cloning theorem for a quantum state and the Heisenberg uncertainty principle, restrict the ability to read quantum information without changing it.

The first complete mathematical proof of the security of the BB84 protocol was obtained in 1996 by D Mayers [10, 11]. Further proofs have followed, for example, Refs [12, 13]. The general mathematical theory of quantum key distribution, which is based on information theory and entropy characteristics, was developed by R Renner [14] and then improved in subsequent papers, among which we highlight Refs [15, 16]. One recent result in this area is the development of the 'entropy accumulation' technique [17], which allows one to map the security proof for the case of so-called collective attacks (easier to analyze) to the case of general attacks (coherent attacks) that are difficult to analyze directly [18, 19]. For the case of BB84, it simplifies the security proof and also allows one to prove resistance against general attacks more generally, for example, in the case of detection-efficiency mismatch [20]. For the operational meaning of the security parameter used in quantum key distribution, see Refs [21, 22].

However, in practical implementations of QKD protocols, differences from ideal abstract protocols naturally arise [19, 23]. These differences have a significant impact on the cryptographic security of implementation. For example, the BB84 protocol assumes the encoding of information into states of single photons. However, the generation of single photons 'on demand' and at a high rate is a technically difficult task; therefore, instead of single photons, QKD uses weak coherent pulses [24]. This makes it possible to realize a photon-number splitting attack [25]: the adversary can measure the number of photons in a pulse in a nondisturbing way, take one photon from all multiphoton states, and block all single-photon (i.e., secure) states, or at least some of them. This allows the adversary to extract the entire key or a significant part of it without introducing errors, which violates the basic property of the protocol about the relationship between the error level and the amount of intercepted information and, thus, makes the protocol implementation unreliable.

The vulnerability of quantum key distribution to such an attack can be eliminated by using the decoy state method, which was proposed in Refs [26–29]. The method is based on the fact that the sender does not use one fixed value for the intensity of coherent states, but each time randomly selects the intensity from a known finite set (also known to the adversary). One of these intensities (the largest) is the signal one, and it is used to generate a key; the rest are decoys, and they are used to estimate the level of the adversary's intervention in the multiphoton pulses.

Being just a parameter in the probability distribution (namely, the Poisson distribution), the intensity is a non-observable quantity, so that only the photon number that is the realization of this random variable is observed. Therefore, the adversary does not know what intensity was used in a given position and carries out their actions based only on the observed number of photons.

After finishing the transmission of quantum states, the sender announces the intensity of each position. The legitimate parties then collect registration statistics for each intensity separately. The states with lower intensities can be called decoy states in the sense that, for an adversary, who does not know the intensity parameter at the time of the attack, they are indistinguishable from the signal states, but after the intensities are announced, they become a sort of 'tag' which can be used to make separate statistics.

From a mathematical point of view, the statistics of detecting states with different intensities gives the legitimate parties additional equations for a better estimation of unknown parameters, such as the number of positions in the sifted key obtained from single-photon pulses (i.e., those that cannot be intercepted without introducing errors) and the fraction of errors in them. In particular, blocking all single-photon states by the adversary would lead to the blocking of almost all low-intensity decoy states.

Today, the decoy-state BB84 QKD protocol has been theoretically studied in detail [20, 26–33], demonstrated in experiments [23, 34], including Russian domestic systems [35], and it is considered to be a candidate for the international standard [36]. Nevertheless, doubts about its security against all possible attacks, not just photon-number splitting attacks, have been expressed [37, 38]. For this reason, in this article, we not only describe the decoy state method but also provide the formal security proof of the decoy state method against all possible attacks. This fact is usually not explained in the literature, since it is regarded as obvious. The proof would not refer to a photon-number splitting attack. However, as demonstrated, the photon-number splitting attack is optimal for the adversary, which explains the fact that countermeasures only against this attack are considered in the literature.

Separately, we compare the photon-number splitting attack with another common attack, namely, the beam splitting attack, and clearly demonstrate the lower efficiency of the latter. At the same time, at realistic levels of losses, as has been shown, these attacks give similar results.

The text is organized as follows. In Section 2, the BB84 protocol is described. In Section 3, the problem in this protocol, which is related to the encoding information using

coherent instead of single-photon states, is discussed, and the photon-number splitting attack is considered. In order to formulate further results concerning the security of the protocol, in Section 4, the concepts of achievable and maximally achievable secret key rates are introduced, and the well-known Devetak–Winter formula [39] for the maximal secret key rate is presented. Section 5 is devoted to reducing the multiphoton case to the single-photon case if the transmitted states are statistical mixtures of Fock states (states with a certain number of photons). The theorem in this section formally justifies the decoy state method and its security against all possible collective attacks. Here, the optimality of the photon-number splitting attack is justified. Section 6 completes this analysis: an equivalent formulation of the protocol in terms of an entangled state allows using the entropy accumulation technique and justifies the security of the protocol to all possible (not just collective) attacks. Section 7 is devoted to describing the decoy state method. In Section 8, another attack, namely the beam splitting attack, is considered, which, unlike the photon-number splitting attack, has been implemented experimentally. In Section 9, we compare the photon-number splitting and beam splitting attacks and explain why the latter is less efficient. Finally, in Section 10, we respond to the doubts expressed in Ref. [40] about the applicability of the decoy state method in the case of phase encoding rather than polarization encoding, and demonstrate the complete equivalence of these encodings.

It should be noted that the field of quantum information processing has already become the subject of several reviews in *Physics–Uspekhi*. In particular, a number of problems in quantum computing were considered in Refs [41, 42], and several aspects of quantum key distribution were considered in Ref. [43]. The progress of recent decades on the development of industrial devices for quantum key distribution has taken research in this area to the next level, where a number of important practical aspects of the implementation of such systems have come to the fore. In particular, one of the central problems of this area is to analyze the resistance to attacks of quantum key distribution protocols, which is the subject of this review. The main result is a rigorous justification of the security of the decoy state method in quantum cryptography.

2. BB84 protocol

In this section, we describe the BB84 protocol [6] under the assumption of a single photon source on the sender side. Each QKD protocol can be divided into two main stages: transmission of quantum states and post-processing of the measurement results. Following Ref. [1], the communication participants that desire to obtain a shared key we call the sender and the receiver, while the eavesdropper side is the adversary. Sender and receiver together are also referred to as legitimate parties.

In the first 'quantum' stage of the BB84 protocol, four quantum states are used, which form two orthogonal bases $z = \{|0\rangle_z, |1\rangle_z\}$ and $x = \{|0\rangle_x, |1\rangle_x\}$ in the two-dimensional Hilbert space $\mathbb{C}^2$. The quantum system that corresponds to this space is called the 'quantum bit' or 'qubit'. The values 0 or 1 indicate which classic bit is encoded by the corresponding basis vector. Elements of the bases are expressed in terms of elements of another basis according to the relations

$$|0\rangle_x = \frac{|0\rangle_z + |1\rangle_z}{\sqrt{2}}, \quad |1\rangle_x = \frac{|0\rangle_z - |1\rangle_z}{\sqrt{2}}. \quad (1)$$

If the information is encoded into photon polarization, then the vectors $|0\rangle_z$ and $|1\rangle_z$ can correspond, for example, to horizontal and vertical polarizations. In this case, $|0\rangle_x$ and $|1\rangle_x$ correspond to two diagonal polarizations that are rotated by 45° and 135°, respectively, relative to the horizontal direction. We assume polarization coding for convenience of the presentation, but, in fact, no restriction is imposed on the method of information encoding: Formally, $|0\rangle_z$, $|1\rangle_z$, $|0\rangle_x$, and $|1\rangle_x$ are vectors in the Hilbert space and one can use any encoding which fulfills relation (1). In particular, we explain the equivalence of the polarization and phase encodings below in Section 10.

As is seen from (1), when measuring a qubit in a basis different from the preparation basis, the result is a random value. In the case of coincidence of the preparation and measurement bases, the result perfectly correlates with the prepared state of the qubit (in the ideal case, i.e., in the absence of errors in the channel and measuring devices).

Let us now describe the BB84 protocol.

(1) The sender randomly chooses a basis from the set $\{z, x\}$ and the value of the transmitted bit of information: 1 or 0. Bits are selected with equal probabilities of $1/2$.

(2) Then, the photons prepared in the corresponding states are transmitted through the quantum channel.

(3) The receiver randomly chooses a measurement basis, z or x, for each qubit and measures the state of the qubit in the selected basis. If the preparation and measurement bases coincide, the received bit value coincides (ideally) with the sent one. If the bases do not coincide, the bits of the sender and the receiver do not correlate (that is, they may or may not coincide with equal probabilities) due to the fact that the bases are mutually unbiased (1). Usually, the communication channel contains large losses; therefore, not all positions are registered by the receiver.

(4) The above steps are repeated many times, i.e., a large number of quantum states are transmitted. As a result, legitimate parties receive two sequences of bits k_A^{raw} and k_B^{raw}, which are called *raw quantum keys*.

Since a perfect copy of a quantum state cannot be created and the adversary does not know the basis in which the bit is encoded in a given position, the adversary needs to employ imperfect copying techniques that induce distortions.

In the original version of the protocol, the bases are chosen with equal probabilities. Later, an improved variant of the protocol was suggested, in which one of the bases (for example, the z basis) is chosen more frequently than the other one [44]. This reduces the number of basis mismatches and, therefore, the portion of sifted positions, i.e., it increases the key rate. Let us denote the probabilities of choices of the bases as p_z and $p_x = 1 - p_z$. In the limit of an infinite number of pulses N, one can put $p_z \to 1$, $p_x \to 0$. For example, one can take $p_x = O(1/\sqrt{N})$: this is enough for the statistical estimation of the parameters related to observations in the x basis, since the statistical fluctuations have an order of $O(1/\sqrt{N})$. Then, the following modification of the protocol can be adopted: only positions in which both parties used the z basis are used for key generation. The bits encoded in the x basis do not participate in the formation of the secret key; they are only needed to estimate the level of eavesdropping. Note that a version of the protocol in which the bases are chosen pseudo-randomly using a pre-distributed random sequence is considered in Ref. [45].

At the second stage, the legitimate parties carry out the classical post-processing of raw keys using communication

over a public authenticated channel [18, 46, 47]. It consists of the following steps:

1. *Announcements*. The receiver announces the position numbers in which the signal was registered. The sender and receiver declare the bases used in all positions. When using the decoy state method, the sender also announces the type of each pulse (signal or decoy). The sender and the receiver can also announce bits in positions that do not participate in the formation of the secret key: in positions in which the parties used the x basis and in the decoy pulses.

2. *Key sifting*. Positions in which decoy intensity were used, registration did not occur, or at least one of the legitimate parties used the x basis are sifted out. The resulting keys, k_A^{sift} and k_B^{sift}, are called *sifted keys*. Ideally, they should match, but as a result of natural noise in the channel or adversary actions, they do not match. Moreover, the adversary may have partial information about them.

3. *Error correction*. One of the sifted keys (for example, belonging to the sender) is considered to be a reference. Differences between it and the sifted key of the other side are considered to be errors. One can use error correction codes or interactive error correction procedures to correct errors. Low-density parity-check (LDPC) codes are quite common. Often, this procedure ends with *verification*: the identity of the sifted keys is checked using hash functions (see Ref. [48]). As a result of this stage, the legitimate parties receive identical *verified keys* $k_A^{\text{ver}} = k_B^{\text{ver}}$ with a high probability. An efficient method for error correction in the BB84 protocol error correction based on LDPC codes is described in Ref. [49]; see also Ref. [50].

4. *Estimation of the level of eavesdropping* and making a decision about creating the key or renouncing it (aborting the protocol) based on the observed data. Quantum cryptography is based on the fact that information encoded in nonorthogonal quantum states cannot be read by a third party (which does not know the basis in which the key bit in a given position was encoded) without 'spoiling' these states. Therefore, interception by the adversary would lead to an increase in the number of errors (i.e., mismatched positions in sifted keys) between the legitimate parties. In this version of the protocol, where only the bits encoded in the z basis are involved in the formation of the key, only the fraction of errors in the x basis is needed to assess the level of eavesdropping. If the error rate exceeds a certain critical threshold, the protocol is aborted. Otherwise, the parties proceed to the last step. Thus, in quantum cryptography, it is impossible to eavesdrop without being detected.

5. *Privacy amplification*. The sender randomly chooses a so-called hash function from a family of 2-universal hash functions and sends it to the receiver via a public channel. Both then compute the hash value of their (identical) sifted keys. As a result, they get a common shorter key (*final key*) $k_A^{\text{fin}} = k_B^{\text{fin}}$, but the information of the adversary about which is negligible. With an infinitely large length of the sifted key, it can be made arbitrarily small. The more information the adversary has about the sifted key (as a result of eavesdropping and as a result of disclosure by legitimate users of some of the information during error correction), the more compression of the key in the privacy amplification procedure is required, i.e., the shorter the final key and the lower the key rate.

As can be noted, the post-processing procedure requires the parties to communicate via the classical channel. It is assumed that the adversary is freely able to listen to this channel but cannot change the messages transmitted over it or send their own. This is provided by message authentication codes. In quantum cryptography, information-theoretically secure Wegman–Carter codes [51] are often used (i.e., provably secure without assumptions about the adversary's computing power). They require legitimate parties to have an initial short secret key. It is sufficient to have an initially shared secret for the first key distribution session. Further, in each session, part of the generated key is kept for use in a message authentication code in the next session and is not used for other purposes. (See Ref. [52] for the latest developments in the reduction of the portion of the key that is consumed during authentication.)

Here, we assumed that the sender is sending single-photon states. This corresponds to the fact that their Hilbert space is $\mathbb{C}^2$. At the end of the Introduction, there are references regarding the history of the security proof for the single-photon BB84 protocol.

3. Information encoding in weak coherent pulses. Photon-number splitting attack

Let us now take into account that, in practice, information is most often encoded not into true single-photon states but into weak coherent pulses. This means that the Hilbert space of the sender is not $\mathbb{C}^2$, but $\mathscr{F}(\mathbb{C}^2)$ (the boson Fock space over $\mathbb{C}^2$). The orthonormal basis in this space is formed by the vectors $|\text{vac}\rangle$ and $|j_0, j_1\rangle_z$, where $|\text{vac}\rangle$ is the vacuum state, and

$$|j_0, j_1\rangle_z = \frac{(a_{z0}^\dagger)^{j_0}(a_{z1}^\dagger)^{j_1}}{\sqrt{j_0! j_1!}} |\text{vac}\rangle, \tag{2}$$

$j_0, j_1 \geqslant 0$ ($|0,0\rangle_z = |\text{vac}\rangle$), $a_{z0}^\dagger$, $a_{z1}^\dagger$, a_{z0}, a_{z1} are creation and annihilation operators of a photon in the states $|0\rangle_z, |1\rangle_z \in \mathbb{C}^2$, respectively. Another orthonormal basis is formed by vectors $|\text{vac}\rangle$ and $|j_0, j_1\rangle_x, j_0, j_1 \geqslant 0$, where

$$|j_0, j_1\rangle_x = \frac{(a_{x0}^\dagger)^{j_0}(a_{x1}^\dagger)^{j_1}}{\sqrt{j_0! j_1!}} |\text{vac}\rangle, \tag{3}$$

$$a_{x0}^\dagger = \frac{a_{z0}^\dagger + a_{z1}^\dagger}{\sqrt{2}}, \qquad a_{x1}^\dagger = \frac{a_{z0}^\dagger - a_{z1}^\dagger}{\sqrt{2}} \tag{4}$$

are creation and annihilation operators of photons in states $|0\rangle_x, |1\rangle_x \in \mathbb{C}^2$, respectively. In particular, vectors $|0\rangle_b, |1\rangle_b \in \mathbb{C}^2$ can be identified with vectors $|1,0\rangle_b, |0,1\rangle_b \in \mathscr{F}(\mathbb{C}^2)$, respectively, $b \in \{z, x\}$.

Then, the transmitted coherent state has the form

$$|\alpha; u\rangle_b = \exp\left(-\frac{\mu}{2}\right)|\text{vac}\rangle + \exp\left(-\frac{\mu}{2}\right)\sum_{j=1}^\infty \frac{\alpha^j}{\sqrt{j!}} |\psi_{ju}^b\rangle, \tag{5}$$

where $u \in \{0, 1\}$, $b \in \{z, x\}$,

$$|\psi_{j0}^b\rangle = |j, 0\rangle_b, \quad |\psi_{j1}^b\rangle = |0, j\rangle_b,$$

$b \in \{z, x\}$. Here, $\alpha \in \mathbb{C}$ is the parameter of the coherent state, $\mu = |\alpha|^2$ is the pulse intensity, $\alpha = \sqrt{\mu} \exp(i\theta)$. The protocol demands a random change in the phase θ of the coherent state from pulse to pulse. This is provided either by a laser operating mode (passive randomization) or by introducing an additional element, which is connected to a random number generator and randomizes the phase, into the optical system of the sender (active randomization) (see also Remark 1 in

Section 5). Then, the adversary and the receiver do not 'observe' a pure coherent state but a mixed one with the density operator

$$\rho_{\mu u}^b = \frac{1}{2\pi} \int_0^{2\pi} d\theta \, |\sqrt{\mu} \exp(i\theta); u\rangle_b \langle \sqrt{\mu} \exp(i\theta); u|$$

$$= \exp(-\mu)|vac\rangle\langle vac| + \exp(-\mu) \sum_{j=1}^{\infty} \frac{\mu^j}{j!} |\psi_{ju}^b\rangle\langle\psi_{ju}^b|. \quad (6)$$

Here, for simplicity, we assume that the basis b and the bit u are fixed; otherwise, it is necessary to average over them. This mixed state can be interpreted as follows. The vacuum state is sent with the probability $\exp(-\mu)$, whereas the state with the j photon in the corresponding polarization is sent with the probability $\exp(-\mu)\mu^j/j!$. Thus, the number of photons in the pulse is distributed according to the Poisson distribution with the parameter (average number of photons) μ. Usually, $\mu < 1$ is chosen; therefore, such impulses are referred to as weak coherent.

The presence of more than one photon in some pulses allows the adversary to carry out a so-called *photon-number splitting attack* [25]. Sometimes this is understood as an attack of a special type, but we mean a whole class of attacks, which we describe now. Each attack of this class begins with the adversary measuring the number of photons, i.e., applying an observable which corresponds to the probability projection-valued measure $\{P_j\}_{j=0}^{\infty}$, where

$$P_j = \sum_{j_0+j_1=j} |j_0, j_1\rangle_z \langle j_0, j_1| = \sum_{j_0+j_1=j} |j_0, j_1\rangle_x \langle j_0, j_1|. \quad (7)$$

For an outcome j, state (6) transforms into $P_j\rho_{\mu u}^b P_j/\mathrm{Tr}(\rho_{\mu u}^b P_j)$. This measurement is also called nondemolition, because the photons are not destroyed, and their polarization is not changed. In practice, such a nondemolition measurement has not yet been implemented, but it is possible in theory, since the corresponding probability projector-valued measure exists. If the adversary observes that there are two or more photons in the transmission ($j \geqslant 2$), then they take one photon into their quantum memory and send the rest to the receiver. After the bases are announced via the public channel, the adversary would find out which basis in a given position the key bit is encoded. They measure with this basis and recognize this bit. In this case, the state of those photons that were sent to the receiver does not change. This violates the basic principle of quantum cryptography that the observation leads to changes in the state and occurrence of (or increase in) errors. If the pulse contains one photon, the adversary can still find out the information encoded in it only at the cost of changing the state and, accordingly, introducing errors. Therefore, the adversary can block all or part of one-photon states, i.e., stop their transmission to the receiver, simulating natural losses in the communication channel. They can attack unblocked single-photon states in the usual way (at the cost of introducing errors).

The blocking of some pulses by the adversary leads to an increase in the level of losses, which can be detected by the legitimate parties. Therefore, it is assumed that the adversary can replace the communication line and even detectors with ideal ones and then block as many single-photon pulses as possible to reproduce the natural level of loss. The higher the level of natural losses (which depends primarily on the length of the communication line (see Section 7)), the more single-photon states the adversary can block. If the natural losses in the channel are so large that the adversary can block all single-photon states, then the adversary would have full information about the key without introducing noise, since all the signals that reach the receiver would be multiphoton. Thus, the quantum key distribution protocol is completely compromised.

4. Secret key rate

The *final (secret) key rate* is understood as the limit of the ratio of the length of the final key to the length of the sifted key, as the number of pulses tends to infinity. The *achievable* secret key rate means the secret key rate at which it is possible to ensure the requirement of an infinitesimal amount of information of the adversary about the final key (in the mentioned limit). As mentioned above, this requires a certain level of compression in the privacy amplification procedure. Of course, if a certain rate is achievable, then lower rates are also achievable. The *maximally achievable* (or simply *maximal*) secret key rate is called the exact upper bound of the set of achievable rates. (For formal definitions, see Ref. [39].)

Note that sometimes the key rate is defined as the limit of the length of the final key to the number of pulses. Since the length of the sifted key is proportional to the number of pulses, these definitions coincide up to a constant factor.

The formula for the maximum secret key rate can be written using the Devetak–Winter theorem [39] (see also Section 6). Its formulation involves a three-particle state of the sender, the receiver, and the adversary, which emerges after the sifting procedure. Our immediate goal is to write the formula for this state.

Let us introduce a register (formally, a quantum system) $\overline{A}$ of dimension 2, which stores the bit value of the sender. We denote a subsystem that contains the transmitted quantum state (6) as A. Then, the joint state $\overline{A}$ and A when using the z basis has the form

$$\rho_{\overline{A}A}^z = \frac{1}{2} \sum_{u=0}^{1} |u\rangle_{\overline{A}} \langle u| \otimes \rho_{\mu u}^z, \quad (8)$$

where $\rho_{\mu u}^z$ is given by Eqn (6).

Due to the action of natural noise, natural losses in the channel, and/or actions by the adversary, the state $\rho_{\mu u}^z$ undergoes the action of some quantum channel, i.e., linear completely positive trace-preserving map $\Upsilon_0: \mathfrak{T}(\mathscr{H}_A) \to \mathfrak{T}(\mathscr{H}_B \otimes \mathscr{H}_E)$, where $\mathscr{H}_A = \mathscr{H}_B = \mathscr{F}(\mathbb{C}^2)$ are Hilbert spaces of the sender and the receiver. $\mathscr{H}_E$ is some (unknown) Hilbert space of the adversary, and $\mathfrak{T}$ is the space of nuclear operators in the corresponding Hilbert space.

The quantum efficiencies of the detectors (which are different in general) and the probabilities of dark counts (also, in general, different) can also be included in the channel Υ_0: in the first case, the state with photons turns, with some probability, into the state without photons, and the other way around in the second case. It should be noted that enabling these effects makes Υ_0 basis-dependent. The transformation of the state in the communication line does not depend on the basis, since the adversary does not know the basis at the time of the attack, and the natural noise and losses do not depend on the basis. But the further transformation of the state associated with the measurement is already dependent on the measurement basis. We are now interested in positions in which both sides use the z basis, since only such positions participate in the key formation. The measurement in the

x basis would correspond to another transformation, but we will not need it.

After this, an 'ideal' measurement (we have already taken into account imperfect detector efficiencies and dark counts in Υ_0) corresponds to the probability projector-valued measure $\{\bar{P}_\varnothing, \bar{P}_0, \bar{P}_1, \bar{P}_{01}\}$, where $\bar{P}_\varnothing = |\text{vac}\rangle\langle\text{vac}|$ corresponds to the no click event in both detectors, $\bar{P}_0 = \sum_{j=1}^{\infty} |j,0\rangle_z \langle j,0|$ and $\bar{P}_1 = \sum_{j=1}^{\infty} |0,j\rangle_z \langle 0,j|$ correspond to the click of exactly one detector, and $\bar{P}_{01} = \sum_{j,k=1}^{\infty} |j,k\rangle_z \langle j,k|$ corresponds to the click of both detectors.

So, the vacuum component of the receiver state is not registered. Therefore, the corresponding positions are sifted out and do not participate in the key formation. Recall that our immediate goal is to write a formula for the three-particle state of the sender, the receiver, and the adversary, which emerges after the sifting procedure. We denote

$$\Upsilon(\rho_A) = \big[(I_B - |\text{vac}\rangle\langle\text{vac}|) \otimes I_E\big]$$
$$\times\, \Upsilon_0(\rho_A)\big[(I_B - |\text{vac}\rangle\langle\text{vac}|) \otimes I_E\big]$$

for any $\rho_A \in \mathfrak{T}(\mathscr{H}_A)$. Here, I_B and I_E are the identity operations in the spaces $\mathscr{H}_B$ and $\mathscr{H}_E$, respectively. Obviously, the map Υ does not preserve the trace, it only does not increase it: $\text{Tr}\,\Upsilon(\rho_A) \leqslant \text{Tr}\,\rho_A$. The reason for the nonconservation of the trace is that Υ includes sifting, which reduces the trace.

Then, the desired formula for the three-particle state of the sender, receiver, and adversary after sifting has the form

$$\rho_{\overline{A}BE} = (Q^{sz})^{-1}(\text{Id}_{\overline{A}} \otimes \Upsilon)(\rho_{\overline{A}A}^z) = \frac{1}{2Q^{sz}}\sum_{u=0}^{1} |u\rangle_{\overline{A}}\langle u| \otimes \Upsilon(\rho_{\mu\mu}^z)\,,$$

$$(9)$$

where

$$Q^{sz} = \text{Tr}\,(\text{Id}_{\overline{A}} \otimes \Upsilon)(\rho_{\overline{A}A}^z)$$

is the probability of the registration of a signal pulse (as indicated by the superscript s, later we would need the probabilities of registration of decoy pulses), and $\text{Id}_{\overline{A}}$ is the identity quantum map of density operators in the space of register $\overline{A}$, i.e., $\mathbb{C}^2$.

According to the Devetak–Winter theorem [39], the maximal secret key rate is as follows:

$$R = H(\overline{A}|E) - H(\overline{A}|B)\,,\qquad(10)$$

where

$$H(\overline{A}|B) = H(\rho_{\overline{A}B}) - H(\rho_B)\,,$$
$$H(\overline{A}|E) = H(\rho_{\overline{A}E}) - H(\rho_E)\qquad(11)$$

are quantum conditional entropies.

Here, we have used the following convention regarding the denotations of the states of subsystems of a composite system: if the state of the composite system is $\rho_{\overline{A}BE}$, then $\rho_{\overline{A}B} = \text{Tr}_E\,\rho_{\overline{A}BE}$, $\rho_B = \text{Tr}_{\overline{A}E}\,\rho_{\overline{A}BE}$, $\rho_E = \text{Tr}_{\overline{A}B}\,\rho_{\overline{A}BE}$, etc. In turn, $H(\rho) = -\text{Tr}\,(\rho\log\rho)$ is the von Neumann entropy, $\log \equiv \log_2$. Since the state $\rho_{\overline{A}BE}$ is classical-quantum (it is classical on $\overline{A}$ and quantum on BE), both terms on the right-hand side of Eqn (10) are nonnegative.

The first term on the right-hand side of Eqn (10) characterizes the *ignorance* or the *lack of information* of the

adversary about the sender's key bit. The second term (without the minus sign before it) characterizes the ignorance (the lack of information) of the receiver about the same bit. Denote m as the minimal amount of information that the sender has to disclose about their sifted key, so that the receiver would be able to correct all errors and get a key that matches the sender's key. If error-correcting codes are used for this purpose, then m is the length of the syndrome. However, iterative error correction procedures can also be used. The second term on the right-hand side of (10) is the ratio m/n as $n \to \infty$. We assume that an optimal error correction code (in the Shannon sense) is used. Otherwise, the factor $f > 1$ has to be added before the second term. So, for example, the value of the factor $f = 1.22$ is achievable for modern error-correcting codes [49].

According to the Fano inequality, the quantity $H(\overline{A}|B)$ can be upper bounded by $h(E^{sz})$, where

$$h(x) = -x\log x - (1-x)\log(1-x)$$

is the binary entropy, and E^{sz} is the fraction of errors in the sifted keys. The superscripts s and z indicate that we are talking about signal states and positions, in which both sides used the basis z. Recall that only these positions are involved in the secret key formation. This value becomes known to the legitimate parties after error correction and key verification: After verification, the keys are likely to coincide; therefore, by the number of positions in which corrections have taken place, the legitimate parties know the error rates in the sifted keys. Then, to obtain a formula for the achievable secret key rate, the legitimate parties have to evaluate the first term on the right-hand side of Eqn (10), i.e., the adversary's ignorance. Estimation of the first term is crucial in proving the security of any QKD protocol.

5. Reducing the multiphoton case to a single-photon one

Let us reduce the problem of upper bounding $H(\overline{A}|E)$ for the state $\rho_{\overline{A}BE}$, which includes multiphoton pulses, to an estimation of the quantum conditional entropy for a state that includes only single-photon pulses. We write

$$\tilde{\rho}_{\overline{A}A}^{(0)} = \frac{1}{2}\sum_{u=0}^{1} |u\rangle_{\overline{A}}\langle u| \otimes P_0\,\rho_{\mu\mu}^z P_0$$
$$= \frac{\exp(-\mu)}{2}\sum_{u=0}^{1} |u\rangle_{\overline{A}}\langle u| \otimes |\text{vac}\rangle\langle\text{vac}|\,,$$
$$\tilde{\rho}_{\overline{A}A}^{(1)} = \frac{1}{2}\sum_{u=0}^{1} |u\rangle_{\overline{A}}\langle u| \otimes P_1\,\rho_{\mu\mu}^z P_1$$
$$= \frac{\mu\exp(-\mu)}{2}\sum_{u=0}^{1} |u\rangle_{\overline{A}}\langle u| \otimes |u\rangle_z\langle u|\,,$$
$$\rho_{\overline{A}BE}^{(\geqslant 2)} = (Q_{(\geqslant 2)}^{sz})^{-1}(\text{Id}_{\overline{A}} \otimes \Upsilon)(\tilde{\rho}_{\overline{A}A}^{(\geqslant 2)})\,,$$
$$Q_j^{sz} = \text{Tr}\,(\text{Id}_{\overline{A}} \otimes \Upsilon)(\tilde{\rho}_{\overline{A}A}^{(j)})\,,\quad j = 0,1\,,$$

where P_j is the projection onto the j-photon subspace in $\mathscr{F}(\mathbb{C}^2)$ (see Eqn (7)), and Q_j^{sz} is the joint probability that the sender's signal pulse contains exactly j photons and is registered by the receiver. Then, the ratio of the j-photon pulses to the pulses registered by the receiver and participating in the formation of the sifted key is Q_j^{sz}/Q^{sz}.

Theorem. *For any linear completely positive trace-non-increasing map* Υ, *the following inequality holds:*

$$H(\overline{A}|E) \geqslant \frac{Q_0^{sz}}{Q^{sz}} + \frac{Q_1^{sz}}{Q^{sz}} H(\overline{A}|E)_{(1)}, \qquad (12)$$

where $H(\overline{A}|E)$ *is calculated for state* $\rho_{\overline{A}BE}$ *and* $H(\overline{A}|E)_{(1)}$ *is calculated for state* $\rho_{\overline{A}BE}^{(1)}$.

Quantum conditional entropy can be expressed in terms of the quantum relative entropy:

$$H(\overline{A}|E) = -D(\rho_{\overline{A}E}\|I_{\overline{A}} \otimes \rho_E).$$

Recall that the quantum relative entropy is defined as

$$D(\rho\|\sigma) = \mathrm{Tr}\,(\rho\log\rho) - \mathrm{Tr}\,(\rho\log\sigma),$$

and it is jointly convex with respect to its arguments [53, 54]

$$D\big(p\rho_1 + (1-p)\rho_2 \,\big\|\, p\sigma_1 + (1-p)\sigma_2\big)$$
$$\leqslant pD(\rho_1\|\sigma_1) + (1-p)D(\rho_2\|\sigma_2)$$

for any states $\rho_{1,2}$, $\sigma_{1,2}$ and $0 \leqslant p \leqslant 1$.

Then, the statement of this theorem is a simple consequence of the fact that the state $\rho_{\mu u}^z$ is a mixture of states with a certain number of photons (6), linearity of Υ, and joint convexity of the quantum relative entropy. Indeed,

$$\rho_{\mu u}^z = P_0\,\rho_{\mu u}^z P_0 + P_1\,\rho_{\mu u}^z P_1 + P_{\geqslant 2}\,\rho_{\mu u}^z P_{\geqslant 2},$$

where $P_{\geqslant 2} = \sum_{j=2}^{\infty} P_j$. Therefore, in view of the linearity of Υ,

$$\rho_{\overline{A}BE} = (Q^{sz})^{-1}(\mathrm{Id}_{\overline{A}} \otimes \Upsilon)(\rho_{\overline{A}A})$$
$$= \frac{Q_0^{sz}}{Q^{sz}}\rho_{\overline{A}BE}^{(0)} + \frac{Q_1^{sz}}{Q^{sz}}\rho_{\overline{A}BE}^{(1)} + \frac{Q_{\geqslant 2}^{sz}}{Q^{sz}}\rho_{\overline{A}BE}^{(\geqslant 2)},$$

where

$$\rho_{\overline{A}BE}^{(\geqslant 2)} = (Q_{\geqslant 2}^{sz})^{-1}\,\mathrm{Tr}\,(\mathrm{Id}_{\overline{A}} \otimes \Upsilon)(\tilde{\rho}_{\overline{A}A}^{(\geqslant 2)}),$$
$$Q_{\geqslant 2}^{sz} = \mathrm{Tr}\,(\mathrm{Id}_{\overline{A}} \otimes \Upsilon)(\tilde{\rho}_{\overline{A}A}^{(\geqslant 2)}),$$
$$\tilde{\rho}_{\overline{A}A}^{(\geqslant 2)} = \frac{1}{2}\sum_{u=0}^{1} |u\rangle_{\overline{A}} \langle u| \otimes P_{\geqslant 2}\,\rho_{\mu u}^z P_{\geqslant 2}.$$

Then, due to the joint convexity of the quantum relative entropy,

$$H(\overline{A}|E) \geqslant \frac{Q_0^{sz}}{Q^{sz}} H(\overline{A}|E)_{(0)} + \frac{Q_1^{sz}}{Q^{sz}} H(\overline{A}|E)_{(1)}$$
$$+ \frac{Q_{\geqslant 2}^{sz}}{Q^{sz}} H(\overline{A}|E)_{(\geqslant 2)} \geqslant \frac{Q_0^{sz}}{Q^{sz}} + \frac{Q_1^{sz}}{Q^{sz}} H(\overline{A}|E)_{(1)},$$

Q.E.D. Here, conditional entropies $H(\overline{A}|E)_{(0)}$ and $H(\overline{A}|E)_{(\geqslant 2)}$ are calculated for the states $\rho_{\overline{A}BE}^{(0)}$ and $\rho_{\overline{A}BE}^{(\geqslant 2)}$, respectively. They are nonnegative, because these states are classical-quantum. We have also used here the fact that $H(\overline{A}|E)_{(0)} = H(\overline{A}) = 1$, which follows from the form of the states $\tilde{\rho}_{\overline{A}A}^{(0)}$ and $\tilde{\rho}_{\overline{A}BE}^{(0)}$. Informally, the vacuum contains no information about the sent bit.

The theorem proves that the decoy state method is universal, i.e., secure against arbitrary attacks (for arbitrary maps Υ), and not only against the photon-number splitting attack. More precisely, the theorem claims the universality of the lower bound (12), whereas the decoy state method provides lower bounds for Q_0^{sz} and Q_1^{sz}, as well as bounds for quantities participating in the estimation of $H(\overline{A}|E)_{(1)}$.

Estimate (12) becomes exact in the case of the photon-number splitting attack, since this attack is optimal. Indeed, this attack provides knowledge of all the bits that are encoded in multiphoton pulses to the adversary, which is the basic assumption of this estimate.

Is it always possible to perform a photon-splitting attack? The removal of a photon from a multiphoton signal by the adversary reduces the registration probability of this signal, that is, increases the level of losses. As mentioned above, the adversary can compensate for this by reducing the level of natural losses in the communication channel or even in the optical scheme of the receiving side. However, if the natural losses are so small that even their reduction to zero does not compensate for the losses introduced due to the removal of photons from multiphoton signals, then the adversary cannot perform a full photon-number splitting attack. Therefore, estimate (12) ceases to be precise (but, of course, remains true): $H(\overline{A}|E)_{(\geqslant 2)} > 0$. Nevertheless, at realistic losses, the adversary can perform a photon-number splitting attack, and estimate (12) is precise.

Let us now pay attention to the first term of the right-hand side of Eqn (12). It is related to the registration of a vacuum pulse. The registration of a vacuum pulse can occur due to the actions of the adversary, who can send their signal to the receiver. It can also happen due to a dark count in the receiver's detectors. However, if key distribution is possible, the fraction of dark counts in the total number of counts (i.e., the ratio Q_0^{sz}/Q^{sz}) is small. Key distribution is only possible with a relatively low error rate. The well-known theoretical maximal tolerable error rate for the BB84 protocol is 11% (under the assumption that the error rate is the same for both bases (see Remark 2 below)) [11, 12, 18]. In practice, the maximal tolerable error rate is even lower due to the presence of multiphoton pulses and due to statistical fluctuations. Since a dark count is erroneous with a probability of 1/2, this means that the fraction of dark counts in the total number of counts on the receiver side does not exceed 6%. For this reason, instead of an accurate estimate (12), a rougher estimate is often used:

$$H(\overline{A}|E) \geqslant \frac{Q_1^{sz}}{Q^{sz}} H(\overline{A}|E)_{(1)}. \qquad (13)$$

We emphasize that the fraction of dark counts affects the closeness of estimate (13) to the exact estimate (12), but not on the validity of Eqn (13), which follows directly from Eqn (12) and the positivity of values Q_0^{sz} and Q^{sz}. This means that Eqn (13) allows secret key generation at any dark count rate, but at a slightly lower speed than is allowed by formula (12).

In what follows, in the decoy state method, dark counts are strictly taken into account in the value Y_0 (see Eqns (22)–(24) in Section 7). At realistic communication channel lengths and without eavesdropping, i.e., during the 'normal' operation of the system, the dark counts (rather than, for example, errors due to inaccurate alignment of the optical scheme) make the main contribution to the error rate.

Remark 1. Here, the requirement of phase randomization (6) is crucial. As mentioned above, it can be achieved in two ways: at the hardware level, when a laser emits a pulse with a

random phase, independent of the phases of previous impulses, or using active randomization, i.e., with the use of a device connected to a random number generator for the random choice of the phases of outgoing pulses. In the latter case, randomization according to a uniform or another continuous distribution is not possible: only a discrete approximation is possible; therefore, it is necessary to take into account the corresponding correction [55].

The Devetak–Winter formula (10) for the maximal secret key rate was initially obtained for the case of a so-called collective attack. Keep in mind that attacks on quantum cryptography protocols are divided (by increasing degree of generality) into individual, collective, and coherent [18]. In a collective attack, it is assumed that the adversary attacks all the transmitted states in the same way, so that, after sending n pulses, the state $\rho_{\overline{\mathbf{ABE}}}^{\otimes n}$ is formed (see Eqn (9)). Then, the adversary performs a collective (i.e., of the general form) measurement over their own parts.

In the most general case, the adversary performs an arbitrary quantum transformation over n pulses, which is not necessarily a tensor power of the transformation over one pulse. These attacks are called coherent attacks. In the asymptotic case $n \to \infty$, which we restrict ourselves to in this paper, the consideration of coherent attacks is reduced to the consideration of collective attacks using the de Finetti quantum representation [14]. Therefore, formally, the use of the Devetak–Winter formula is not a limitation. However, the corrections associated with the finiteness of n, when using the de Finetti representation, turn out to be large enough for realistic n; therefore, in practice, the de Finetti representation is usually not used. Let us explain why the consideration of the photon-number splitting attack does not limit the generality in this case either.

For n pulses, instead of state (8), we now have the state

$$\rho_{\overline{\mathbf{A}}\mathbf{A}}^z = \frac{1}{2^n} \sum_{\mathbf{u} \in \{0,1\}^n} |\mathbf{u}\rangle_{\overline{\mathbf{A}}} \langle \mathbf{u}| \otimes \rho_{\mu\mathbf{u}}^z \,, \tag{14}$$

where $\mathbf{u} = u_1, \ldots, u_n$ is a binary string, $|\mathbf{u}\rangle = |u_1\rangle \otimes \ldots \otimes |u_n\rangle$,

$$\rho_{\mu\mathbf{u}}^z = \rho_{\mu u_1}^z \otimes \ldots \otimes \rho_{\mu u_n}^z \,,$$

and bold marking of the registers ($\overline{\mathbf{A}}, \mathbf{A}$) means that registers are 'vectors'.

Since

$$\rho_{\mu u}^z = \sum_{j=0}^{\infty} P_j \rho_{\mu u}^z P_j \,,$$

it can be stated that

$$\rho_{\mu\mathbf{u}}^z = \sum_{j_1=0}^{\infty} \ldots \sum_{j_n=0}^{\infty} (P_{j_1} \rho_{\mu u_1}^z P_{j_1}) \otimes \ldots \otimes (P_{j_n} \rho_{\mu u_n}^z P_{j_n}) \,. \tag{15}$$

Each term on the right-hand side of Eqn (15) represents a state (up to normalization) with a certain number of photons in each position. Since transformations of quantum states are linear (or affine) maps, any state transformation (15) is a convex sum of the results of state transformations with a certain number of photons in each pulse. Therefore, the consideration of only such states does not limit the generality. Measurements of the number of photons in each pulse in a photon-number splitting attack do not change the state (15) (since it already has a diagonal form with respect to the operators $P_{j_1} \otimes \ldots \otimes P_{j_n}$), but simply allow the adversary to find out the number of photons in each pulse. In this sense, the photon-number splitting attack is optimal: if each pulse has a certain number of photons and one can find out this number without introducing noise, then it is optimal to do this, that is, to measure the number of photons in each pulse.

A rigorous estimate of the entropy characterizing the ignorance of the adversary for a state of form (15) for a finite n was performed in Ref. [56]. The purpose of this consideration was to justify the fact that the consideration of states with a certain number of photons in each pulse does not limit the generality.

6. Formulation in terms of entangled states

For the generalization of the Devetak–Winter results for the case of coherent attacks, one can use the entropy accumulation technique [17]. It consists of estimating the smoothed Renyi min-entropy for a state in $(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_E)^{\otimes n}$ (which is necessary to estimate the ignorance of the adversary during a coherent attack) through the von Neumann entropy, which is the first term on the right-hand side of the Devetak–Winter formula (10). Therefore, if it is possible to apply this technique, the Devetak–Winter formula gives the maximally achievable secret key rate in the case of coherent (i.e., general) attacks. Also, the entropy accumulation technique makes it possible to take into account the effects associated with the finite size of the statistical sample (finite number n), which is outside the scope of this work: recall that we are working in the limit of infinitely large n.

In Ref. [17], this technique was used to prove the Devetak–Winter formula for the BB84 protocol with a single-photon source in the case of general attacks. However, it uses an equivalent entangled state representation of the BB84 protocol. Therefore, the purpose of this section is to formulate the BB84 protocol with phase-randomized coherent states in terms of an entangled state.

Recall that $\mathscr{H}_A$ denotes the Hilbert space, corresponding to a quantum information carrier: $\mathbb{C}^2$ in the single-photon case and $\mathscr{F}(\mathbb{C}^2)$ in the general case. $\overline{A}$ denotes a binary register which stores the sender's bit value. Let us introduce yet another Hilbert space $\mathscr{H}_{\widetilde{A}}$, which is related to the sender. In the BB84 protocol, the sender transmits the states $\rho_{\mu u}^b \in \mathfrak{T}(\mathscr{H}_A)$, $b \in \{z, x\}$, $u \in \{0, 1\}$ of the form (6) with the probabilities $p_b/2$. To define the protocol in terms of entangled states, let us assume that an entangled state $\rho \in \mathfrak{T}(\mathscr{H}_{\widetilde{A}} \otimes \mathscr{H}_A)$ of the composite system $\mathscr{H}_{\widetilde{A}} \otimes \mathscr{H}_A$ is generated on the sender side. The sender measures subsystem $\widetilde{A}$, whereas subsystem A, as previously, is sent to the receiver via the communication channel. Let the sender's observation of subsystem $\widetilde{A}$ be given by the probability projector-valued measure $\Pi = \{\Pi_{ub}\}_{u \in \{0,1\}, b \in \{z,x\}}$ in the space $\mathscr{H}_{\widetilde{A}}$. We require the fulfilment of the following conditions,

$$\mathrm{Tr}_{\widetilde{A}} (\Pi_{ub} \rho \Pi_{ub}) = \frac{p_b}{2} \rho_{\mu u}^b \,, \tag{16}$$

for all u and b, where $\mathrm{Tr}_{\widetilde{A}}$ is the partial trace in the space $\mathscr{H}_{\widetilde{A}}$. Then, the sender can prepare the states $\rho_{\mu u}^b$ with the corresponding probabilities by measuring the observable Π of the subsystem $\widetilde{A}$, so that we obtain a mathematically equivalent scheme of the protocol. For its security, the state ρ must be entangled; the title of this scheme of the protocol comes from this fact. If, in reality, an entangled state is not

generated and the sender does not measure one of the subsystems of an entangled state, then the system $\mathscr{H}_{\widetilde{A}}$ and the measurement in it are 'fictitious', so they are used only for a mathematically equivalent formulation.

In the single-photon case (when $\mathscr{H}_A = \mathbb{C}^2$ and the states $\rho_{\mu u}^b$ contain the single-photon component only), one can take $\mathscr{H}_{\widetilde{A}} = \mathbb{C}^2$, $\rho = |\Phi\rangle\langle\Phi|$, where

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle_z \otimes |1,0\rangle_z + |0,1\rangle_z \otimes |0,1\rangle_z\right)$$

$$= \frac{1}{\sqrt{2}}\left(|1,0\rangle_x \otimes |1,0\rangle_x + |0,1\rangle_x \otimes |0,1\rangle_x\right) \in \mathbb{C}^2 \otimes \mathbb{C}^2 \quad (17)$$

and $\Pi_{ub} = p_b|u\rangle_b\langle u|$. The security of this protocol, which is based on the entangled state $|\Phi\rangle$, is proved in Ref. [17] using the entropy accumulation technique. In this case, in the result of the measurement of the observable Π, $\widetilde{A}$ stores the sender's bit value. So, register $\widetilde{A}$ can be identified with $\overline{A}$. However, generally speaking, they are not identical.

In order to extend the results of Ref. [17] for the multiphoton case, one needs to present the protocol scheme in terms of an entangled state in such a way that the projection onto the single-photon subspace followed by the normalization again gives state (17) and observable $\{p_b|u\rangle_b\langle u|\}$. State (17) cannot be directly generalized to the multiphoton case, since

$$\frac{1}{\sqrt{2}}\left(|j,0\rangle_z \otimes |j,0\rangle_z + |0,j\rangle_z \otimes |0,j\rangle_z\right)$$

$$\neq \frac{1}{\sqrt{2}}\left(|j,0\rangle_x \otimes |j,0\rangle_x + |0,j\rangle_x \otimes |0,j\rangle_x\right)$$

if $j \geqslant 2$.

Let us extend the space $\mathscr{H}_{\widetilde{A}}$: let $\mathscr{H}_{\widetilde{A}} = \mathbb{C}^2 \oplus \mathbb{C}^4$. We will still use $\{|0\rangle_z, |1\rangle_z\}$ and $\{|0\rangle_x, |1\rangle_x\}$ as the bases for the space $\mathbb{C}^2$: each element of the basis marks the sender's bit. Take new vectors $\{|0z\rangle, |1z\rangle, |0x\rangle, |1x\rangle\}$ as the basis for the space $\mathbb{C}^4$. Each vector marks the bit and the basis (in $\mathbb{C}^2$), which is used by the sender. An equivalent entanglement-based representation of the protocol can be constructed using the states

$$\rho = \mu \exp(-\mu)|\Phi\rangle\langle\Phi| + \sum_{u\in\{0,1\}} \sum_{b\in\{z,x\}} p_b \exp(-\mu)|ub\rangle\langle ub|$$

$$\otimes \left(|\mathrm{vac}\rangle\langle\mathrm{vac}| + \sum_{j=2}^{\infty} \frac{\mu^j}{j!}|\psi_{ju}^b\rangle\langle\psi_{ju}^b|\right) \quad (18)$$

and the observable Π, where $\Pi_{ub} = p_b|u\rangle_b\langle u| + |ub\rangle\langle ub|$. The projection onto the single-photon component (see (7)) followed by the normalization to unity turns the state ρ into the projector on $|\Phi\rangle$. Then, only the second term in expression Π_{ub} remains relevant, so this reproduces the previous observable. In state (18), entanglement takes place only in the single-photon component. There is no need to build a state in which entanglement is also contained in multiphoton pulses, since multiphoton pulses are considered insecure in any case, and there is no need to make them secure.

Thus, a combination of theorem, which reduces the estimation of adversary's ignorance in terms of the von Neumann entropy to the estimation of the corresponding entropy for states with single-photon pulses, and the estimate of the latter in Ref. [17] allows using the entropy accumula-

tion technique for the BB84 protocol with the source of coherent states concluding that the Devetak–Winter formula gives the maximally achievable key rate without assumptions about the class of adversary attacks.

7. Decoy state method

As follows from Eqn (13), the problem of obtaining achievable key rates (10) in the case of arbitrary collective attacks in the space $\mathscr{F}(\mathbb{C}^2)$ splits into two subproblems: the estimation of the factor Q_1^{sz}/Q^{sz}, i.e., the fraction of the position in the sifted key obtained from the single-photon pulses, and the estimation of the adversary's ignorance $H(\overline{A}|E)_{(1)}$ about a single bit of this part of the key.

The expression for $H(\overline{A}|E)_{(1)}$ is well known [12, 13, 17] and has the form

$$H(\overline{A}|E)_{(1)} = 1 - h(e_1^x), \quad (19)$$

where e_1^x is the probability of bit error in the single-photon states conditioned on the use of the x basis by both parties. Therefore, the expression for the maximally achievable key rate takes the form

$$R = \frac{Q_1^{sz}}{Q^{sz}}\left[1 - h(e_1^x)\right] - h(E^{sz}). \quad (20)$$

Remark 2. Keep in mind that, in the described variant of the BB84 protocol, the basis x is rarely used. But the probability e_1^x is estimated only for those few positions in which both sides have chosen the x basis. Using Eqn (20), let us comment on the threshold error rate at which key distribution is possible, i.e., $R > 0$. For simplicity, we assume that all the states are single photon, i.e., $Q_1^{sz} = Q^{sz}$. If the error rate does not depend on the basis, i.e., $e_1^x = E^{sz} = e$, then the key distribution is possible if $1 - 2h(e) > 0$, i.e., if $e < e_{\mathrm{crit}} \approx 0.11$. However, in a theoretically possible situation of various e_1^x and E^{sz}, the statement on the critical error rate of 11%, generally speaking, is not true anymore. For example, if $E^{sz} = 0$, then the critical error rate for e_1^x increases to 50%. By analogy, if $e_1^x = 0$, then the critical error rate for E^{sz} increases to 50% as well.

The decoy state method allows estimating the factor Q_1^{sz}/Q^{sz}, as well as the value of e_1^x, in an efficient manner. The general idea is that, in some positions randomly selected and not known in advance, the sender transmits not the signal pulses (i.e., used to form a key) with an intensity μ (see Eqn (5)), but decoy pulses with lower intensities. The positions in which the decoy pulses are used do not participate in the key formation. After the end of the transfer of quantum states, at the stage of announcements, the sender announces the intensities used in each message. Based on this information, the legitimate parties calculate the statistics for each intensity and then compare the results for states of different intensities. Informally speaking, the idea of the method is that the adversary measuring the number of photons does not know the intensity of a given pulse. Therefore, the adversary does not have the ability to deal differently with the signal and decoy states with the same number of photons (which, on the contrary, the adversary is supposed to know). If the adversary blocks all single-photon components, they block almost all low-intensity decoy states that would be noticeable on the receiver side. Formally, this leads to a zero key rate, which corresponds to the detection of eavesdropping.

The most common decoy state method, which we will describe, is based on one signal and two decoy states. We use notations that are similar to the ones from Refs [29, 32]. We also assume that the efficiencies and dark count probabilities of the detectors are the same. In the opposite case, Eqn (19) should be corrected (see Ref. [20], in which an adaptation of the decoy state method for the case of detection-efficiency mismatch is discussed in detail). If the efficiencies and dark count probabilities are identical, index z of the values Q_1^{sz} and Q^{sz} can be removed: detection probabilities do not depend on the basis.

Let Y_i be the probability that one of the detectors on the receiving side clicks provided that, on the sender's side, the transmitted state contained i photons. This probability does not depend on the intensity of the pulse (it depends only on the number of photons in it, i.e., i), but it can depend both on the attenuation in the channel and on the actions of the adversary, which can block some of the states or, on the contrary, send them to the receiving side without attenuation. Note that Y_0 is nonzero and is equal to the probability of the dark count in at least one of the detectors.

Q_i^v is the probability that the transmitted state contains i photons, and one of the detectors on the receiving side clicks provided that the sender used a type $v \in \{s, d_1, d_2\}$ state (signal or one of two decoys). Let us denote the intensity of the signal pulse $\mu_s = \mu$. The intensities of decoy pulses are $\mu_{d_1} = v_1$, $\mu_{d_2} = v_2$, and we require that

$$0 \leqslant v_2 < v_1, \quad v_1 + v_2 < \mu. \tag{21}$$

Since the probability that the pulse contains exactly i photons (under the condition of pulse intensity μ), equal to $\exp(-\mu)\,\mu^i/i!$, then

$$Q_i^v = \exp(-\mu_v)\,\frac{\mu_v^i}{i!}\,Y_i. \tag{22}$$

The probability of a click in at least one of the detectors on the receiving side provided that the pulse is a v type is

$$Q^v = \sum_{i=0}^{\infty} Q_i^v = \sum_{i=0}^{\infty} \exp(-\mu_v)\,\frac{\mu_v^i}{i!}\,Y_i. \tag{23}$$

Quantities Q^v become known to the legitimate parties at the stage of announcements (more precisely, their estimates, but in the limit of an infinite number of messages, they coincide with the true values). They can be used to estimate the unknown quantity Y_1 and, consequently, quantity Q_1^s that appears in Eqn (13).

First, from the chain of inequalities

$$v_1 Q^{d_2} \exp v_2 - v_2 Q^{d_1} \exp v_1$$
$$= (v_1 - v_2) Y_0 - v_1 v_2 \sum_{i=2}^{\infty} (v_1^{i-1} - v_2^{i-1})\frac{Y_i}{i!} \leqslant (v_1 - v_2) Y_0$$

we obtain the lower bound for Y_0:

$$Y_0 \geqslant Y_0^L = \max\left\{\frac{v_1 Q^{d_2} \exp v_2 - v_2 Q^{d_1} \exp v_1}{v_1 - v_2},\, 0\right\}. \tag{24}$$

This inequality gives an estimate of the probability of dark counts in at least one of the detectors of the receiving side, which is supposed to be unknown to legitimate users in advance and may be controlled by the adversary.

The estimate for Y_1 comes from the chain of inequalities

$$Q^{d_1} \exp v_1 - Q^{d_2} \exp v_2 = (v_1 - v_2) Y_1 + \sum_{i=2}^{\infty}(v_1^i - v_2^i)\frac{Y_i}{i!}$$

$$\leqslant (v_1 - v_2) Y_1 + \frac{v_1^2 - v_2^2}{\mu^2}\sum_{i=2}^{\infty}\frac{\mu^i}{i!}\,Y_i$$

$$= (v_1 - v_2) Y_1 + \frac{v_1^2 - v_2^2}{\mu^2}\left(Q^s \exp \mu - Y_0 - Y_1\mu\right)$$

$$\leqslant (v_1 - v_2) Y_1 + \frac{v_1^2 - v_2^2}{\mu^2}\left(Q^s \exp \mu - Y_0^L - Y_1\mu\right). \tag{25}$$

The first inequality of this chain uses conditions (21) as well as the inequality $a^i - b^i \leqslant a^2 - b^2$ for $0 < a + b < 1$ and $i > 2$. Hence,

$$Y_1 \geqslant Y_1^L = \frac{\mu}{\mu(v_1 - v_2) - (v_1^2 - v_2^2)}$$
$$\times \left[Q^{d_1} \exp v_1 - Q^{d_2} \exp v_2 - \frac{v_1^2 - v_2^2}{\mu^2}(Q^s \exp \mu - Y_0^L)\right], \tag{26}$$

$$Q_1^s \geqslant Q_1^{sL} = \mu \exp(-\mu) Y_1^L. \tag{27}$$

Then, we denote by e_i^x the probability of bit error in the i-photon state provided that both parties used the x basis. Let us estimate the probability of e_1^x participating in Eqn (19). This probability can include both imperfections of the devices and eavesdropping. The error probability E^{vx}, provided that the pulse is a v type and the x basis is used by both parties, is

$$E^{vx}Q^v = \sum_{i=0}^{\infty} e_i^x Y_i \frac{\mu_v^i}{i!} \exp(-\mu). $$

Then, from the inequality

$$E^{d_1 x}Q^{d_1} \exp v_1 - E^{d_2 x}Q^{d_2} \exp v_2 = e_1^x(v_1 - v_2) Y_1$$
$$+ \sum_{i=2}^{\infty} e_i^x(v_1^i - v_2^i)\frac{Y_i}{i!} \geqslant e_1^x(v_1 - v_2) Y_1 \geqslant e_1^x(v_1 - v_2) Y_1^L$$

we obtain an upper bound on e_1^x:

$$e_1^x \leqslant e_1^{xU} = \frac{E^{d_1 x}Q^{d_1} \exp v_1 - E^{d_2 x}Q^{d_2} \exp v_2}{(v_1 - v_2) Y_1^L}. \tag{28}$$

The substitution of the obtained estimates into Eqns (13) and (19) yields the formula for the achievable secret key rate:

$$R = \frac{Q_1^{sL}}{Q^s}\left[1 - h(e_1^{xU})\right] - h(E^{sz}). \tag{29}$$

In the absence of eavesdropping, the exact values of all quantities that participate in the definition of the key rate take the form (see Eqn (5)–(11) in Ref. [29])
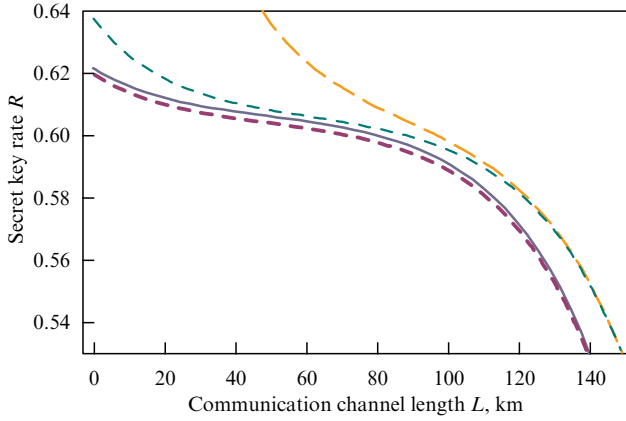
$$Q^s = p_d + 1 - \exp\left[-\eta\mu T(L)\right], \tag{30}$$

$$Y_1 = p_d + \eta T(L), \tag{31}$$

$$Q_1^s = \left[p_d + \eta T(L)\right]\mu \exp(-\mu), \tag{32}$$

$$E^{sz} = \frac{p_d}{2}, \tag{33}$$

$$e_1^x = \frac{p_d}{2Y_1}, \tag{34}$$

Figure. (Color online.) Secret key rate depending on the communication channel length. Solid blue line: calculation for a photon-number splitting attack with a coherent attack on one-photon states by Eqn (20). Dashed purple line: calculation for the same attack using Eqn (29). In this formula, instead of, generally speaking, unknown values of Q_1^μ and e_1, their lower and upper estimations are used, respectively (formulas (27) and (28) with formulas (30) and (33) for values of the observed statistics of registrations). Dashed green line: calculation for a beam splitting attack (Eqn (37) with $t = \eta T(L)$). Dashed orange line: calculation for a beam splitting attack in which the adversary does not change the efficiency of detectors on the receiver side (Eqn (37) with $t = T(L)$). Parameters: intensities of signal and decoy states are $\mu = 0.5$, $v_1 = 0.01$, $v_2 = 0.001$, dark count probability is $p_d = 10^{-6}$, quantum efficiency of each single-photon detector is $\eta = 0.1$, specific loss factor in the communication channel is $\delta = 0.2$ dB km^{-1}.

where p_d is the probability of a dark count of at least one of the detectors, $T(L) = 10^{-\delta L/10}$ is the transmission coefficient in a channel of length L, δ is the specific loss factor, and η is the quantum efficiency of each single-photon detector. We assume that errors occur only due to dark counts, and the optical part is perfectly tuned.

It is possible to consider the dependence of the key length on the length of the communication line with realistic parameters on the receiving side: the intensity of the signal and decoy states $\mu = 0.5$, $v_1 = 0.01$, $v_2 = 0.001$, $p_d = 10^{-6}$, $\eta = 0.1$, $\delta = 0.2$ dB km^{-1}. In the figure, the plot of R, which is calculated using Eqns (20) and (29), as a function of the communication channel length is presented. In both cases, the observed statistics of Q^μ, Q^{v_1}, Q^{v_2}, E^μ, E^{v_1}, and E^{v_2} are calculated using Eqns (30) and (33), i.e., for the case of the absence of eavesdropping.

In Ref. [29] it is shown that at $v_1, v_2 \to 0$, and without eavesdropping (or when the eavesdropping does not change the registration statistics), the estimates $Q_1^{\mu, L}$ and e_1^U become exact, i.e., they tend to the values of Q_1^μ and e_1, which are defined by formulas (32) and (34). Then, in the asymptotic case, the key rate is defined by Eqn (20), where Q^μ, Q_1^μ, and e_1 are defined by formulae (30)–(34).

Remark 3. It is important to note that estimates (26)–(28) do not rely on knowledge of the transmission coefficient of the channel $T(L)$, dark count probability p_d, detector efficiencies η, or other parameters of the optical and detection system of the receiving side. In the derivation of these estimates, it is not assumed that these coefficients are the same for all pulses. Thus, in fact, the decoy state method provides security even when the adversary can change these parameters. This is explained in detail, for example, in Ref. [20]. Thus, we assume that the adversary can reduce natural losses and natural errors in the communication channel and

even in the detectors up to creating a communication line and detectors without losses and errors. This gives the adversary certain freedom in creating the desired statistics of registration of states with different intensities on the receiving side.

8. Beam splitting attack

As was noted in Section 5, at the practical level of losses in the channel, estimates (12) and, therefore, (20) become exact when the adversary performs a photon-number splitting attack. However, this attack has not yet been implemented in practice. Let us compare this attack with the simpler beam splitting attack, which is also often considered in quantum cryptography [18, 57–59].

A simple version of the attack consists of the fact that the adversary, with the use of a beam splitter, takes away the part of the signal (a coherent state) that is absorbed in the channel as a result of natural losses. The adversary transmits the rest of the signal to the receiver via an ideal channel, i.e., a lossless channel. As a result, this attack does not change the statistics of the receiver state registrations in comparison with the natural conditions (in the absence of an adversary).

From the formal point of view, the attack is described by the isometry $V_{BS}: \mathscr{F}(\mathbb{C}^2) \to \mathscr{F}(\mathbb{C}^2) \otimes \mathscr{F}(\mathbb{C}^2)$, for the determination of which it is enough to specify its action on all possible coherent states (5):

$$V_{BS}|\alpha, u\rangle_b = \left|\sqrt{t}\,\alpha, u\right\rangle_b \otimes \left|\sqrt{1-t}\,\alpha, u\right\rangle_b, \tag{35}$$

where t and $1 - t$ are transmittance and refractive indices, respectively. The first space in the tensor product of V_{BS} output is interpreted as the receiver's space, while the second is the adversary's space. The composition of the map

$$\rho_{\mu u}^z \mapsto V_{BS}\,\rho_{\mu u}^z\,V_{BS}^\dagger, \tag{36}$$

describing the eavesdropping, with a map describing the measurement on the receiver side gives channel Υ_0 (see Section 5), which corresponds to this attack. In any case, since, after map (36), the state of the adversary does not undergo changes anymore, map (36) is enough to determine the state $\rho_{\overline{A}E}$ and, therefore, define entropy $H(\overline{A}|E)$ in Eqn (10):

$$\rho_{\overline{A}E} = \frac{1}{2}\sum_{u=0}^{1}|u\rangle_{\overline{A}}\langle u| \otimes \mathrm{Tr}_{\overline{B}}\left(V_{BS}\,\rho_{\mu u}^z\,V_{BS}^\dagger\right)$$

$$= \frac{\exp(-\mu_E)}{2}\sum_{u=0}^{1}|u\rangle_{\overline{A}}\langle u|$$

$$\otimes\left[|vac\rangle\langle vac| + \sum_{j=1}^{\infty}\frac{\mu_E^j}{j!}\,|\psi_{j\mu_E}^z\rangle_E\langle\psi_{j\mu_E}^z|\right]$$

$$= \frac{\exp(-\mu_E)}{2}\,I_{\overline{A}} \otimes |vac\rangle\langle vac| + \frac{\exp(-\mu_E)}{2}\sum_{u=0}^{1}|u\rangle_{\overline{A}}\langle u|$$

$$\otimes\sum_{j=1}^{\infty}\frac{\mu_E^j}{j!}\,|\psi_{j\mu_E}^z\rangle_E\langle\psi_{j\mu_E}^z|,$$

where $\mu_E = (1 - t)\mu$, $u \in \{0, 1\}$. We see that the adversary has zero information about the key bit (accordingly, the ignorance is equal to one) if the vacuum component is actualized (with probability $\exp(-\mu_E)$). Otherwise, the adversary has

complete information about the key bit. Since state (35) has the form of a tensor product, the realization of the adversary's vacuum component does not depend on the photon registration event on the receiver's side. Therefore, the probability of the vacuum component being conditioned on a click of a receiver's detector is equal to the unconditional probability of this event. Therefore, $H(\overline{A}|E) = \exp\left[-(1-t)\mu\right]$ and

$$R_{\mathrm{BS}} = \exp\left[-(1-t)\mu\right] - h(E^{\mathrm{s}z}). \tag{37}$$

In the absence of eavesdropping, the actual transmission coefficient of the entire optical system (communication line and detectors) is $\eta T(L)$. If we assume that the portion of the signal absorbed in the channel and on the detectors goes entirely to the adversary, then $t = \eta T(L)$ should be set. This is usually explained as follows: we assume that the adversary can replace the communication line and detectors with ideal ones (i.e., without losses) and, due to this, take away a share of the signal $1 - \eta T(L)$ reproducing the natural level of losses. If we assume that the adversary can replace the communication line with an ideal one, but has no power over the efficiency of the detectors η, then we can put $t = T(L)$, which reduces the adversary's information about the key and allows the legitimate parties to generate the key at a higher rate, under this assumption about the adversary.

In review [18], the feasibility of the assumption about the ability of the adversary to replace the channel with a noiseless one is discussed. It is noted that all existing solutions have fundamental limitations on the minimal loss factor. There are hypothetical solutions that are theoretically capable of providing a lossless channel, but this review concludes that they are unrealistic in any foreseeable future. However, quantum cryptography often assumes unrealistically large adversary capabilities in order to fundamentally resolve the issue of secure key distribution. So, for example, even if the adversary cannot create a lossless communication line, they can create a communication line with a lower level of losses. It can also affect the efficiency of detectors within certain limits. In order not to discuss the issues of what these limits may be, one can make the weakest assumption about the complete control of the adversary over the transmission coefficient of the line and the effectiveness of the detectors. But, let us recall, here we are considering the case of identical detector efficiencies, i.e., we are assuming that the adversary can only change the efficiency of all detectors by the same amount.

Plots of R_{BS} for $t = \eta T(L)$ and $t = T(L)$ are presented in the figure. By comparing them with the calculated achievable rates (20) and (29), one can conclude that R_{BS} is higher for the calculated achievable rates. This was expected, since a beam splitting attack is a particular type of attack, while formulas (20) and (29) are derived for the general case. In view of the importance of the beam splitting attack, in the next section, we consider why the beam splitting attack is less effective than the photon-number splitting attack.

By comparing plots R_{BS} for $t = \eta T(L)$ and $t = T(L)$, we see that, if the length is small, so that the main contribution to the losses comes from the detectors, then the possibility of the adversary diverting a larger portion of the signal by increasing the efficiency of the detectors greatly reduces the achievable key rate and brings it closer to the achievable key rate for the photon-number splitting attack. At communication line lengths from 50 km, the main contribution to the losses is no longer from the detectors but from the communication channel; therefore, the curves for these two cases approach each other and practically coincide at lengths from 120 km.

Note that, in recent studies [60–63], generalizations of the beam splitting attack for the B92, COW (Coherent One Way), and DPS (Differential Phase Shift) protocols are considered. In these generalizations, the adversary can change the intensity of states, and their further actions depend on whether they have managed to extract information from the part of the state diverted by the beam splitter.

9. Comparison of photon-number splitting and beam splitting attacks

Beam splitting and photon-number splitting attacks are very important in quantum cryptography, so, in this section, we explain why the first attack is less effective than the second one. To do this, we first prove the inequality

$$R < R_{\mathrm{BS}}, \tag{38}$$

where R is calculated using formula (20) and R_{BS} is calculated using formula (37) for $t = \eta T(L)$ (i.e., with the weakest assumption about the adversary). If we replace inequality (38) with the nonstrict one, then it follows directly from formula (20), because formula (20) is derived for a general attack. Let us prove a strict inequality, i.e., that the beam splitting attack is always suboptimal. We also recall that the photon-number splitting attack is optimal, i.e., key rate (20) is maximally achievable.

Let us prove (38) for the case $\mu \leqslant 1$. The case $\mu > 1$ can also be considered, but in practice, $\mu \leqslant 1$, so, for simplicity, we restrict ourselves to considering only this case. We also assume that the quantity $\eta T(L)$ is strictly positive (otherwise, not only the key distribution, but also any communication is impossible). Recall also that $\eta T(L) \leqslant 1$.

Since the term $h(E^{\mathrm{s}z})$ in both formulas (20) and (29) is the same, the proof of (38) is reduced to the proof of the inequality

$$\frac{Q_1^{\mu}}{Q^{\mu}}\left[1 - h(e_1^x)\right] < \exp\left[-(1-t)\mu\right]. \tag{39}$$

Let us prove a stricter inequality,

$$\frac{Q_1^{\mu}}{Q^{\mu}} < \exp\left[-(1-t)\mu\right]. \tag{40}$$

Using (30)–(32), for the left-hand side, we have

$$\frac{Q_1^{\mu}}{Q^{\mu}} = \frac{\mu \exp\left(-\mu\right)(p_{\mathrm{d}} + t)}{p_{\mathrm{d}} + 1 - \exp\left(-\mu t\right)}. \tag{41}$$

Let us consider the fraction

$$\frac{p_{\mathrm{d}} + t}{p_{\mathrm{d}} + 1 - \exp\left(-\mu t\right)}. \tag{42}$$

In view of the inequality $1 - \exp\left(-x\right) < x$ for $x > 0$ and, therefore, $1 - \exp\left(-\mu t\right) < \mu t \leqslant t$, one can conclude that the fraction decreases with increasing p_{d}, so that

$$\frac{\mu \exp\left(-\mu\right)(p_{\mathrm{d}} + t)}{p_{\mathrm{d}} + 1 - \exp\left(-\mu t\right)} \leqslant \frac{\mu t \exp\left(-\mu\right)}{1 - \exp\left(-\mu t\right)}. \tag{43}$$

Thus, it is necessary to prove the inequality

$$\frac{\mu t \exp\left(-\mu\right)}{1 - \exp\left(-\mu t\right)} < \exp\left[-\mu(1-t)\right], \tag{44}$$

or

$$\frac{\mu t}{\exp\left(\mu t\right) - 1} < 1 . \tag{45}$$

This inequality obviously follows from $\exp x - 1 > x$ for $x > 0$. Inequality (40) and, therefore, inequality (38) have been proved.

Let us analyze the reasons why inequality (38) is strict, so that the beam splitting attack is not optimal. First, in the proof of (38), we have used the inequality $h(e_1^x) > 0$ for $e_1^x > 0$. This means that the beam splitting attack does not attack single-photon transmissions at the cost of introducing noise, in contrast to the photon-number splitting attack. This is the first reason why the beam splitting attack is nonoptimal.

Second, inequality (40) arises from the following effect. Since the sent state is a mixture of Fock states, we can think about a certain number of photons in a pulse, even if this observable is not actually measured by anyone. One can imagine another participant who, before the actions of the adversary, measures the number of photons in the pulse (without changing the state) and then observes the adversary's actions with the knowledge of the number of photons. They then observe that, in the case of the photon-number splitting attack, the adversary recognizes the information encoded in multiphoton pulses with certainty, while in the case of the beam splitting attack, with a certain probability, they can transmit all photons to the receiver without leaving a single photon for themselves or, conversely, they take all the photons for themselves without passing a single one to the receiver. The last alternative leads to the no registration event (unless a dark count occurs) on the receiver's side, so this position is not included in the sifted key. In this case, the fraction of multiphoton (insecure) states in the sifted key decreases. In contrast, in the photon-number splitting attack, only the single-photon transmissions are blocked. Probabilistic processing of multiphoton pulses in the beam splitting attack, instead of optimal deterministic processing in the photon-number splitting attack, is the reason for inequality (40). Moreover, if, after measuring the number of photons, the adversary performs a probabilistic processing of the multiphoton pulses, then they can reproduce (simulate) the beam splitting attack.

In Ref. [37], it is noted that, in the beam splitting attack, the adversary takes away almost all quantum states. However, only those positions in which the receiver also registers a photon participate in the key generation. Therefore, the withdrawal of the adversary of almost all quantum states leads to losses but does not necessarily lead to a large amount of knowledge of the adversary about the sifted key.

From the figure (see Section 7), we see that, at the considered parameters and the length of the communication line up to approximately 140 km, the possibilities of these two attacks practically coincide: the achievable secret key rate for the case of the beam splitting attack is only slightly higher than the achievable secret key rate for the case of the photon-number splitting attack. At communication channel lengths over 140 km, the advantages of the photon number splitting attack become significant, and the curves diverge. Over a length of approximately 200 km, the achievable rate in the case of the photon-number splitting attack drops to zero, while the secret key can still be generated in the case of the beam splitting attack.

From the above reasoning, it is possible once again (see the end of Section 5) to easily deduce the optimality of the photon-number splitting attack. If it is possible to measure the number of photons without spoiling the state, it is optimal to do this. Next, one should take actions that are optimal for a given known number of photons. Obviously, if the state is multiphoton, then it is optimal to remove one photon from it (more is possible, but one photon also gives complete information about the key bit). If the transmission is single photon, it is optimal to carry out the optimal attack for the single-photon pulses at the cost of introducing noise. Since the transmitted state is a mixture of Fock states and any quantum transformation is linear, any possible attack can be simulated by measuring the number of photons and applying one probabilistic treatment of a pulse or another, depending on the number of photons in it. In fact, the theorem (see Section 5) is a formalization of these discussions.

In concluding this section, let us mention the unambiguous state discrimination attack (USD attack). For the BB84 protocol, it is discussed in Ref. [58]. It is emphasized that, in the case of coherent states, with a randomized phase, the photon-number splitting attack (without attacking the single-photon pulses) is an optimal discrimination of states with an unambiguous outcome.

10. Polarization and phase encoding

Some researchers cast doubts on the applicability of the decoy state method in the case of the widely used phase encoding instead of polarization encoding [40]. To eliminate these doubts, in this section, we show that these two encoding methods are completely equivalent; therefore, the decoy state method is applicable to phase encoding in the same way as to the polarization one.

Note that the previous discussion did not rely on what kind of encoding is used, although we have referred to the polarization encoding, for example.

In the polarization encoding, creation operators $a_{z0}^\dagger$, $a_{z1}^\dagger$, $a_{x0}^\dagger$, and $a_{x1}^\dagger$ in Eqns (2)–(4) can be, for example, photon creation operators with horizontal, vertical, diagonal, and antidiagonal polarizations: $a_{\mathrm{H}}^\dagger$, $a_{\mathrm{V}}^\dagger$, $a_{\mathrm{D}}^\dagger$, and $a_{\mathrm{A}}^\dagger$, respectively. The transmitted states can then be rewritten in the form

$$|\alpha, 0\rangle_z = |\alpha\rangle_{z0}|0\rangle_{z1} \equiv |\alpha\rangle_{\mathrm{H}}|0\rangle_{\mathrm{V}} ,$$

$$|\alpha, 1\rangle_z = |0\rangle_{z0}|\alpha\rangle_{z1} \equiv |0\rangle_{\mathrm{H}}|\alpha\rangle_{\mathrm{V}} ,$$

$$|\alpha, 0\rangle_x = |\alpha\rangle_{x0}|0\rangle_{x1} \equiv |\alpha\rangle_{\mathrm{D}}|0\rangle_{\mathrm{A}} = \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{H}}\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{V}} , \tag{46}$$

$$|\alpha, 1\rangle_x = |0\rangle_{x0}|\alpha\rangle_{x1} \equiv |0\rangle_{\mathrm{D}}|\alpha\rangle_{\mathrm{A}} = \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{H}}\left|-\frac{\alpha}{\sqrt{2}}\right\rangle_{\mathrm{V}} ,$$

where $|\alpha\rangle = \exp\left(-\mu/2\right)\sum_{j=1}^{\infty}(\alpha^j/\sqrt{j!})|j\rangle$ and $|j\rangle, j = 0, 1, \ldots$ are a coherent state and a state with a definite number of photons in the corresponding mode, respectively, $\alpha \in \mathbb{C}$, $\mu = |\alpha|^2$.

However, in the phase encoding, the employed states have the following form [18, 40]:

$$\left|(-1)^u \frac{\exp\left(\mathrm{i}\varphi_b\right)\alpha}{\sqrt{2}}\right\rangle_1 \left|\frac{\alpha}{\sqrt{2}}\right\rangle_2 , \tag{47}$$

where $u \in \{0, 1\}$ is the coding bit, $b \in \{z, x\}$ is the basis, $\varphi_z = 0$, $\varphi_x = \pi/2$, and modes 1 and 2 correspond to two time windows. That is, each signal consists of two phase-matched pulses. The phase in each pair of pulses is randomly selected,

i.e., the adversary and the receiver 'observe' a state of the form

$$\frac{1}{2\pi}\int_0^{2\pi} d\theta \left(\left| (-1)^u \exp\left[i(\varphi_b+\theta)\right]\sqrt{\frac{\mu}{2}} \right\rangle_1 \left| \exp(i\theta)\sqrt{\frac{\mu}{2}} \right\rangle_2 \right)$$
$$\times \left({}_2\!\left\langle \exp(i\theta)\sqrt{\frac{\mu}{2}} \right|_1 \left\langle (-1)^u \exp\left[i(\varphi_b+\theta)\right]\sqrt{\frac{\mu}{2}} \right| \right). \quad (48)$$

The interference scheme on the receiver side is designed in such a way that only the phase difference in the two windows matters.

Let us show that the states of polarization encoding can be represented in a form equivalent to expression (47). Consider creation operators of photons with right and left circular polarizations:

$$a_R^\dagger = \frac{a_H^\dagger - i a_V^\dagger}{\sqrt{2}},$$
$$a_L^\dagger = \frac{a_H^\dagger + i a_V^\dagger}{\sqrt{2}}. \quad (49)$$

Then, states (46) can be written in the from

$$|\alpha,0\rangle_z = \left| \frac{\alpha}{\sqrt{2}} \right\rangle_R \left| \frac{\alpha}{\sqrt{2}} \right\rangle_L,$$
$$|\alpha,1\rangle_z = \left| \frac{i\alpha}{\sqrt{2}} \right\rangle_R \left| -\frac{i\alpha}{\sqrt{2}} \right\rangle_L,$$
$$|\alpha,0\rangle_x = \left| \frac{(1+i)\alpha}{2} \right\rangle_R \left| \frac{(1-i)\alpha}{2} \right\rangle_L, \quad (50)$$
$$|\alpha,1\rangle_x = \left| \frac{(1-i)\alpha}{2} \right\rangle_R \left| \frac{(1+i)\alpha}{2} \right\rangle_L.$$

The first state coincides with state (47) for $u = 0$ and $b = z$, the second state coincides with the corresponding state (47) when both phases are shifted by $\pi/2$ (i.e., with α replaced by $\exp(i\pi/2)\alpha)$), the third state is when phases are shifted by $\pi/4$, and, finally, the fourth state is when phases are shifted by $-\pi/4$. In view of the phase randomization (6) and (48), these phase shifts play no role. Application of the inverse phase shifts in expressions (47) and the inverse transformation with respect to transformation (49) (with a different label for the modes, since they now do not correspond to the polarizations) gives states (6).

Thus, polarization and phase encoding are completely mathematically equivalent: they correspond to different mode expansions of the same states. That is why we can conclude that the theorem (see Section 5) and estimates (27) and (28) do not depend on the type of encoding: states of both polarization and phase encoding can be expressed in form (6).

This is confirmed by the results from Ref. [40], where for the case of phase coding, the same decoy state method estimates are obtained as for the polarization coding. But it should be noted that an equivalence takes place when the *total* pulse intensity in two windows in Eqn (47) coincides with the pulse intensity for polarization coding (46) $\mu = |\alpha|^2$. The pulse intensity in each window should be, respectively, two times less. Taking into account this remark, the estimates derived in Ref. [40] completely coincide with the well-known estimates derived in Ref. [29].

It is important that transformation (49) preserve the photon number:

$$a_H^\dagger a_H + a_V^\dagger a_V = a_D^\dagger a_D + a_A^\dagger a_A = a_R^\dagger a_R + a_L^\dagger a_L.$$

This means that estimates related to the number of single-photon pulses and the corresponding errors obtained for one mode expansion are also valid for the other expansion of the same state.

Using the described transformations, it is possible, for example, to reformulate the photon-number splitting attack, which was originally formulated for polarization encoding, for phase encoding. Of course, the mathematical equivalence of the two coding methods does not imply the same technological complexity of the photon-number splitting attack in these two cases. However, when calculating the key length, we are not interested in the technological complexity of certain adversary operations, since we assume that the adversary can carry out any transformations allowed by the mathematical apparatus.

11. Conclusion

In this paper, we have presented the decoy state method in quantum cryptography, focusing on issues that are usually not covered in the literature. The first one is a formal proof that the security of the protocol with a phase-randomized coherent state source is reduced to the security of the corresponding single-photon source protocol. This proof strongly justifies the security of the decoy state protocol against all kinds of attacks, not just the photon-number splitting attack.

The emphasis on the photon-number splitting attack in the literature is related to the fact that this attack is optimal. However, the security proof of the decoy state method does not rely on this fact. Notably, we have compared the photon-number splitting attack with the beam splitting attack and both analytically and numerically demonstrated the lower efficiency of the latter.

Another issue considered in the paper is the equivalence of polarization and phase encoding from the viewpoint of the security of quantum cryptography with decoy states. Despite the fact that, technologically, these two methods of state encoding and, therefore, attacks on the corresponding implementations are significantly different, they are completely equivalent mathematically. In the security analysis, we assume that the adversary can realize any transformations that are allowed by the mathematical apparatus; therefore, the argument of mathematical equivalence is sufficient to justify the equal theoretical security of protocols using these two types of encoding.

Thus, in numerous theoretical papers dealing with the decoy state BB84 protocol, as well as in experimental implementations of this protocol, including the implementation described in Ref. [35], the estimate of the secret key length is justified and rigorously proven.

We also note that, in Ref. [33], a method of calculating estimates for the decoy state method taking into account statistical fluctuations is proposed. Also, in Ref. [20], a generalization of the decoy state method estimates in the case of detection-efficiency mismatch is presented.

References

1. Alferov A P et al. *Osnovy Kriptografii* (Basics of Cryptography) 2nd ed. (Moscow: Gelios ARV, 2002)
2. Schneier B *Applied Cryptography: Protocols, Algorithms, and Source Code in C* 2nd ed. (New York: Wiley, 1996)
3. Shor P W *SIAM J. Comput.* **26** 1484 (1997)
4. Anschuetz E et al., in *Quantum Technology and Optimization Problems. QTOP 2019* (Lecture Notes in Computer Science, Vol. 11413, Eds S Feld, C Linnhoff-Popien) (Cham: Springer, 2019) p. 74
5. Mosca M *IEEE Secur. Priv.* **16** (5) 38 (2018)
6. Bennet C H, Brassard G, in *Proc. of the IEEE Intern. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (New York: IEEE, 1984) p. 175
7. Ekert A K *Phys. Rev. Lett.* **67** 661 (1991)
8. Holevo A S *Matematicheskie Osnovy Kvantovoi Informatiki* (Mathematical Foundations of Quantum Informatics) (Lektsionnye Kursy NOTs, Issue 30) (Moscow: MIAN, 2018) p. 3
9. Wiesner S *ACM SIGACT News* **15** (1) 78 (1983)
10. Mayers D, in *Advances in Cryptology — CRYPTO 96. CRYPTO 1996* (Lecture Notes in Computer Science, Vol. 1109, Ed. N Koblitz) (Berlin: Springer, 1996) p. 343; quant-ph/9606003
11. Mayers D *J. ACM* **48** 351 (2001)
12. Shor P W, Preskill J *Phys. Rev. Lett.* **85** 441 (2000)
13. Koashi M *New J. Phys.* **11** 045018 (2009)
14. Renner R "Security of quantum key distribution", Ph.D. Thesis (Zürich: ETH, 2005); quant-ph/0512258
15. Tomamichel M et al. *Nat. Commun.* **3** 634 (2012)
16. Tomamichel M, Leverrier A *Quantum* **1** 14 (2017)
17. Dupuis F, Fawzi O, Renner R *Commun. Math. Phys.* **379** 867 (2020)
18. Gisin N et al. *Rev. Mod. Phys.* **74** 145 (2002)
19. Scarani V et al. *Rev. Mod. Phys.* **81** 1301 (2009)
20. Bochkov M K, Trushechkin A S *Phys. Rev. A* **99** 032308 (2019)
21. Portmann C, Renner R, arXiv:1409.3525
22. Trushechkin A S *Quantum Electron.* **50** 426 (2020); *Kvantovaya Elektron.* **50** 426 (2020)
23. Diamanti E et al. *npj Quantum Inf.* **2** 16025 (2016)
24. Huttner B et al. *Phys. Rev. A* **51** 1863 (1995)
25. Brassard G et al. *Phys. Rev. Lett.* **85** 1330 (2000)
26. Hwang W-Y *Phys. Rev. Lett.* **91** 057901 (2003)
27. Lo H-K, Ma X, Chen K *Phys. Rev. Lett.* **94** 230504 (2005)
28. Wang X-B *Phys. Rev. Lett.* **94** 230503 (2005)
29. Ma X et al. *Phys. Rev. A* **72** 012326 (2005)
30. Curty M et al. *Nat. Commun.* **5** 3732 (2014)
31. Lim C C W et al. *Phys. Rev. A* **89** 022307 (2014)
32. Zhang Z et al. *Phys. Rev. A* **95** 012333 (2017)
33. Trushechkin A S, Kiktenko E O, Fedorov A K *Phys. Rev. A* **96** 022316 (2017)
34. Lo H-K, Curty M, Tamaki K *Nat. Photon.* **8** 595 (2014)
35. Duplinskiy A V et al. *J. Russ. Laser Res.* **39** 113 (2018)
36. Chen K, Ma J, Shi H, Talk, ISO/IEC JTC1 SC27 WG3 SP Proposal, Security Requirements, Test and Evaluation Methods for the Decoy State BB84 Quantum Key Distribution (QKD), Berlin, Germany, 10/31/2017; ISO/IEC JTC 1/SC 27/WG 3 N 1537, 30th ISO/IEC JTC1/SC27 Working Group Meeting, H Shi, J Ma, G Pradel Wuhan, China, April 2018 30th Security Requirements, Test and Evaluation Methods for Quantum Key Distribution
37. Molotkov S N, Kravtsov K S, Ryzhkin M I *J. Exp. Theor. Phys.* **128** 544 (2019); *Zh. Eksp. Teor. Fiz.* **155** 636 (2019)
38. Molotkov S N, Kravtsov K S, Ryzhkin M I *J. Exp. Theor. Phys.* **129** 319 (2019); *Zh. Eksp. Teor. Fiz.* **156** 379 (2019)
39. Devetak I, Winter A *Proc. R. Soc. Lond. A* **461** 207 (2005)
40. Kulik S P, Molotkov S N *Laser Phys. Lett.* **14** 125205 (2017)
41. Kilin S Ya *Phys. Usp.* **42** 435 (1999); *Usp. Fiz. Nauk* **169** 507 (1999)
42. Valiev K A *Phys. Usp.* **48** 1 (2005); *Usp. Fiz. Nauk* **175** 3 (2005)
43. Molotkov S N *Phys. Usp.* **49** 750 (2006); *Usp. Fiz. Nauk* **176** 777 (2006)
44. Lo H-K, Chau H F, Ardehali M *J. Cryptology* **18** 133 (2005)
45. Trushechkin A S et al. *Phys. Rev. A* **97** 012311 (2018)
46. Fung C-H F, Ma X, Chau H F *Phys. Rev. A* **81** 012318 (2010)
47. Kiktenko E, Trushechkin A, Kurochkin Yu, Fedorov A *J. Phys. Conf. Ser.* **741** 012081 (2016)
48. Fedorov A K, Kiktenko E O, Trushechkin A S *Lobachevskii J. Math.* **39** 992 (2018)
49. Kiktenko E O et al. *Phys. Rev. Appl.* **8** 044017 (2017)
50. Kronberg D A *Mat. Vopr. Kriptogr.* **8** (2) 77 (2017)
51. Wegman M N, Carter J L *J. Comput. Syst. Sci.* **22** 265 (1981)
52. Kiktenko E O et al. *IEEE Trans. Inform. Theory* **66** 6354 (2020)
53. Lieb E H *Adv. Math.* **11** 267 (1973)
54. Holevo A S *Quantum Systems, Channels, Information*: a Mathematical Introduction (Berlin: De Gruyter, 2012); Translated from Russian: *Kvantovye Sistemy, Kanaly, Informatsiya* (Moscow: Izd. MTsNMO, 2010)
55. Cao Z et al. *New J. Phys.* **17** 053014 (2015)
56. Lim C C W et al. *Phys. Rev. A* **89** 022307 (2014)
57. Bennett C H et al. *J. Cryptology* **5** 3 (1992)
58. Dušek M, Jahma M, Lütkenhaus N *Phys. Rev. A* **62** 022306 (2000)
59. Félix S et al. *J. Mod. Opt.* **48** 2009 (2001)
60. Kronberg D A, Kurochkin Yu V *Quantum Electron.* **48** 843 (2018); *Kvantovaya Elektron.* **48** 843 (2018)
61. Kronberg D A, Kiktenko E O, Fedorov A K, Kurochkin Yu V *Quantum Electron.* **47** 163 (2017); *Kvantovaya Elektron.* **47** 163 (2017)
62. Avanesov A S, Kronberg D A, Pechen A N *P-Adic Num. Ultrametr. Anal. Appl.* **10** 222 (2018)
63. Kronberg D A, Nikolaeva A S, Kurochkin Y V, Fedorov A K *Phys. Rev. A* **101** 032334 (2020)