ISSN 1063-7761, Journal of Experimental and Theoretical Physics, 2020, Vol. 131, No. 6, pp. 877–894. © Pleiades Publishing, Inc., 2020.
Russian Text © The Author(s), 2020, published in Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2020, Vol. 158, No. 6, pp. 1011–1031.

ATOMS, MOLECULES, OPTICS

Robustness of Quantum Cryptography Systems with Phase–Time Coding against Active Probing Attacks

S. N. Molotkov[a,b,c,*]

[a] *Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow oblast, 142432 Russia*
[b] *Academy of Cryptography of the Russian Federation, Moscow, 121552 Russia*
[c] *Quantum Technology Center, Moscow State University, Moscow, 119899 Russia*
**e-mail: sergei.molotkov@gmail.com*

Received May 11, 2020; revised May 11, 2020accepted July 3, 2020

Abstract—The robustness of a quantum cryptography system is considered that uses a protocol with phase–time coding on attenuated coherent states. This protocol admits an effective fiber optic implementation, which does not require a phase modulator on the receiver side and adjusting the polarization state at the input of the receiver side. The absence of a phase modulator on the receiver side excludes a side channel of information leakage associated with the active probing of the phase modulator at the receiving station, thus making the system more robust against such attacks compared to other systems. The nonstrict single-photon nature of information states, as well as information leakage through side channels, is considered by the generalized decoy state method, which takes into account joint collective measurements of information quantum states and quantum states in side channels. An estimate for the secret key length is obtained that is expressed only in terms of observed quantities at the receiving station and the parameters of quantum states in side channels.

DOI: 10.1134/S1063776120110138

1. INTRODUCTION

Quantum cryptography systems are designed to create a shared secret—a secret key between spatially remote users. The distribution of keys is based on the transmission and measurement of quantum states. Attempts to intrude into quantum communication channel lead to the perturbation of states and errors on the receiver side [1].

The fundamental laws of quantum mechanics make it possible to associate the information leakage to the eavesdropper with the observed level of errors on the receiver side [2, 3].

For various quantum key distribution protocols, fundamental upper bounds for information leakage to the eavesdropper during attacks on states in a quantum communication channel were obtained. The source of quantum states—a strongly attenuated coherent state—is not a strictly single-photon source; this leads to a number of new attacks on the transmitted quantum states that are absent in the case of a strictly single-photon source [4]. In [5–8], the authors developed methods that take into account that the source of quantum information states is not strictly single-photon.

To date, a sufficient understanding has been achieved regarding attacks on transmitted quantum states in a communication channel. When proving the secrecy of keys in quantum cryptography, it is implicitly assumed that the receiving and transmitting equipment is absolutely isolated from the outside world.

In any cryptographic system, side channels are an important source of information leakage. In classical cryptographic systems, one of these channels is the side electromagnetic radiation of electronic equipment, which can be detected remotely without direct access to the equipment itself.

In the case of quantum cryptography systems, the situation with side channels of information leakage is even more delicate than in classical cryptography. Quantum cryptography systems are open systems in the sense that, in addition to detecting the side radiation of the transmitting and receiving equipment, the eavesdropper can actively probe the state of active elements (phase modulators, an intensity modulator, backscattering radiation of avalanche detectors, etc.) by external radiation through a fiber communication line. The fundamental difference between intrusion into a quantum communication channel and the detection of side radiation and active probing of the equipment is that the detection of states in side channels does not lead to errors on the receiver side, since it does not disturb the transmitted states.

The further logic of proving key secrecy with regard to the side channels of information leakage and a nonstrictly single-photon source of information states is as follows. The statistics of laser radiation is Poisson in

terms of the number of photons: the communication channel with Poisson probabilities contains Fock states with different numbers of photons. The secret key is composed only of the single-photon component of the states. The information contained in multiphoton components with the number of photons $k \geq 2$ is assumed, conservatively in favor of the eavesdropper, to be known to the eavesdropper. The most general attack of the eavesdropper on single-photon states is a unitary attack, which is constructed explicitly. A unitary attack is an attack where the eavesdropper uses her auxiliary (ancilla) state and entangles it with the transmitted state using a unitary operator. The eavesdropper sends the distorted information state to the receiver side and leaves her subsystem in quantum memory. After measurements on the receiver side, error correction, and enhancing secrecy, the eavesdropper performs collective measurements over all quantum states in her memory.

Each side leakage channel is a quantum state that represents the state of the equipment, phase modulators, intensity modulators, and avalanche detectors. As a result, in each message, the eavesdropper has at her disposal additional quantum states that are "tied" to information states. Of course, side channels also arise when the communication channel contains states with the number of photons $k \geq 2$, but the information contained in these messages is already given (is conservatively assumed to be known) to the eavesdropper. Therefore, quantum states in side channels can be considered "linked" only to the single-photon component of information states.

The eavesdropper also stores quantum states from the side channels in quantum memory until the end of the protocol, and then performs joint collective measurements on the ancilla state and the quantum states from the side channels.

The next step is to estimate the fraction of the single-photon component that reaches the receiver side. In this case, the decoy state method is used, which is reduced to sending randomly coherent states with a different average number of photons in different messages. The intensity modulation of coherent states occurs using an intensity modulator. The decoy state method is based on the fact that the eavesdropper, having detected a Fock state with a given number k of photons in the channel, cannot determine from which coherent state and with what average number of photons a given component comes from. In the presence of active probing of the intensity modulator, the eavesdropper can, albeit with a certain error probability, determine from which state a given number of photons come from. For this reason, the standard decoy state method must be modified in the case of an attack on the intensity modulator. This modification will be made below.

In a unitary attack on single-photon states without side channels of information leakage, one can use the fundamental entropy uncertainty relations, which relate the error on the receiver side to the information leakage to the eavesdropper. In this case, the explicit construction of an attack of the eavesdropper—a unitary operator, ancilla state, etc.—is not required. In the presence of side channels of information leakage, one has to explicitly construct an attack on the single-photon component of states, since the side channels do not lead to errors on the receiver side, and the relation between the information leakage and the errors on the receiver side is broken. The explicit construction of an attack is necessary also because the quantum states in the side channels are attached in each message to information states, which requires their explicit knowledge.

2. PHASE–TIME CODING, THE SINGLE-PHOTON CASE

The implementation of quantum cryptography with phase–time coding discussed below is remarkable in that a polarization-sensitive element—a phase modulator—is not used on the receiver side; this makes the system more robust against active probing attacks compared to other systems. In addition, the absence of polarization-sensitive elements on the receiver side leads to the fact that the system does not require the adjustment of the polarization of the states arriving at the receiver side from the quantum communication channel.

Further, such a system allows one to implement, in addition to the phase–time coding protocol, the BB84 protocol [9], which provides even greater flexibility and universality of the system.

In a real system, strongly attenuated coherent states are used as information states. The phase–time coding protocol uses two bases, L and R (see the explanations in Fig. 1; the indices L and R correspond to left and right), each of which has a pair of orthogonal states. Due to the overlap in time of the bases, the states are pairwise nonorthogonal.

The states in the basis L have the form

$$0_L \to |\alpha\rangle_1 \otimes |\alpha\rangle_2, \quad 1_L \to |\alpha\rangle_1 \otimes |-\alpha\rangle_2, \qquad (1)$$

where indices "1" and "2" correspond to the time window (see Fig. 1) and $|\alpha|^2 = \mu$ is the average number of photons in a strongly attenuated coherent state, $|\alpha|^2 = \mu \ll 1$. Similarly, in the basis R,

$$0_R \to |\alpha\rangle_2 \otimes |\alpha\rangle_3, \quad 1_R \to |-\alpha\rangle_2 \otimes |\alpha\rangle_3. \qquad (2)$$

Logical bits 0 and 1 in each basis are encoded in the relative phase of coherent states in time windows 1 and 2 in basis L and in time windows 2 and 3 in basis R. Since in each message the pulsed laser is turned on and off during the formation of information states, the phase θ of the coherent state itself (parameter $\alpha = e^{i\theta}|\alpha|$) is random. For this reason, the eavesdropper sees in the communication channel a statistical

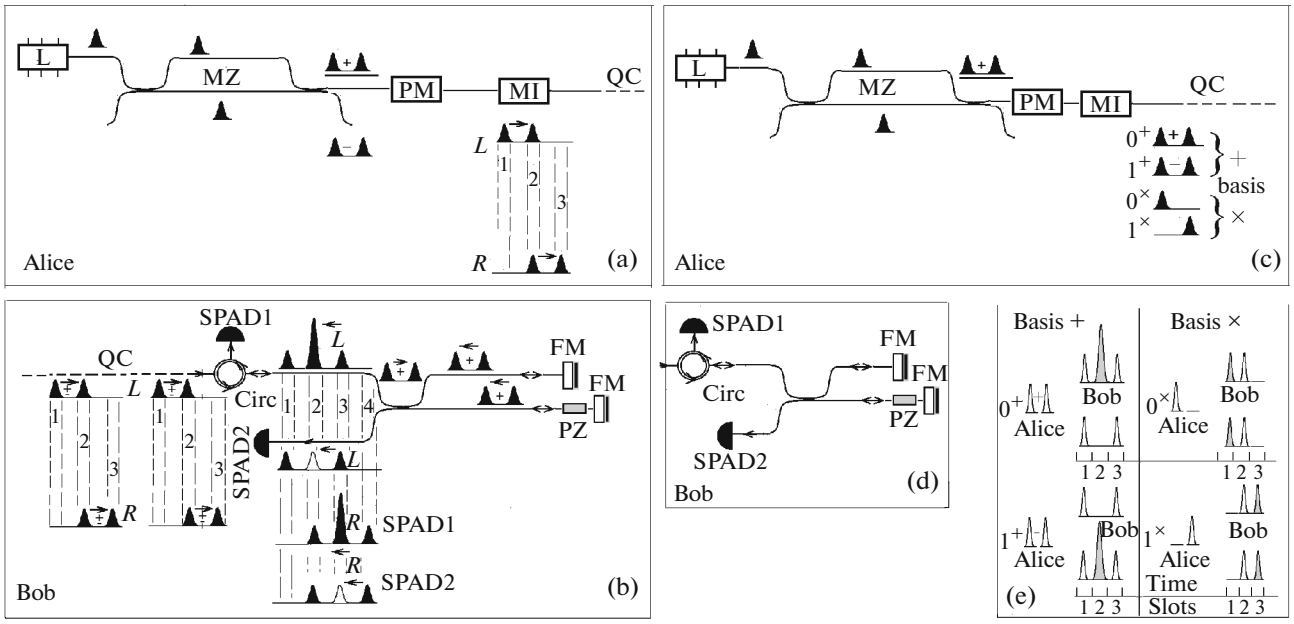

Fig. 1. (a, b) Implementation of a system with phase–time coding. (a) Transmitter side (Alice): L is a laser operating in the CW mode, MZ is a Mach–Zehnder interferometer, MI is an intensity modulator, and PM is a phase modulator. The whole optical path at the transmitting station is based on a polarization-maintaining fiber. (b) Receiver side (Bob): the whole optical path is based on a standard single-mode SM fiber. Circ is a fiber-optic polarization-independent circulator, SPAD1,2 are single-photon avalanche detectors, FM is a Faraday mirror, PZ is a controlled piezoelectric element for equalizing the path difference between the upper and lower arms of the interferometer, and QC is a communication line based on SM fiber. The arrows indicate the evolution of states, as well as the formation of interference on the receiver side. (c–e) Implementation of a system with the BB84 protocol. (c) Transmitting station and evolution of states. (d) Receiving station and evolution of states in the direct (subscript +) and conjugate (subscript ×) bases. (e) Interference of states on the receiver side in the direct and conjugate bases.

mixture of coherent states rather than pure coherent states. In the basis L, we have

$$\rho^x(\mu) = e^{-2\mu}\sum_{k=0}^{\infty}\frac{(2\mu)^k}{k!}|\Psi_k^x\rangle_{BB}\langle\Psi_k^x| = \sum_{k=0}^{\infty}P^{(k)}(\mu)|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|, \quad (3)$$

$$P^{(k)}(\mu) = e^{-2\mu}\frac{(2\mu)^k}{k!}, \qquad |\Psi_k^x\rangle_B = \sqrt{\frac{k!}{2^k}}\sum_{m=0}^{k}e^{i\varphi_x m}\frac{|m\rangle_1\otimes|k-m\rangle_2}{\sqrt{m!(k-m)!}}, \quad (4)$$

where $x = 0, 1$; $\varphi_x = 0$ ($x = 0$) and $\varphi_x = \pi$ ($x = 1$), φ_x is the relative phase of the states localized in time windows 1 and 2 into which information about the key bits is encoded; and the states $|m\rangle_1 \otimes |k - m\rangle_2$ are Fock states in time windows 1 and 2 (subscripts). In the basis R, the expression for the density matrix is similar to (3), (4), with the replacement of the indices of time windows for states, $(1, 2) \to (2, 3)$.

The secret key is derived from the single-photon component of states. The information contained in the multiphoton components of states (3) and (4) is assumed, conservatively in favor of the eavesdropper, to be known to her. For the single-photon component, the intrusion into the communication channel leads to a disturbance and errors on the receiver side. A further task is to establish a relationship between the probability of errors on the receiver side and the amount of information that can be extracted by the eavesdropper for a given observed error probability. In what follows, we estimate by the modified decoy state method the fraction of the single-photon component on the receiver side from which the secret key is derived.

The single-photon component of information states in the left basis has the form

$$|0_L\rangle_X = \frac{1}{\sqrt{2}}(|1\rangle_1\otimes|0\rangle_2 + |0\rangle_1\otimes|1\rangle_2) = \frac{1}{\sqrt{2}}(|1\rangle_1 + |1\rangle_2), \quad (5)$$

$$|1_L\rangle_X = \frac{1}{\sqrt{2}}(|1\rangle_1\otimes|0\rangle_2 - |0\rangle_1\otimes|1\rangle_2) = \frac{1}{\sqrt{2}}(|1\rangle_1 - |1\rangle_2), \quad (6)$$

while, in the right basis, the states are as follows:

$$|0_R\rangle_X = \frac{1}{\sqrt{2}}(|1\rangle_2\otimes|0\rangle_3 + |0\rangle_2\otimes|1\rangle_3) = \frac{1}{\sqrt{2}}(|1\rangle_2 + |1\rangle_3), \quad (7)$$

$$|1_R\rangle_X = \frac{1}{\sqrt{2}}(|1\rangle_2\otimes|0\rangle_3 - |0\rangle_2\otimes|1\rangle_3) = \frac{1}{\sqrt{2}}(|1\rangle_2 - |1\rangle_3), \quad (8)$$

to save notation, we omitted the vacuum component of the field in the corresponding time windows; below,

$|1\rangle_i$ is a single-photon state localized in time window i. In the basis L, information states are a superposition of single-photon states in time windows 1 and 2; accordingly, in the basis R, these states are a superposition in time windows 2 and 3. Inside the basis, the information states are orthogonal and are therefore reliably distinguishable. The states of the bases L and R are pairwise nonorthogonal and reliably indistinguishable. The nonorthogonality of states from different bases guarantees that the intrusion of the eavesdropper into the quantum communication channel perturbs the transmitted states and leads to errors on the receiver side. In contrast to the BB84 protocol, the perturbation of states will also lead to counts in the control time windows [10, 11].

A unitary attack on single-photon states can be represented as

$$\begin{aligned}|\Psi_{0_L}\rangle_{XYQ} &= |0_L\rangle_X \otimes U_{BE}(|0_L\rangle_Y \otimes |E\rangle_Q),\\ |\Psi_{1_L}\rangle_{XYQ} &= |1_L\rangle_X \otimes U_{BE}(|1_L\rangle_Y \otimes |E\rangle_Q),\end{aligned} \tag{9}$$

where $|E\rangle_Q$ is an auxiliary state of Eve, ancilla; $|0_L\rangle_X$ and $|1_L\rangle_X$ are Alice's reference states that are inaccessible to the eavesdropper, and $|0_L\rangle_Y$ and $|1_L\rangle_Y$ are states in the quantum communication channel transmitted to Bob, that are accessible to Eve's attack.

Similar equations are obtained in the basis R. The entanglement of the information state and the ancilla state of Eve in the basis R is obtained from (5)–(8) by linear transformation (9)–(11).

In the basis L, we find (see [10, 11] for details; henceforth, we omit the subscript L for brevity)

$$\begin{aligned}|\Psi_0\rangle_{XYQ} &= |0_L\rangle_X \otimes [|0_L\rangle_Y \otimes |\Phi_0\rangle_Q\\ &+ |1_L\rangle_Y \otimes |\Theta_0\rangle_Q + |c_L\rangle_Y \otimes |\Lambda_0\rangle_Q],\end{aligned} \tag{10}$$

$$\begin{aligned}|\Psi_1\rangle_{XYQ} &= |1_L\rangle_X \otimes [|1_L\rangle_Y \otimes |\Phi_1\rangle_Q\\ &+ |0_L\rangle_Y \otimes |\Theta_1\rangle_Q + |c_L\rangle_Y \otimes |\Lambda_1\rangle_Q].\end{aligned} \tag{11}$$

The expansion (10), (11) is the Schmidt expansion in the tensor product of the state spaces of Eve and Bob. The expansion in the basis R is obtained by linear transformation (9)–(11).

The normalization of states has the form (see [10, 11] for details)

$$\begin{aligned}{}_Q\langle\Phi_{0,1}|\Phi_{0,1}\rangle_Q &= (1-\zeta)(1-Q),\\ {}_Q\langle\Theta_{0,1}|\Theta_{0,1}\rangle_Q &= (1-\zeta)Q,\\ {}_Q\langle\Lambda_{0,1}|\Lambda_{0,1}\rangle_Q &= \zeta.\end{aligned} \tag{12}$$

For what follows, it is convenient to introduce the normalized states

$$\begin{aligned}\sqrt{(1-\zeta)(1-Q)}|\bar\Phi_{0,1}\rangle_Q &= |\Phi_{0,1}\rangle_Q,\\ \sqrt{(1-\zeta)Q}|\bar\Theta_{0,1}\rangle_Q &= |\Theta_{0,1}\rangle_Q,\\ \sqrt{\zeta}|\bar\Lambda_{0,1}\rangle_Q &= |\Lambda_{0,1}\rangle_Q,\end{aligned} \tag{13}$$

taking into account (12) and (13), instead of (10) and (11) we obtain

$$\begin{aligned}|\Psi_0\rangle_{XYQ} &= |0_L\rangle_X \otimes \sqrt{1-\zeta}[\sqrt{1-Q}|0_L\rangle_Y \otimes |\bar\Phi_0\rangle_Q\\ &+ \sqrt{Q}|1_L\rangle_Y \otimes |\bar\Theta_0\rangle_Q] + \sqrt{\zeta}|c_L\rangle_Y \otimes |\bar\Lambda_0\rangle_Q,\end{aligned} \tag{14}$$

$$\begin{aligned}|\Psi_1\rangle_{XYQ} &= |1_L\rangle_X \otimes \sqrt{1-\zeta}[\sqrt{1-Q}|1_L\rangle_Y \otimes |\bar\Phi_1\rangle_Q\\ &+ \sqrt{Q}|0_L\rangle_Y \otimes |\bar\Theta_1\rangle_Q] + \sqrt{\zeta}|c_L\rangle_Y \otimes |\bar\Lambda_1\rangle_Q.\end{aligned} \tag{15}$$

A measurement at the receiving station in the basis L is given by the resolution of identity:

$$I_Y = |0_L\rangle_{YY}\langle 0_L| + |1_L\rangle_{YY}\langle 1_L| + |c_L\rangle_{YY}\langle c_L|, \tag{16}$$

where $|c_L\rangle_Y = |1\rangle_3$ is a state in time window 3 in the basis L. A similar resolution of identity, describing a measurement in the basis R, has the form

$$I_Y = |0_R\rangle_{YY}\langle 0_R| + |1_R\rangle_{YY}\langle 1_R| + |c_R\rangle_{YY}\langle c_R|, \tag{17}$$

where $|c_R\rangle_Y = |1\rangle_1$ is a state in time window 3 in the basis R.

In what follows, we omit the index L for brevity. After measurements in the corresponding basis, we obtain the following expression for the Alice–Bob–Eve density matrix:

$$\begin{aligned}\rho_{XYQ} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-\zeta)[(1-Q)|0\rangle_{YY}\langle 0|\\ &\otimes |\bar\Phi_0\rangle_{QQ}\langle\bar\Phi_0| + Q|1\rangle_{YY}\langle 1| \otimes |\bar\Theta_0\rangle_{QQ}\langle\bar\Theta_0|] + \zeta|c\rangle_{YY}\langle c|\\ &\otimes |\bar\Lambda_0\rangle_{QQ}\langle\Lambda_0|] + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-\zeta)[(1-Q)|1\rangle_{YY}\langle 1|\\ &\otimes |\bar\Phi_1\rangle_{QQ}\langle\bar\Phi_1|] + Q|0\rangle_{YY}\langle 0| \otimes |\bar\Theta_1\rangle_{QQ}\langle\bar\Theta_1|]\\ &+ \zeta|c\rangle_{YY}\langle c| \otimes |\bar\Lambda_1\rangle_{QQ}\langle\bar\Lambda_1|].\end{aligned} \tag{18}$$

The density matrix (18) should be given a physical interpretation. With probability 1/2, Alice sends a state corresponding to 0 to the channel, and, with probability 1/2, she sends a state corresponding to 1.

Suppose that Alice sends the state $|0\rangle_{YY}\langle 0|$ in the basis L (the reference state $|0\rangle_{XX}\langle 0|$ remains at Alice's disposal). After Eve's attack and Bob's measurements on the receiver side, Bob sees with probability $(1-\zeta)(1-Q)$ the state $|0\rangle_{YY}\langle 0|$, which will give the correct outcome of measurements. Bob will interpret the outcome of measurements as logical 0. In this case, Eve has the state $|\bar\Phi_0\rangle_{QQ}\langle\bar\Phi_0|$ at her disposal.

Further, with probability $(1-\zeta)Q$, Bob sees the state $|1\rangle_{YY}\langle 1|$, which gives an erroneous outcome of measurements. Bob will interpret the outcome of the measurements as logical 1. In this case, Eve will have the state $|\bar\Theta_0\rangle_{QQ}\langle\bar\Theta_0|$ at her disposal.

The total probability of counts, both correct and erroneous, in information time windows 1 and 2 is $(1-\zeta)(1-Q) + (1-\zeta)Q = 1-\zeta$. In addition to the counts in the information time windows 1 and 2, the perturbed states will give counts in the control time window 3 in the basis L (respectively, in the control window 1 in the basis R). The unperturbed states in the basis L never give counts in the control time window 3.

The probability of counts in the control time window 3 is ζ. In this case, Eve has the state $|\bar{\Lambda}_0\rangle_{QQ}\langle\bar{\Lambda}_0|$ at her disposal. As a result, the total probability of counts in the information and control time windows is $1-\zeta+\zeta=1$.

We emphasize that information leakage to the eavesdropper is determined not only by the error in information time windows but also by the count probability in the control time window (see details in [10, 11]). To calculate the information leakage to Eve, one needs to know (measure) the probability of counts in the control time window 3.

Since the key is obtained only from the counts in information windows, in what follows it is convenient to pass to the reduced density matrix—the matrix normalized by the probability of counts in information time windows. We obtain (omitting the index L in Bob's states)

$$\begin{aligned}\bar{\rho}_{XYQ} &= \frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-Q)|0\rangle_{YY}\langle 0|\\ &\otimes|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0|+Q|1\rangle_{YY}\langle 1|\otimes|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|]\\ &+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-Q)|1\rangle_{YY}\langle 1|\\ &\otimes|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|+Q|0\rangle_{YY}\langle 0|\otimes|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{19}$$

Accordingly, for the Alice–Eve density matrix we obtain

$$\begin{aligned}\bar{\rho}_{XQ} &= \frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-Q)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0|\\ &+Q|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|]+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-Q)|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|\\ &+Q|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{20}$$

The Alice–Bob density matrix has the form

$$\begin{aligned}\bar{\rho}_{XY} &= \frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-Q)|0\rangle_{YY}\langle 0|+Q|1\rangle_{YY}\langle 1|]\\ &+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-Q)|1\rangle_{YY}\langle 1|+Q|0\rangle_{YY}\langle 0|].\end{aligned} \tag{21}$$

The density matrix that is seen by Eve is

$$\begin{aligned}\bar{\rho}_{Q} &= \frac{1}{2}|(1-Q)[|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0|+|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|]\\ &+\frac{1}{2}Q[|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|+|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{22}$$

Similarly, the density matrix that is seen by Bob is

$$\bar{\rho}_{Y} = \frac{1}{2}[|0\rangle_{YY}\langle 0|+|1\rangle_{YY}\langle 1|]. \tag{23}$$

An estimate of the secret key length in the asymptotic limit for error correction by random Shannon codes is given by (see details in [2])

$$\ell = H(\bar{\rho}_{XQ}\mid\bar{\rho}_{Q})-H(\bar{\rho}_{XY}\mid\bar{\rho}_{Y}), \tag{24}$$

where the von Neumann conditional entropies are

$$\begin{aligned}H(\bar{\rho}_{XQ}\mid\bar{\rho}_{Q}) &= H(\bar{\rho}_{XQ})-H(\bar{\rho}_{Q}),\\ H(\bar{\rho}_{XY}\mid\bar{\rho}_{Y}) &= H(\bar{\rho}_{XY})-H(\bar{\rho}_{Y}).\end{aligned} \tag{25}$$

Taking into account (19)–(25), we obtain

$$\begin{aligned}H(\bar{\rho}_{XQ}) &= 1+h(Q),\\ H(\bar{\rho}_{Q}) &= h\left(\frac{\zeta}{1-\zeta}\right)+h(Q),\\ H(\bar{\rho}_{XQ}\mid\bar{\rho}_{Q}) &= 1-h\left(\frac{\zeta}{1-\zeta}\right),\end{aligned} \tag{26}$$

$$\begin{aligned}H(\bar{\rho}_{XY}) &= 1+h(Q),\quad H(\bar{\rho}_{Y}) = 1,\\ H(\bar{\rho}_{XY}\mid\bar{\rho}_{Y}) &= h(Q).\end{aligned} \tag{27}$$

Taking into account (24), we obtain the following expression for estimating the secret key length:

$$\ell = \left[1-h\left(\frac{\zeta}{1-\zeta}\right)\right]-h(Q). \tag{28}$$

If the error correction is performed by constructive codes, then the last term in (28) must be replaced by leak(Q):

$$\begin{aligned}\ell &= \left[1-h\left(\frac{\zeta}{1-\zeta}\right)\right]-\mathrm{leak}(Q)\\ &= [1-\chi_{\mathrm{Hol}}(\zeta)]-\mathrm{leak}(Q),\end{aligned} \tag{29}$$

where leak(Q) is the information leakage during error correction, which depends on the total error.

Formula (29) has an intuitively transparent interpretation. It implies that the protocol is a two-parameter protocol and the length of the secret key depends not only on the observed error Q in information time windows but also on the probability of counts ζ in the control time windows. This reason can be easily understood by an example of the simplest intercept–resend attack. The states from different bases L and R are nonorthogonal; they overlap in time window 2 (see Fig. 1). Eve does not know the basis, so the resending of states in a wrong basis will inevitably lead to counts in the control time window, where they should not be present. For example, if the basis of Alice and Bob is L and Eve resends the states in the basis R, then this leads to counts in the control time window 3. Similarly, for the measurement basis R of Alice and Bob, resending of states in the basis L leads to counts in the control time window 1, where they should not be present. Of course, the intercept–resend attack is not the most common attack. The most common attack on single-photon states is the unitary attack (9)–(11).

3. DETECTION OF THE SIDE RADIATION OF THE TRANSMITTING EQUIPMENT

The eavesdropper can obtain information about the transmitted key not only from the quantum communication channel, but also using side channels of information leakage. In this case, obtaining information from these channels does not lead to the distor-

tion of information states and errors on the receiver side. Side channels of leakage are an informational "free bonus." One of these channels is the side electromagnetic radiation of the transmitting equipment. When the equipment prepares the state $|0\rangle_{XX}\langle 0|$, a quantum state $|e_0\rangle_{SS}\langle e_0|$ arises outside Alice's transmitting station. If the equipment prepares the state $|1\rangle_{XX}\langle 1|$, then this leads to the emission of the state $|e_0\rangle_{SS}\langle e_0|$. The states corresponding to 0 and 1 in the side channel can be considered orthogonal, and their indistinguishability can be taken into account in the discrimination probability p. Effectively, the eavesdropper sees in the side channel the density matrix $(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|$, which is interpreted as follows: with probability $1-p$, the eavesdropper sees the state $|0\rangle_{XX}\langle 0|$ and believes that Alice has prepared bit 0. In this case, Eve recognizes the key bit by measuring the side radiation. With probability p, Eve detects the state $|1\rangle_{XX}\langle 1|$ and believes that Alice has prepared bit 1, that is, Eve makes an error with probability p, and similarly if Alice prepared bit 1. Taking into account the aforesaid, we can rewrite the Alice–Bob–Eve density matrix as

$$\begin{aligned}\rho_{XYQS} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|] \\ &\otimes [(1-\zeta)(1-Q)|0\rangle_{YY}\langle 0| \otimes |\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| \\ &+ (1-\zeta)Q|1\rangle_{YY}\langle 1| \otimes |\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| + \zeta|c\rangle_{YY}\langle c| \\ &\otimes |\bar{\Lambda}_0\rangle_{QQ}\langle\bar{\Lambda}_0|] \\ &+ \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| + p|e_0\rangle_{SS}\langle e_0|] \\ &\otimes [(1-\zeta)(1-Q)|1\rangle_{YY}\langle 1| \otimes |\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1| \\ &+ (1-\zeta)Q|0\rangle_{YY}\langle 0| \otimes |\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1| \\ &+ \zeta|c\rangle_{YY}\langle c| \otimes |\bar{\Lambda}_1\rangle_{YY}\langle\bar{\Lambda}_1|].\end{aligned} \tag{30}$$

In order not to complicate the calculations, in (30) the side channel of information leakage is assumed to be symmetric for preparing 0 and 1. A generalization to the asymmetric case is done in a similar way. Passing to the reduced density matrix, we have

$$\begin{aligned}\bar{\rho}_{XYQS} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|] \\ &\otimes [(1-Q)|0\rangle_{YY}\langle 0| \otimes |\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| \\ &+ Q|1\rangle_{YY}\langle 1| \otimes |\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|] + \frac{1}{2}|1\rangle_{XX}\langle 1| \\ &\otimes [(1-p)|e_1\rangle_{SS}\langle e_1| + p|e_0\rangle_{SS}\langle e_0|] \\ &\otimes [(1-Q)|1\rangle_{YY}\langle 1| + |\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1| \\ &+ Q|0\rangle_{YY}\langle 0| + |\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|],\end{aligned} \tag{31}$$

$$\begin{aligned}\bar{\rho}_{XY} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-Q)|0\rangle_{YY}\langle 0| + Q|1\rangle_{YY}] \\ &+ \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-Q)|1\rangle_{YY}\langle 1| + Q|0\rangle_{YY}\langle 0|].\end{aligned} \tag{32}$$

Bob's density matrix is expressed as

$$\bar{\rho}_Y = \frac{1}{2}|0\rangle_{YY}\langle 0| + \frac{1}{2}|1\rangle_{YY}\langle 1|. \tag{33}$$

The conditional entropy has the form

$$H(\bar{\rho}_{XY} \mid \bar{\rho}_Y) = H(\bar{\rho}_{XY}) - H(\bar{\rho}_Y) = h(Q), \tag{34}$$

where $h(x) = -x\log(x) - (1-x)\log(1-x)$, $\log \equiv \log_2$.

Let us calculate the Alice–Eve density matrix:

$$\begin{aligned}\bar{\rho}_{XQS} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| \\ &+ p|e_1\rangle_{SS}\langle e_1|] \otimes [(1-Q)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + Q|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|] \\ &+ \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| + p|e_0\rangle_{SS}\langle e_{00}|] \\ &\otimes [(1-Q)|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1| + Q|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{35}$$

Eve's density matrix is expressed as

$$\begin{aligned}\bar{\rho}_{QS} &= \frac{1}{2}(1-Q)[(1-p)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + p|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|] \\ &\otimes |e_0\rangle_{SS}\langle e_0| + \frac{1}{2}(1-Q)[p|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + (1-p)|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|] \\ &\otimes |e_1\rangle_{SS}\langle e_1| + \frac{1}{2}Q[(1-p)|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| \\ &+ p|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|] \otimes |e_0\rangle_{SS}\langle e_0| + \frac{1}{2}Q[p|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| \\ &+ (1-p)|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|] \otimes |e_1\rangle_{SS}\langle e_1|.\end{aligned} \tag{36}$$

The eigenvalues of $\bar{\rho}_{XQS}$ are

$$\frac{1}{2}(1-p)(1-Q), \quad \frac{1}{2}(1-p)Q, \quad \frac{1}{2}p(1-Q), \quad \frac{1}{2}pQ \tag{37}$$

and are doubly degenerate. The entropy $H(\bar{\rho}_{XQS})$ is

$$H(\bar{\rho}_{XQS}) = 1 + h(p) + h(Q). \tag{38}$$

Eve's density matrix takes the form

$$\begin{aligned}\bar{\rho}_{QS} &= \frac{1}{2}(1-Q)[(1-p)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + p|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|] \\ &\otimes |e_0\rangle_{SS}\langle e_0| + \frac{1}{2}(1-Q)[p|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + (1-p)|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|] \\ &\otimes |e_1\rangle_{SS}\langle e_1| + \frac{1}{2}(1-Q)[(1-p)|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| \\ &+ p|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|] \otimes |e_0\rangle_{SS}\langle e_0| + \frac{1}{2}(1-Q)[p|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| \\ &+ (1-p)|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|] \otimes |e_1\rangle_{SS}\langle e_1|.\end{aligned} \tag{39}$$

Taking into account that (see [10, 11] for details)

$$\begin{aligned}{}_Q\langle\bar{\Theta}_{0,1} \mid \bar{\Theta}_{0,1}\rangle_Q &= {}_Q\langle\bar{\Phi}_{0,1} \mid \bar{\Phi}_{0,1}\rangle_Q = \varepsilon(\zeta), \\ \varepsilon(\zeta) &= 1 - 2\kappa(\zeta), \quad \kappa(\zeta) = \frac{\zeta}{1-\zeta},\end{aligned} \tag{40}$$

it suffices to diagonalize the terms in each individual square bracket. For the first bracket, the eigenvalue problem gives

$$[(1-p)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + p|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|] - \lambda I = 0, \quad (41)$$

where I is the identity operator in the subspace spanned by $\{|\bar{\Phi}_0\rangle_Q, |\bar{\Phi}_0\rangle_Q\}$; in the basis of these vectors, the determinant of the secular equation has the form

$$\mathrm{Det}\begin{pmatrix} (1-p)+p\varepsilon(\zeta)^2-\lambda & (1-p)\varepsilon(\zeta)+p\varepsilon(\zeta)-\lambda\varepsilon(\zeta) \\ (1-p)\varepsilon(\zeta)+p\varepsilon(\zeta)-\lambda\varepsilon(\zeta) & (1-p)\varepsilon(\zeta)^2+p-\lambda \end{pmatrix} = 0. \quad (42)$$

The roots of (42) are given by

$$\lambda_\pm(\zeta, p) = \frac{1 \pm \varepsilon(\zeta, p)}{2},$$
$$\varepsilon(\zeta, p) = \sqrt{1 - 4\frac{[(1-p)+p\varepsilon(\zeta)^2][(1-p)\varepsilon(\zeta)^2+p] - \varepsilon(\zeta)^2}{1-\varepsilon(\zeta)^2}}. \quad (43)$$

Carrying out similar calculations for other terms, we obtain a complete set of eigenvalues

$$\frac{1}{2}(1-Q)\frac{1+\varepsilon(\zeta, p)}{2}, \quad \frac{1}{2}(1-Q)\frac{1-\varepsilon(\zeta, p)}{2}, \quad \frac{1}{2}Q\frac{1+\varepsilon(\zeta, p)}{2}, \quad \frac{1}{2}Q\frac{1-\varepsilon(\zeta, p)}{2}, \quad (44)$$

which are doubly degenerate. The von Neumann entropy $\bar{\rho}_{QS}$ is equal to

$$H(\bar{\rho}_{XS}) = 1 + h(Q) + \chi\left(\frac{1 \pm \varepsilon(\zeta, p)}{2}\right), \quad (45)$$

where χ is the Holevo information [12–14],

$$\chi\left(\frac{1 \pm \varepsilon(\zeta, p)}{2}\right) = -\frac{1+\varepsilon(\zeta, p)}{2}\log\left(\frac{1+\varepsilon(\zeta, p)}{2}\right) - \frac{1-\varepsilon(\zeta, p)}{2}\log\left(\frac{1-\varepsilon(\zeta, p)}{2}\right). \quad (46)$$

Finally, taking into account (40)–(46), we obtain the following expression for the conditional entropy:

$$H(\bar{\rho}_{XQS} \mid \bar{\rho}_{QS}) = h(p) - \chi\left(\frac{1 \pm \varepsilon(\zeta, p)}{2}\right). \quad (47)$$

Accordingly, for the key length we obtain

$$\ell = H(\bar{\rho}_{XQS} \mid \bar{\rho}_{QS}) - H(\bar{\rho}_{XY} \mid \bar{\rho}_Y) = h(p) - \chi\left(\frac{1 \pm \varepsilon(\zeta, p)}{2}\right) - h(Q) = [1 - \chi_{\mathrm{Hol}}(\zeta, p)] - h(Q). \quad (48)$$

Note that the information leakage in (48) during error correction corresponds to the Shannon limit. When correcting errors by constructive codes, the last term in (48) should be replaced by leak, the number of bits per message spent on error correction.

It is important that, in formula (48), the lower bound for Eve's lack of information admitted by the fundamental laws of quantum theory is expressed in terms of conditional entropy. This lower bound is attained on the collective joint measurements of Eve, which implies joint collective measurements of Eve over quantum states in the side channel and over distorted ancilla states in the quantum communication channel.

Formula (48) has a simple interpretation. If the probability of distinguishing between states 0 and 1 in the side channel is $p = 1/2$, then $h(p) = 1$, and expression (48) turns into expression (28) for the key length without taking into account the side channel of information leakage. If $p = 0$, then Eve reliably distinguishes between states 0 and 1 in the side channel and knows the transmitted key bits even without intruding into the quantum communication channel and without making errors ($Q = 0$) on the receiver side. In this case, $h(p) = 0$, and the length of the secret key turns out to be formally negative; i.e., the secret key cannot be distributed. Thus, the leakage of information through the side communication channel reduces the length of the secret key. To reduce information leakage through this side channel, the transmitting station should be effectively shielded. The discrimination parameters of the state p must be determined experimentally for each specific implementation of the quantum cryptography system.

4. ACTIVE PROBING OF THE PHASE MODULATOR STATE AT THE TRANSMITTING STATION

The eavesdropper can probe the state of the phase modulator at the transmitting station through the fiber-optic communication line. The state of the phase modulator is uniquely related to the key bit transmitted by Alice. Eve has at her disposal an additional quantum state correlated with the state of the phase modulator. In favor of Eve, we can assume that the reflected states are pure, which increases their distinguishability. Our method allows us to take into

account not only pure reflected states but also the density matrices. Pure states are chosen in order not to overload the calculations with insignificant technical details.

The intensity of the reflected probing states is not known exactly, but the intensity of the input probing states can be limited by input fiber-optic isolators with known backward transmission. The input intensity of the probing radiation is limited, since it cannot exceed the critical intensity at which the fiber melts. By choosing a proper backward transmission of the optical isolator, one can limit the output intensity of reflected states to the required value.

In an attack with active probing of the state of the equipment by external radiation, we should introduce another side channel. Formally, this reduces to introducing quantum states correlated with Alice's state. We obtain

$$|0\rangle_X \to |0\rangle_X \otimes |\lambda_0\rangle_T, \quad |1\rangle_X \to |1\rangle_X \otimes |\lambda_1\rangle_T. \tag{49}$$

For the density matrix, instead of (30) we obtain

$$\begin{aligned}\bar{\rho}_{XYQT} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|0\rangle_{YY}\langle 0| \\ &\otimes |\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + |1\rangle_{YY}\langle 1| \otimes |\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|] \\ &+ \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|1\rangle_{YY}\langle 1| \\ &\otimes [|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1| + |0\rangle_{YY}\langle 0| \otimes |\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{50}$$

The Alice–Eve density matrix takes the form

$$\begin{aligned}\bar{\rho}_{XQT} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes [|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| \\ &+ |\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|] + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \\ &\otimes [|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1| + |\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{51}$$

Taking into account the normalization (13), (40), we can rewrite the eigenvalues as

$$\frac{1}{2}(1-Q), \quad \frac{1}{2}Q, \quad \frac{1}{2}(1-Q), \quad \frac{1}{2}Q. \tag{52}$$

For the entropy, we find

$$H(\bar{\rho}_{XQT}) = 1 + h(Q). \tag{53}$$

To calculate the eigenvalues, we should diagonalize the density matrix $\bar{\rho}_{QT}$; we obtain

$$\begin{aligned}\bar{\rho}_{QT} &= \frac{1}{2}(1-Q)[|\lambda_0\rangle_{TT}\langle\lambda_0| \otimes |\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| \\ &+ |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes |\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|] + \frac{1}{2}Q[|\lambda_0\rangle_{TT}\langle\lambda_0| \\ &\otimes |\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| + |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes |\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{54}$$

If the probing occurs by coherent states whose phase is uniquely linked, conservatively in favor of Eve, to the state of the phase modulator, i.e., if the phase is equal to either 0 ($|\lambda_0\rangle_T = |\sqrt{\mu_T}\,\rangle_T$ or π ($|\lambda_1\rangle_T = |-\sqrt{\mu_T}\,\rangle_T$) depending on the transmitted bit, then we obtain $|_T\langle\lambda_0|\lambda_1\rangle_T| = \eta = e^{-2\mu_T}$ for the scalar product of the reflected states. With this in mind, we find the secular equation for the first term in (54):

$$\mathrm{Det}\begin{pmatrix} \dfrac{1+\eta^2\varepsilon(\zeta)^2}{2} - \lambda & 2\eta\varepsilon(\zeta) - \lambda\eta\varepsilon(\zeta) \\ 2\eta\varepsilon(\zeta) - \lambda\eta\varepsilon(\zeta) & \dfrac{1+\eta^2\varepsilon(\zeta)^2}{2} - \lambda \end{pmatrix} = 0. \tag{55}$$

Taking into account the secular equation, we can write the eigenvalues of the density matrix as

$$\begin{aligned}&(1-Q)\frac{1+\eta\varepsilon(\zeta)}{2}, \quad (1-Q)\frac{1-\eta\varepsilon(\zeta)}{2}, \\ &Q\frac{1+\eta\varepsilon(\zeta)}{2}, \quad Q\frac{1-\eta\varepsilon(\zeta)}{2}.\end{aligned} \tag{56}$$

For the entropy $H(\bar{\rho}_{QT})$, we obtain

$$H(\bar{\rho}_{QT}) = h(Q) + \chi\left(\frac{1\pm\eta\varepsilon(\zeta)}{2}\right), \tag{57}$$

where the Holevo information is [12–14]

$$\begin{aligned}\chi\left(\frac{1\pm\eta\varepsilon(\zeta)}{2}\right) &= -\frac{1+\eta\varepsilon(\zeta)}{2}\log\left(\frac{1+\eta\varepsilon(\zeta)}{2}\right) \\ &-\frac{1-\eta\varepsilon(\zeta)}{2}\log\left(\frac{1-\eta\varepsilon(\zeta)}{2}\right).\end{aligned} \tag{58}$$

Finally, taking into account (53) and (57), we obtain the following expression for the length of the secret key:

$$\begin{aligned}\ell &= H(\bar{\rho}_{XQT} \mid \bar{\rho}_{QT}) - H(\bar{\rho}_{XY} \mid \bar{\rho}_Y) \\ &= 1 - \chi\left(\frac{1\pm\eta\varepsilon(\zeta)}{2}\right) - h(Q) \\ &= [1 - \chi_{\mathrm{Hol}}(\zeta,\eta)] - h(Q).\end{aligned} \tag{59}$$

The smaller the average number of photons μ_T in the reflected states, the larger the scalar product η: the states stick together stronger, and therefore the reflected states are less distinguishable. As $\eta \to 1$ ($\mu_T \to 0$), the states stick together completely and are completely indistinguishable. For small μ_T, the length of the secret key decreases and becomes equal to

$$\begin{aligned}\ell &= 1 - h(\varepsilon(\zeta) + O(\mu_T)) - h(Q) \\ &= 1 - h\left(\frac{\zeta}{1-\zeta} + O(\mu_T)\right) - h(Q) \\ &< 1 - h\left(\frac{\zeta}{1-\zeta}\right) - h(Q),\end{aligned} \tag{60}$$

which is less than the length without probing the phase modulator. We also note that the lower bound for the lack of eavesdropper's information, which is expressed in terms of the conditional entropy, is attained in joint collective measurements of reflected quantum states and of the ancilla quantum states under an attack on information quantum states in the communication channel.

5. JOINT DETECTION OF SIDE RADIATION AND ACTIVE PROBING OF THE PHASE MODULATOR STATE AT THE TRANSMITTING STATION

Consider a combined attack with the detection of side radiation of the transmitting station and active probing of the phase modulator. To this end, we have to include quantum states in both side channels of information leakage in the density matrix. Taking into account formulas (30) and (50), we rewrite the Alice–Eve density matrix for the combined attack as

$$\begin{aligned}\bar{\rho}_{XQST} &= \frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|]\\ &\otimes|\lambda_0\rangle_{TT}\langle\lambda_0|\otimes[|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| + |\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|]\\ &+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[p|e_0\rangle_{SS}\langle e_0| + (1-p)|e_1\rangle_{SS}\langle e_1|]\\ &\otimes|\lambda_1\rangle_{TT}\langle\lambda_1|\otimes[|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1| + |\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|].\end{aligned} \tag{61}$$

The calculation of the entropy for the density matrix (61) yields

$$H(\bar{\rho}_{XQST}) = 1 + h(p) + h(Q). \tag{62}$$

Further, with regard to (61), the partial density matrix that Eve has at her disposal is expressed as

$$\begin{aligned}\bar{\rho}_{QST} &= \frac{1}{2}(1-Q)[(1-p)|\lambda_0\rangle_{TT}\langle\lambda_0|\otimes|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0|\\ &+ p|\lambda_1\rangle_{TT}\langle\lambda_1|\otimes|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|]\otimes|e_0\rangle_{SS}\langle e_0|\\ &+\frac{1}{2}(1-Q)[p|\lambda_0\rangle_{TT}\langle\lambda_0|\otimes|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0|\\ &+(1-p)|\lambda_1\rangle_{TT}\langle\lambda_1|\otimes|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|\otimes|e_1\rangle_{SS}\langle e_1|\\ &+\frac{1}{2}Q[(1-p)|\lambda_0\rangle_{TT}\langle\lambda_0|\otimes|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|\\ &+ p|\lambda_1\rangle_{TT}\langle\lambda_1|\otimes|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|]\otimes|e_0\rangle_{SS}\langle e_0|\\ &+\frac{1}{2}Q[p|\lambda_0\rangle_{TT}\langle\lambda_0|\otimes|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| + (1-p)|\lambda_1\rangle_{TT}\langle\lambda_1|\\ &\otimes|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1|] + |e_1\rangle_{TT}\langle e_1|.\end{aligned} \tag{63}$$

Similar to the previous case (see (42), (55)), the secular equation for the eigenvalues of the density matrix (63) is expressed as

$$\mathrm{Det}\begin{pmatrix}(1-p)+p\eta^2\varepsilon(\zeta)^2-\lambda & (1-p)\eta\varepsilon(\zeta)+p\eta\varepsilon(\zeta)-\lambda\eta\varepsilon(\zeta)\\ (1-p)\eta\varepsilon(\zeta)+p\eta\varepsilon(\zeta)-\lambda\eta\varepsilon(\zeta) & (1-p)\eta^2\varepsilon(\zeta)^2+p-\lambda\end{pmatrix} = 0. \tag{64}$$

Taking into account the secular equation (64), we have the eigenvalues of (63):

$$\begin{gathered}\frac{1}{2}(1-Q)\left(\frac{1+\varepsilon(\zeta,\eta,p)}{2}\right),\\ \frac{1}{2}(1-Q)\left(\frac{1-\varepsilon(\zeta,\eta,p)}{2}\right),\\ \frac{1}{2}Q\left(\frac{1+\varepsilon(\zeta,\eta,p)}{2}\right),\quad \frac{1}{2}Q\left(\frac{1-\varepsilon(\zeta,\eta,p)}{2}\right),\end{gathered} \tag{65}$$

where

$$\varepsilon(\zeta,\eta,p) = \sqrt{1-4\frac{[(1-p)+p\eta^2\varepsilon(\zeta)^2][(1-p)\eta^2\varepsilon(\zeta)^2+p]-\eta^2\varepsilon(\zeta)^2}{1-\eta^2\varepsilon(\zeta)^2}}. \tag{66}$$

Taking into account (65), we obtain the following expression for the entropy $H(\bar{\rho}_{QST})$:

$$H(\bar{\rho}_{QST}) = 1 + h(Q) + \chi\left(\frac{1\pm\varepsilon(\zeta,\eta,p)}{2}\right), \tag{67}$$

where the Holevo information is [12–14]

$$\begin{aligned}\chi\left(\frac{1\pm\varepsilon(\zeta,\eta,p)}{2}\right) &= -\frac{1+\varepsilon(\zeta,\eta,p)}{2}\log\left(\frac{1+\varepsilon(\zeta,\eta,p)}{2}\right)\\ &-\frac{1-\varepsilon(\zeta,\eta,p)}{2}\log\left(\frac{1-\varepsilon(\zeta,\eta,p)}{2}\right).\end{aligned} \tag{68}$$

Combining formulas (62) and (67), we finally obtain the following expression for the length of the secret key:

$$\begin{aligned}\ell &= H(\bar{\rho}_{XQST}\mid\bar{\rho}_{QST}) - H(\bar{\rho}_{XY}\mid\bar{\rho}_Y)\\ &= h(p) - \chi\left(\frac{1\pm\varepsilon(\zeta,\eta,p)}{2}\right) - h(Q)\\ &= [1-\chi_{\mathrm{Hol}}(\zeta,p,\eta)] - h(Q).\end{aligned} \tag{69}$$

6. JOINT DETECTION OF SIDE RADIATION, ACTIVE PROBING OF THE PHASE MODULATOR OF THE TRANSMITTING STATION, AND DETECTION OF THE BACKWARD RADIATION OF AVALANCHE DETECTORS ON THE RECEIVER SIDE

Taking into account the above-mentioned side channels of information leakage, we can represent the Alice–Bob–Eve density matrix as

$$\rho_{XYSQTD} = \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|]$$
$$\otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes \{(1-Q)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| \otimes [(1-d)|d_0\rangle_{DD}\langle d_0|$$
$$+ d|d_1\rangle_{DD}\langle d_1|] \otimes |0\rangle_{YY}\langle 0| + Q|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|$$
$$\otimes [(1-d)|d_1\rangle_{DD}\langle d_1| + d|d_0\rangle_{DD}\langle d_0|]$$
$$\otimes |1\rangle_{YY}\langle 1|\} + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| \qquad (70)$$
$$+ p|e_0\rangle_{SS}\langle e_0|] \otimes |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes \{(1-Q)|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|$$
$$\otimes [(1-d)|d_1\rangle_{DD}\langle d_1| + d|d_0\rangle_{DD}\langle d_0|] \otimes |1\rangle_{YY}\langle 1|$$
$$+ Q|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1| \otimes [(1-d)|d_0\rangle_{DD}\langle d_0|$$
$$+ d|d_1\rangle_{DD}\langle d_1|] \otimes |0\rangle_{YY}\langle 0|\}.$$

The density matrix has a simple interpretation. The detection of the states $|0\rangle_{YY}\langle 0|$ or $|1\rangle_{YY}\langle 1|$ on the receiver side is performed by two avalanche detectors (see Fig. 1). When the detector is triggered, an avalanche of carriers is formed; the recombination of these carriers may give rise to backward radiation into the fiber-optic communication channel, which can be detected by Eve. To take into account such radiation, it is necessary to introduce one more side leakage channel, more precisely, a quantum state associated with backward radiation.

If, for example, the state $|0\rangle_{YY}\langle 0|$ is detected, then this gives rise to the state $[(1-d)|d_0\rangle_{DD}\langle d_0| + d|d_1\rangle_{DD}\langle d_1|]$ of the density matrix in the side channel. Informally, this means that, with probability $1-d$, Eve will have the state $|d_0\rangle_{DD}\langle d_0|$ at her disposal and, with probability d, she will have the state $|d_1\rangle_{DD}\langle d_1|$. The states $|d_0\rangle_{DD}\langle d_0|$ and $|d_1\rangle_{DD}\langle d_1|$ can be considered orthogonal (in order not to overload the calculations with insignificant details); then, with probability of $1-d$, Eve correctly recognizes the detected key bit by detecting the backward radiation, but, with probability d, she makes an error. The probability of discrimination is included in the probability d. The states in the side channel are taken into account in a similar way when 1 is detected. Note that we consider a symmetric situation in the side channel. This is done solely to save mathematical calculations. It is not difficult to generalize the calculations to the case when the states and probabilities when detecting 0 and 1 are different.

The implementation of the phase–time coding protocol (see Fig. 1) does not involve a phase modulator on the receiver side; therefore, there is no side channel of information leakage associated with probing the phase modulator on the receiver side. The absence of a phase modulator is due to the use of the phase–time coding protocol, which makes the system robust against such an attack compared to other systems.

When detecting 0 or 1, the state of the electronic equipment of the receiving station is different; therefore, the side electromagnetic radiation associated with the operation of the electronics is also different. Electromagnetic radiation can be detected by Eve. The side channel associated with the electromagnetic radiation of the electronic equipment of the receiving station during detecting 0 and 1 can be included in the states $|d_0\rangle_{DD}\langle d_0|$ and $|d_1\rangle_{DD}\langle d_1|$, which correspond to probabilities $d-1$ and d. With regard to (70), the Alice–Eve density matrix is given by a partial trace over Bob's state space; we obtain

$$\rho_{XSQTD} = \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes [(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|]$$
$$\otimes |\lambda_0\rangle_{TT}\langle\lambda_0| \otimes \{(1-Q)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| \otimes [(1-d)|d_0\rangle_{DD}\langle d_0|$$
$$+ d|d_1\rangle_{DD}\langle d_1|] \otimes |0\rangle_{YY}\langle 0| + Q|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0|$$
$$\otimes [(1-d)|d_1\rangle_{DD}\langle d_1| + d|d_0\rangle_{DD}\langle d_0|]\}$$
$$+ \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| \qquad (71)$$
$$+ p|e_0\rangle_{SS}\langle e_0|] \otimes |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes \{(1-Q)|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|$$
$$\otimes [(1-d)|d_1\rangle_{DD}\langle d_1| + d|d_0\rangle_{DD}\langle d_0|]$$
$$+ Q|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1| \otimes [(1-d)|d_0\rangle_{DD}\langle d_0| + d|d_1\rangle_{DD}\langle d_1|]\}.$$

The eigenvalues of (71) are

$$\frac{1}{2}(1-Q)(1-p)(1-d), \quad \frac{1}{2}Q(1-p)(1-d), \qquad (72)$$
$$\frac{1}{2}(1-Q)p(1-d), \quad \frac{1}{2}Qp(1-d),$$

$$\frac{1}{2}(1-Q)(1-p)d, \quad \frac{1}{2}Q(1-p)d, \qquad (73)$$
$$\frac{1}{2}(1-Q)pd, \quad \frac{1}{2}Qpd,$$

the eigenvalues are doubly degenerate. Taking into account (72) and (73), we obtain the following expression for the entropy:

$$H(\rho_{XSQTDD}) = 1 + h(p) + h(d) + h(Q). \qquad (74)$$

Let us proceed to calculating $H(\rho_{SQTD})$. For the density matrix ρ_{SQTD}, we find

$$\rho_{SQTD} = \frac{1}{2}[(1-p)|e_0\rangle_{SS}\langle e_0| + p|e_1\rangle_{SS}\langle e_1|]$$
$$\otimes |\lambda_0\rangle_{QQ}\langle\lambda_0| \otimes [(1-Q)|\bar{\Phi}_0\rangle_{QQ}\langle\bar{\Phi}_0| \otimes [(1-d)|d_0\rangle_{DD}\langle d_0|$$
$$+ d|d_1\rangle_{DD}\langle d_1|] + Q|\bar{\Theta}_0\rangle_{QQ}\langle\bar{\Theta}_0| \otimes [(1-d)|d_1\rangle_{DD}\langle d_1|$$
$$+ d|d_0\rangle_{DD}\langle d_0|]] + \frac{1}{2}[(1-p)|e_1\rangle_{SS}\langle e_1| \qquad (75)$$
$$+ p|e_0\rangle_{SS}\langle e_0|] \otimes |\lambda_1\rangle_{TT}\langle\lambda_1| \otimes [(1-Q)|\bar{\Phi}_1\rangle_{QQ}\langle\bar{\Phi}_1|$$
$$\otimes [(1-d)|d_1\rangle_{DD}\langle d_1| + d|d_0\rangle_{DD}\langle d_0|]$$
$$+ Q|\bar{\Theta}_1\rangle_{QQ}\langle\bar{\Theta}_1| \otimes [(1-d)|d_0\rangle_{DD}\langle d_0| + d|d_1\rangle_{DD}\langle d_1|]].$$

The eigenvalues of ρ_{SQTD} are given by the roots of the secular equations

$$\mathrm{Det}\begin{pmatrix} A_i - \lambda & \varepsilon(\zeta)\eta(C_i - \lambda) \\ \varepsilon(\zeta)\eta(C_i - \lambda) & B_i - \lambda \end{pmatrix} = 0, \qquad (76)$$

where

$$A_1 = (1-p)(1-d) + pd\varepsilon(\zeta)^2\eta^2,$$
$$B_1 = (1-p)(1-d)\varepsilon(\zeta)^2\eta^2 + pd, \quad (77)$$
$$C_1 = (1-p)(1-d) + pd,$$

$$A_2 = (1-p)d + p(1-d)\varepsilon(\zeta)^2\eta^2,$$
$$B_2 = (1-p)d\varepsilon(\zeta)^2\eta^2 + p(1-d), \quad (78)$$
$$C_2 = (1-p)d + p(1-d),$$

$$A_3 = p(1-d) + (1-p)d\varepsilon(\zeta)^2\eta^2,$$
$$B_3 = p(1-d)\varepsilon(\zeta)^2\eta^2 + (1-p)d, \quad (79)$$
$$C_3 = p(1-d) + (1-p)d,$$

$$A_4 = pd + (1-p)(1-d)\varepsilon(\zeta)^2\eta^2,$$
$$B_4 = pd\varepsilon(\zeta)^2\eta^2 + (1-p)(1-d), \quad (80)$$
$$C_4 = pd + (1-p)(1-d).$$

The roots of (76)–(80) are

$$\lambda_{i\pm} = \frac{1}{2(1-\varepsilon(\zeta)^2\eta^2)} \times\left[A_i + B_i - 2\varepsilon(\zeta)^2\eta^2 C_i \pm \sqrt{[A_i + B_i - 2\varepsilon(\zeta)^2\eta^2 C_i]^2 - 4[A_iB_i - \varepsilon(\zeta)^2\eta^2 C_i^2](1-\varepsilon(\zeta)^2\eta^2)}\right]. \quad (81)$$

The eigenvalues of (76)–(80) are

$$\frac{1}{2}(1-Q)\lambda_{i\pm}, \quad \frac{1}{2}Q\lambda_{i\pm}, \quad i = 1,2,3,4. \quad (82)$$

Introduce the notation

$$\chi_i(\zeta, p, d, \eta) = -\lambda_{i+}\log(\lambda_{i+}) - \lambda_{i-}\log(\lambda_{i-}),$$
$$\chi(\zeta, p, \eta, d) = \frac{1}{2}\sum_{i=1}^{4}\chi_i(\zeta, p, d, \eta). \quad (83)$$

For the conditional entropy, we obtain

$$H(\rho_{XSQTD} \mid \rho_{SQTD}) = h(p) + h(d) - \chi(\zeta, p, d, \eta). \quad (84)$$

As a result, taking into account (74) and (83), we have the following estimate for the length of the secret key in the strictly single-photon case:

$$\ell = \lim_{n\to\infty}\frac{\ell_n}{n} = h(p) + h(d) - \chi(\zeta, p, d, \eta) - h(Q) = [1 - \chi_{\mathrm{Hol}}(\zeta, p, d, \eta)] - h(Q), \quad (85)$$

where the information leakage during error correction is taken in the Shannon limit. During the correction with constructive codes, the last term on the right-hand side of (85) should be replaced by the real number of bits per position, which was found during error correction, $h(Q) \to$ leak.

Note once again that expression (85) for the secret key length takes into account the joint collective measurements of Eve over quantum states in side channels and in the quantum communication channel.

7. ACTIVE PROBING OF THE INTENSITY MODULATOR STATE AT THE TRANSMITTING STATION

Above, we obtained formulas for the length of the secret key, taking into account the side channels of information leakage when the states are strictly single-photon. In a real situation, information states in a quantum communication channel are a statistical mixture of different Fock (photon-number) states. We emphasize that the implementation of a system using a pulsed laser, which is turned on and off in each message on the transmitter side (see Fig. 1), leads to the randomization of the phases of information coherent states in different messages. It is for this reason that the quantum communication channel contains a statistical mixture of Fock states with Poisson statistics on the number of photons, rather than pure coherent states.

The secret key is composed solely of the single-photon component of the statistical mixture of states. Conservatively in favor of the eavesdropper, it is assumed that the information contained in the multi-photon components of states is known to the eavesdropper. Therefore, to estimate the fraction of the single-photon component of states that reaches the receiver side, one applies the decoy state method. In this method, states with different average numbers of photons are randomly sent to the quantum communication channel. A Fock state with k photons can be obtained from a state with any average number of photons. The key point of the decoy state method is the fact that, having found a Fock state with a given number of photons in a quantum communication channel, the eavesdropper cannot know from which state and with what average number of photons a given component of states occurs.

In active probing of the state of the intensity modulator, this condition is violated. The eavesdropper, albeit with some probability, knows from which state the component of Fock states with a given number of photons comes from. For this reason, the standard decoy state method does not work in the case of active probing of the intensity modulator. Below we clearly show at what stage this occurs.

The side channel of information leakage associated with active probing of the intensity modulator at the transmitting station is fundamentally different from other side channels. The probing states reflected from the intensity modulator do not carry direct information about the transmitted key bit, but only about the

intensity of a state—the average number of photons. Therefore, the reflected quantum states cannot be directly included in the Alice–Bob–Eve density matrix, in terms of which the conditional entropy and information leakage to the eavesdropper are calculated.

In the previous sections, we "linked" the states in the side channels of information leakage to the single-photon component of states. Naturally, side leakage channels also exist in the case when there are non-single-photon components of states in the quantum channel. However, since the information about the key bits contained in these components is assumed, conservatively in favor of the eavesdropper, to be known to Eve, there is no need to "link" the states in the side channels to the multiphoton components of information states.

The probing of the intensity modulator state, in contrast to probing the state of the phase modulator, does not give direct information about the transmitted key bit, but gives information only about the intensity of the transmitted state. The fraction of the single-photon component of the states and the error probability in it in the messages in which the information states were sent is estimated in terms of the change in the statistics of photocounts in the messages in which "decoy" states have been sent. Having additional information about what state is transmitted in a particular message—either information state or a decoy state—the eavesdropper can change her strategy for a given detected number k of photons. For example, if it is known that a decoy state has been sent, then the eavesdropper does nothing (behaves passively) and does not distort the statistics of photocounts of the decoy states.

Below we modify the decoy state method for the case of active probing of the intensity modulator informally, when the eavesdropper additionally has at her disposal a reflected quantum state that carries information about the state of the intensity modulator, and, hence, about the average number of photons.

Denote the probing quantum state reflected from the intensity modulator by $|\psi(\xi)\rangle_{S_M}$. Assume that this state depends only on the state of the intensity modulator, i.e., on which state with the average number of photons $\xi \in \mathcal{J} = \{\mu, \nu_1, \nu_2\}$ is sent to the communication channel. A generalization to the case when this state also depends on the state of the phase modulator is possible. However, in order not to overload the calculations, we give the derivation only for the former case.

When measuring the number of photons in a communication channel, instead of the state $|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|$, which does not depend on the average number of photons ξ, Eve has the state $|\Psi_k^x(\xi)\rangle_{BSBS}\langle\Psi_k^x(\xi)|$ at her disposal. This state contains information about the average number of photons, which is given by the presence of the reflected probing state $|\psi(\xi)\rangle_{S_M}$. This state gives Eve additional information about the intensity of the transmitted state. The information quantum state, together with the reflected probing state accessible to Eve, has the form

$$\rho^x(\xi) = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}|\Psi_k^x(\xi)\rangle_{BS_MBS_M}\langle\Psi_k^x(\xi)| = \sum_{k=0}^{\infty}P^{(k)}(\xi)|\Psi_k^x(\xi)\rangle_{BS_MBS_M}\langle\Psi_k^x(\xi)|, \quad (86)$$

$$P^{(k)}(\xi) = e^{-2\xi}\frac{(2\xi)^k}{k!},$$

$$|\Psi_k^x(\xi)\rangle_{BS_M} = |\Psi_k^x\rangle_B \otimes |\psi(\xi)\rangle_{S_M}, \quad \xi = \mu, \nu_1, \nu_2,$$

where the state $|\psi(\xi)\rangle_{S_M}$ reflected from the intensity modulator does not depend on the information state.

Eve has at her disposal a quantum state reflected from the intensity modulator; therefore, Eve's actions after detecting a Fock state with a given number of photons depend also on the additional information that the eavesdropper can obtain from the reflected state. Eve's actions are determined by the result of on-the-go measurement of the reflected state. The purpose of Eve's measurements is to find out from the state with what average number of photons ξ the component with a given number k of photons came from. In fact, the purpose of the eavesdropper is to distinguish one of the states $|\psi(\mu)\rangle_{S_M}$, $|\psi(\nu_1)\rangle_{S_M}$, or $|\psi(\nu_2)\rangle_{S_M}$.

The complete measurement of Eve and Bob ($\mathcal{J} = \{\mu, \nu_1, \nu_2\}$) is given by the resolution of identity:

$$I_{BS_M} = I_B \otimes I_{S_M} = \left(\sum_{\xi'\in\mathcal{J}}\mathcal{F}_{\xi'}\right)\otimes\left(\sum_{y\in\mathcal{Y}}\mathcal{M}_y\right), \quad \xi' \in \{\mu, \nu_1, \nu_2\}. \quad (87)$$

The eavesdropper's measurement over the reflected state is given by positive-valued measures $\mathcal{F}_{\xi'}$. Naturally, the eavesdropper chooses an optimal measurement that minimizes the error in distinguishing between reflected states corresponding to states with different average numbers of photons. To construct an optimal measurement, one should know the structure of the reflected state, which should be determined experimentally for a specific implementation of the cryptographic system.

Further, we do not explicitly need the reflected states themselves; we only need to know the probabilities of distinguishing between different states, which we consider to be known from experimental measurements. Taking into account (86) and (87), we obtain

$$P_{J|I}(\xi' \mid I = \xi) = \mathrm{Tr}_S\{\mathcal{F}_{\xi'}|\psi(\xi)\rangle_{SS}\langle\psi(\xi)|\}, \quad \mathcal{J} = \{\mu, \nu_1, \nu_2\}, \quad (88)$$

where $P_{J|I}(\xi'|I=\xi)$ is the conditional probability that a state with average number of photons ξ was sent to the channel and the eavesdropper, as a result of measurements (87) and (88), obtained an outcome ξ'—Eve made a decision that the channel contains a state with average number of photons ξ'.

In view of the aforesaid, the action of Eve's superoperator can be represented as

$$\mathcal{T}_{BS_M}[|\Psi_k^x\rangle_B \otimes |\psi(\xi)\rangle_{S_M S_M}\langle\psi(\xi)| \otimes_B \langle\Psi_k^x|] = \sum_{\xi'\in\mathcal{J}} P_{J|I}(\xi' \mid I=\xi)\rho^x_{k,\xi',B}. \quad (89)$$

Let us give an interpretation of formula (89). After detecting k photons in the channel, Eve, depending on the outcome of measurements over the reflected quantum state, transforms the Fock information state.

This means that the transformed density matrix $\rho^x_{k,\xi',B}$, in contrast to the situation without a side channel, depends on the initial state—on the average number of photons ξ in it. This dependence is expressed in terms of the transition probabilities $P_{J|I}(\xi'|I=\xi)$, which are determined by the distinguishability of the reflected states.

In fact, it is for this reason that the standard decoy state method does not work under an active probing attack on the intensity modulator.

The probability of measurement outcomes on the receiver side of Bob is expressed in terms of the density matrix in (89); taking into account (88), we find

$$P^{(k)}_{X|Y}(y,\xi' \mid X=x) = \mathrm{Tr}_B\{\mathcal{M}_y\rho^x_{k,\xi',B}\}, \quad x=0,1, \quad y=0,1,c. \quad (90)$$

For the partial count rate in information time windows on the receiver side, we obtain

$$P^{\mathrm{inf}}_{\xi}(y \mid X=x) = \sum_{k=0}^{\infty} P^{(k)}(\xi) \times \sum_{\xi'\in\mathcal{J}} P_{J|I}(\xi' \mid I=\xi)P^{(k)}_{X|Y}(y,\xi' \mid X=x), \quad y=0,1. \quad (91)$$

Similarly, for the partial count rate in the control time window on the receiver side, we get

$$P^{\mathrm{contr}}_{\xi}(y \mid X=x) = \sum_{k=0}^{\infty} P^{(k)}(\xi) = \sum_{\xi'\in\mathcal{J}} P_{J|I}(\xi' \mid I=\xi)P^{(k)}_{X|Y}(y,\xi' \mid X=x), \quad y=c. \quad (92)$$

For the total count rate in information time windows $y=0$, 1, taking into account (91), we find

$$P^{\mathrm{inf,tot}}_{\xi} = \sum_{x\in\{0,1\}}\sum_{y\in\{0,1\}} P_X(x)P^{\mathrm{inf}}_{\xi}(y \mid X=x) = \sum_{k=0}^{\infty} P^{(k)}(\xi)\sum_{\xi'\in\mathcal{J}} P_{J|I}(\xi' \mid I=\xi) \times \sum_{x\in\{0,1\}}\sum_{y\in\{0,1\}} P_X(x)P^{(k)}_{X|Y}(y,\xi' \mid X=x). \quad (93)$$

For the total count rate in the control window (index c) 3 in the basis L and in window 1 in the basis R, taking into account (92), we find

$$P^{\mathrm{contr,tot}}_{\xi} = \sum_{x\in\{0,1\}}\sum_{y\in\{C\}} P_X(x)P^{\mathrm{contr}}_{\xi}(y \mid X=x) = \sum_{k=0}^{\infty} P^{(k)}(\xi)\sum_{\xi'\in\mathcal{J}} P_{J|I}(\xi' \mid I=\xi) \times \sum_{x\in\{0,1\}}\sum_{y\in\{C\}} P_X(x)P^{(k)}_{X|Y}(y,\xi' \mid X=x). \quad (94)$$

Passing to more compact notation for the probabilities of counts in information time windows, we obtain

$$Y^{\mathrm{inf}}_k(\xi') = \sum_{x\in\{0,1\}}\sum_{y\in\{0,1\}} P_X(x)P^{(k)}_{X|Y}(y,\xi' \mid X=x). \quad (95)$$

To avoid misunderstandings, it is necessary to interpret the quantities $P^{(k)}_{X|Y}(y, \xi' \mid X=x)$ and explain the notation. Although this quantity looks like a probability, it is not normalized to unity. Consider messages in which the bases of Alice and Bob coincided and Alice sent states with an average number of photons ξ. Let us single out the messages in which Alice sent states corresponding to bit x with probability $P_X(x)$. Suppose that there were $N(x)$ such messages. Consider Bob's counts in information time windows. Eve's actions depend on the outcome of measurements over the states reflected from the intensity modulator. Suppose that Eve decided that the k-photon component of the states came from the states with the average number of photons ξ' for a given (real) ξ (see formula (91)). On the receiver side, for the k-photon component of states, provided that Eve has decided that, in the channel of the state with the average number of photons ξ', the information bit is x, $N^{(k)}(\xi', y)$ counts are detected, and the result of detection of the bit is interpreted by Bob as y. For large $N(\xi, x)$, the fraction $\dfrac{N^{(k)}(\xi', y)}{N(x)}$ of counts tends to $P^{(k)}_{X|Y}(y, \xi' \mid X=x)$ (see formula (95)).

For the probability of counts in control time windows, we obtain

$$Y^{\mathrm{contr}}_k(\xi') = \sum_{x\in\{0,1\}}\sum_{y\in\{C\}} P_X(x)P^{(k)}_{X|Y}(y,\xi' \mid X=x). \quad (96)$$

Next, denoting for brevity $P(\xi'|\mu) = P_{J|I}(\xi' \mid I=\mu)$ for (88), we find

$$P_{\mu}^{\text{inf,tot}} = \sum_{k=0}^{\infty} P^{(k)}(\mu) \sum_{\xi' \in \mathcal{J}} P(\xi' \mid \mu) Y_k^{\text{inf}}(\xi'), \quad (97)$$

$$P_{\mu}^{\text{contr,tot}} = \sum_{k=0}^{\infty} P^{(k)}(\mu) \sum_{\xi' \in \mathcal{J}} P(\xi' \mid \mu) Y_k^{\text{contr}}(\xi'). \quad (98)$$

We obtain the following expression for the partial error in information states:

$$e_k(\xi') = \frac{\sum_{x=0,1,y=0,1,x\neq y} P_X(i) P_{X|Y}^{(k)}(y, \xi' \mid X = x)}{\sum_{x=0,1,y=0,1} P_X(i) P_{X|Y}^{(k)}(y, \xi' \mid X = x)}. \quad (99)$$

Using (91), (93), and (96), we obtain an expression for the total error in information states:

$$\text{Err}_{\mu}^{\text{tot}} = \sum_{k=0}^{\infty} P^{(k)}(\mu) \sum_{\xi' \in \mathcal{J}} P(\xi' \mid \mu) Y_k^{\text{inf}}(\xi'). \quad (100)$$

8. ESTIMATION OF THE PARAMETERS OF THE SINGLE-PHOTON COMPONENT OF INFORMATION STATES AT THE RECEIVING STATION

Our further goal is to estimate the probability of the single-photon component and the error in the single-photon component to determine the length of the secret key. To calculate the length of the secret key, one needs to know separately the quantities $Y_1(\mu)$, $Y_1(\nu_1)$, and $Y_1(\nu_2)$; similarly, for the error probability, one needs separate quantities $e_1(\mu)$, $e_1(\nu_1)$, and $e_1(\nu_2)$.

The decoy state method does not allow one to obtain expressions for individual fractions of single-photon components and errors. The decoy state method allows one to obtain only their combinations (the sum of all values, see below). However, it is possible to obtain an estimate for the key length using only the sum of the values.

Let us proceed to obtaining the necessary combinations of single-photon components. For what follows, we introduce new notation:

$$\begin{aligned} \overline{P}_{\xi}^{\text{inf,tot}} &= e^{2\xi} P_{\xi}^{\text{inf,tot}} \\ &= \sum_{k=0}^{\infty} \frac{(2\xi)^k}{k!} \sum_{\xi' \in \mathcal{J}} P(\xi' \mid \xi) Y_k^{\text{inf}}(\xi), \end{aligned} \quad (101)$$

$$\begin{aligned} \overline{P}_{\xi}^{\text{contr,tot}} &= e^{2\xi} P_{\xi}^{\text{contr,tot}} \\ &= \sum_{k=0}^{\infty} \frac{(2\xi)^k}{k!} \sum_{\xi' \in \mathcal{J}} P(\xi' \mid \xi) Y_k^{\text{contr}}(\xi). \end{aligned} \quad (102)$$

Note that, unlike the standard decoy state method, the expression for the count rate of states with different average numbers of photons includes different quantities $Y_k^{\text{inf,contr}}$ with different weight coefficients—conditional probabilities depending on the states reflected from the intensity modulator.

Introduce new, more convenient notation for the error probability:

$$\begin{aligned} \overline{\text{Err}}_{\xi}^{\text{tot}} &= e^{2\xi} \text{Err}_{\xi}^{\text{tot}} \\ &= \sum_{k=0}^{\infty} \frac{(2\xi)^k}{k!} \sum_{\xi' \in \mathcal{J}} P(\xi' \mid \xi) e_k(\xi) Y_k^{\text{inf}}(\xi). \end{aligned} \quad (103)$$

Next, denote

$$\begin{aligned} p^{\min}(\xi) &= \min_{\xi' \in \{\mu, \nu_1, \nu_2\}} P(\xi' \mid \xi), \\ p^{\max}(\xi) &= \min_{\xi' \in \{\mu, \nu_1, \nu_2\}} P(\xi' \mid \xi). \end{aligned} \quad (104)$$

Using (101)–(104), we obtain the following chain of inequalities:

$$\begin{aligned} \overline{P}_{\mu}^{\text{inf,tot}} &\geq p^{\min}(\mu) Y_0^{\text{inf},\Sigma} \\ &+ p^{\min}(\mu) \left[2\mu Y_1^{\text{inf},\Sigma} + \sum_{k=2}^{\infty} \frac{(2\mu)^k}{k!} Y_k^{\text{inf},\Sigma} \right], \end{aligned} \quad (105)$$

$$\begin{aligned} Y_k^{\text{inf},\Sigma} &= Y_k^{\text{inf}}(\mu) + Y_k^{\text{inf}}(\nu_1) + Y_k^{\text{inf}}(\nu_2), \\ Y_0^{\text{inf},\Sigma} &= \sum_{\xi \in \{\mu, \nu_1, \nu_2\}} Y_0^{\text{inf}}(\xi). \end{aligned} \quad (106)$$

Next, we have

$$\begin{aligned} \overline{P}_{\nu_1}^{\text{inf,tot}} &\geq p^{\max}(\nu_1) Y_0^{\text{inf},\Sigma} + p^{\max}(\nu_1) \\ &\times \left[2\nu_1 Y_1^{\text{inf},\Sigma} + \sum_{k=2}^{\infty} \frac{(2\nu_1)^k}{k!} Y_k^{\text{inf},\Sigma} \right], \end{aligned} \quad (107)$$

$$\begin{aligned} \overline{P}_{\nu_2}^{\text{inf,tot}} &\geq p^{\min}(\nu_2) Y_0^{\text{inf},\Sigma} + p^{\min}(\nu_2) \\ &\times \left[2\nu_2 Y_1^{\text{inf},\Sigma} + \sum_{k=2}^{\infty} \frac{(2\nu_2)^k}{k!} Y_k^{\Sigma} \right]. \end{aligned} \quad (108)$$

We introduced the notation

$$\begin{aligned} \overline{P}_{\mu}^{\text{inf,tot,min}} &= \frac{P_{\mu}^{\text{inf,tot}}}{p^{\min}(\mu)}, \\ \overline{P}_{\nu_1}^{\text{inf,tot,max}} &= \frac{P_{\nu_1}^{\text{inf,tot}}}{p^{\max}(\nu_1)}. \end{aligned} \quad (109)$$

Combining (105)–(109), we obtain

$$\begin{aligned} (2\nu_1 - 2\nu_2) Y_1^{\text{inf},\Sigma} &\geq [\overline{P}_{\nu_1}^{\text{inf,tot,max}} - \overline{P}_{\nu_2}^{\text{inf,tot,min}}] \\ &- \sum_{k=2}^{\infty} \frac{(2\nu_1)^k - (2\nu_2)^k}{k!} Y_k^{\text{inf},\Sigma}. \end{aligned} \quad (110)$$

Taking into account that

$$\begin{aligned} &\frac{(2\nu_1)^2 - (2\nu_2)^2}{(2\mu)^2} \sum_{k=2}^{\infty} \frac{(2\mu)^k}{k!} Y_k^{\text{inf},\Sigma} \\ &\geq \sum_{k=2}^{\infty} \frac{(2\nu_1)^k - (2\nu_2)^k}{k!} Y_k^{\text{inf},\Sigma}, \end{aligned} \quad (111)$$

as well as (110) and (111), we obtain

$$\bar{P}_{\mu}^{\text{inf,tot,min}} - Y_0^{\text{inf},\Sigma} - 2\mu Y_1^{\text{inf},\Sigma} \geq \sum_{k=2}^{\infty} \frac{(2\mu)^k}{k!} Y_k^{\text{inf},\Sigma}. \quad (112)$$

Finally we have

$$Y_1^{\text{inf},\Sigma} \geq \frac{1}{(2\nu_1 - 2\nu_2) - \dfrac{(2\nu_1)^2 - (2\nu_2)^2}{2\mu}} \times \left\{ [\bar{P}_{\nu_1}^{\text{inf,tot,max}} - \bar{P}_{\nu_2}^{\text{inf,tot,max}}] - \frac{(2\nu_1)^2 - (2\nu_2)^2}{(2\mu)^2} \times [\bar{P}_{\mu}^{\text{inf,tot,max}} - Y_0^{\text{inf},\Sigma}] \right\}. \quad (113)$$

As mentioned above and seen in (106) and (113), we can obtain only an estimate for the sum of single-photon components Y_1^{Σ}, rather than an estimate for individual components. At the same time, the estimate for the length of the secret key (see formula (129) below) includes the values of individual components. Below we will see that this problem can be circumvented by using the convexity of conditional entropies (see below).

To estimate the total fraction of the vacuum component Y_0^{Σ}, we obtain

$$Y_0^{\text{inf},\Sigma} \geq \max\left\{ \frac{2\nu_1 \bar{P}_{\nu_2}^{\text{inf,tot,max}} - 2\nu_2 \bar{P}_{\nu_1}^{\text{inf,tot,min}}}{2\nu_1 - 2\nu_2}, 0 \right\}, \quad (114)$$

where

$$\bar{P}_{\nu_{1,2}}^{\text{inf,tot,min}} = \frac{P_{\nu_{1,2}}^{\text{inf,tot}}}{p^{\min}(\nu_{1,2})}, \quad \bar{P}_{\nu_{1,2}}^{\text{inf,tot,max}} = \frac{P_{\nu_{1,2}}^{\text{inf,tot}}}{p^{\max}(\nu_{1,2})}. \quad (115)$$

According to formulas (28) and (40), the length of the secret key for the single-photon component includes the ratio of count probabilities in the control time windows and information time windows, $\zeta/(1-\zeta)$ (see details in [10, 11]). Eve's lack of information about the key is expressed in terms of this ratio.

Let us obtain an estimate for the probability of error in the single-photon component of states:

$$\overline{\text{Err}}_{\nu_1}^{\text{tot}} \geq p^{\min}(\nu_1) \left\{ \sum_{k=0}^{\infty} \frac{(2\nu_1)^k}{k!} (eY)_k^{\Sigma} \right\}. \quad (116)$$

Similar to the previous case, we find

$$\overline{\text{Err}}_{\nu_2}^{\text{tot}} \geq p^{\max}(\nu_2) \left\{ \sum_{k=0}^{\infty} \frac{(2\nu_2)^k}{k!} (eY)_k^{\Sigma} \right\}, \quad (117)$$

where the following notation is introduced:

$$(eY)_k^{\Sigma} = e_k(\mu) Y_k^{\text{inf}}(\mu) + e_k(\nu_1) Y_k^{\text{inf}}(\nu_1) + e_k(\nu_2) Y_k^{\text{inf}}(\nu_2). \quad (118)$$

Combining inequalities (116) and (117), we obtain

$$(eY)_1^{\Sigma} \leq \frac{\overline{\text{Err}}_{\nu_1}^{\text{tot,min}} - \overline{\text{Err}}_{\nu_2}^{\text{tot,min}}}{2\nu_1 - 2\nu_2}, \quad (119)$$

where the notation

$$\overline{\text{Err}}_{\nu_1}^{\text{tot,min}} = \frac{\overline{\text{Err}}_{\nu_1}^{\text{tot}}}{p^{\min}(\nu_1)}, \quad \overline{\text{Err}}_{\nu_2}^{\text{tot,min}} = \frac{\overline{\text{Err}}_{\nu_2}^{\text{tot}}}{p^{\max}(\nu_2)} \quad (120)$$

is introduced. Let us estimate the probability of the single-photon component of the states in the control time windows:

$$\bar{P}_{\nu_1}^{\text{contr,tot}} \geq p^{\min}(\nu_1) \left\{ \sum_{k=0}^{\infty} \frac{(2\nu_1)^k}{k!} Y_k^{\text{contr},\Sigma} \right\}. \quad (121)$$

Similar to the previous case, we find

$$\bar{P}_{\nu_2}^{\text{contr,tot}} \leq p^{\max}(\nu_2) \left\{ \sum_{k=0}^{\infty} \frac{(2\nu_2)^k}{k!} Y_k^{\text{contr},\Sigma} \right\}. \quad (122)$$

Combining inequalities (121) and (122), we obtain

$$Y_1^{\text{contr},\Sigma} \leq \frac{\bar{P}_{\nu_1}^{\text{contr,tot,min}} - \bar{P}_{\nu_2}^{\text{contr,tot,max}}}{2\nu_1 - 2\nu_2}, \quad (123)$$

where the following notation is introduced:

$$\bar{P}_{\nu_1}^{\text{contr,tot,min}} = \frac{\bar{P}_{\nu_1}^{\text{contr,tot}}}{p^{\min}(\nu_1)}, \quad \bar{P}_{\nu_2}^{\text{contr,tot,max}} = \frac{\bar{P}_{\nu_2}^{\text{tot}}}{p^{\max}(\nu_2)}. \quad (124)$$

For what follows, we need the ratio that appears in Eve's lack of information about the key in the single-photon component. For the k-photon component, we have

$$\frac{Y_k^{\text{contr}}(\xi)}{Y_k^{\text{inf}}(\xi)} = \frac{\zeta_k(\xi)}{1 - \zeta_k(\xi)}. \quad (125)$$

Next, denote for brevity

$$Y_1^{\text{inf},\Sigma} = Y_1^{\text{inf}}(\mu) + Y_1^{\text{inf}}(\nu_1) + Y_1^{\text{inf}}(\nu_2), \quad (126)$$

$$Y_k^{\text{inf},\Sigma} = Y_k^{\text{inf}}(\mu) + Y_k^{\text{inf}}(\nu_1) + Y_k^{\text{inf}}(\nu_2). \quad (127)$$

The modified decoy state method does not allow one to obtain the partial ratios separately. It only provides the integral ratios

$$(\zeta Y)_1^{\text{inf},\Sigma} = \frac{Y_1^{\text{contr},\Sigma}}{Y_1^{\text{inf},\Sigma}}, \quad (128)$$

which, together with the convexity of the entropy, are sufficient to calculate the length of the secret key.

9. ESTIMATION OF THE SECRET KEY LENGTH WITH REGARD TO SIDE CHANNELS OF INFORMATION LEAKAGE AND THE NON-SINGLE-PHOTON NATURE OF INFORMATION STATES

Above, we obtained estimates for the length of the secret key for a strictly single-photon component. In this case, the parameters describing the side radiation (p, d, and η) should be referred to messages in which information states with an average number of photons μ were transmitted. Expressions for the secret key length have the following structure:

$$\ell = P_\mu^{\text{inf,tot}}\left\{\frac{e^{-2\mu}(2\mu)}{P_\mu^{\text{inf,tot}}}\right.$$
$$\times\left(\sum_{\xi=\mu,\nu_1,\nu_2} P(\xi\,|\,\mu)Y_1^{\text{inf}}(\xi)[1-\chi_{\text{Hol}}(\zeta_1(\xi),p,\eta,d)]\right)$$
$$\left.-\text{leak}(\text{Err}_\mu^{\text{tot}})\right\} = P_\mu^{\text{inf,tot}}\left\{\frac{e^{-2\mu}(2\mu)}{P_\mu^{\text{inf,tot}}}\right. \quad (129)$$
$$\times\left(\sum_{\xi'} P(\xi'\,|\,\mu)Y_1^{\text{inf}}(\xi)\right)\left(\sum_{\xi=\mu,\nu_1,\nu_2}\frac{P(\xi\,|\,\mu)Y_1^{\text{inf}}(\xi)}{\sum_{\xi'} P(\xi'\,|\,\mu)Y_1^{\text{inf}}(\xi')}\right.$$
$$\left.\times[1-\chi_{\text{Hol}}(\zeta_1(\xi),p,\eta,d)]\right)-\text{leak}(\text{Err}_\mu^{\text{tot}})\Bigg\}.$$

Informally speaking, after detecting a state with the number of photons k in the channel, Eve performs measurements over the reflected probing state in order to find out from which state, information state or a decoy state, the detected state came from. After the measurement, the probability of the outcome is given by the conditional probability $P(\xi'|\xi)$, and Eve makes a conclusion about further actions. In other words, the probabilities of counts in the control windows, $\zeta_1(\xi)$, and of the fraction of the single-photon component, $Y_1^{\text{inf}}(\xi)$, depend on the outcome of the measurements over the reflected state. The conditional probabilities $P(\xi'|\xi)$ are known. Note that the length of the secret key (129) includes the partial quantities $\zeta_1(\xi)\left(\frac{\zeta_1(\xi)}{1-\zeta_1(\xi)}\right)$, which are different in messages for states with different intensities ξ.

The functions $\chi_{\text{Hol}}(\zeta_1(\xi), p, \eta, d)$ in (129) are convex functions of the arguments. By definition, a convex function $f(x)$ satisfies the inequality

$$\sum_i \lambda_i f(x_i) \le f\left(\sum_i \lambda_i x_i\right),$$
$$0 \le \lambda_i \le 1, \quad \sum_i \lambda_1 = 1. \quad (130)$$

Since

$$\sum_{\xi'} P(\xi'\,|\,\mu)Y_1^{\text{inf}}(\xi') \ge p^{\min}(\mu)Y_1^{\text{inf},\Sigma}, \quad (131)$$

taking into account (130), we obtain the following chain of inequalities:

$$\sum_{\xi=\mu,\nu_1,\nu_2}\frac{P(\xi\,|\,\mu)Y_1^{\text{inf}}(\mu)}{\sum_{\xi'} P(\xi'\,|\,\mu)Y_1^{\text{inf}}(\xi')}\chi_{\text{Hol}}(\zeta_1(\xi),p,\eta,d)$$
$$\le\frac{p^{\max}(\mu)}{p^{\min}(\mu)}\sum_{\xi=\mu,\nu_1,\nu_2}\frac{Y_1^{\text{inf}}(\xi)}{Y_1^{\text{inf},\Sigma}}\chi_{\text{Hol}}(\zeta_1(\xi),p,\eta,d)$$
$$\le\frac{p^{\max}(\mu)}{p^{\min}(\mu)}\chi_{\text{Hol}}\left(\sum_{\xi=\mu,\nu_1,\nu_2}\frac{Y_1^{\text{inf}}(\xi)\zeta_1(\xi)}{Y_1^{\text{inf},\Sigma}},p,\eta,d\right)$$
$$=\frac{p^{\max}(\mu)}{p^{\min}(\mu)}\chi_{\text{Hol}}\left(\sum_{\xi=\mu,\nu_1,\nu_2}\frac{Y_1^{\text{contr}}(\xi)}{Y_1^{\text{inf},\Sigma}},p,\eta,d\right) \quad (132)$$
$$=\frac{p^{\max}(\mu)}{p^{\min}(\mu)}\chi_{\text{Hol}}\left(\sum_{\xi=\mu,\nu_1,\nu_2}\frac{Y_1^{\text{contr},\Sigma}}{Y_1^{\text{inf},\Sigma}},p,\eta,d\right)$$
$$=\frac{p^{\max}(\mu)}{p^{\min}(\mu)}\chi_{\text{Hol}}((\zeta Y)_1^{\text{inf},\Sigma}p,\eta,d).$$

In (132), we took into account that

$$\zeta_1(\xi)=\frac{Y_1^{\text{contr}}(\xi)}{Y_1^{\text{inf}}(\xi)}, \quad (\zeta Y)_1^{\text{inf},\Sigma}=\frac{Y_1^{\text{contr},\Sigma}}{Y_1^{\text{inf},\Sigma}}. \quad (133)$$

As a result, using (132) and, for brevity, notation (133), we obtain the following expression for the fraction of secret bits:

$$\sum_{\xi=\mu,\nu_1,\nu_2}\frac{P(\xi\,|\,\mu)Y_1^{\text{inf}}(\xi)}{\sum_{\xi'} P(\xi'\,|\,\mu)Y_1^{\text{inf}}(\xi')}[1-\chi_{\text{Hol}}(\zeta_1(\xi),p,\eta,d)]$$
$$\ge 1-\frac{p^{\max}(\mu)}{p^{\min}(\mu)}\chi_{\text{Hol}}((\zeta Y)_1^{\text{inf},\Sigma},p,\eta,d). \quad (134)$$

Taking into account (134), we find

$$\ell = P_\mu^{\text{inf,tot}}\left\{\frac{e^{-2\mu}(2\mu)p^{\min}(\mu)Y_1^{\text{inf},\Sigma}}{P_\mu^{\text{inf,tot}}}\right. \quad (135)$$
$$\left.\times\left(1-\frac{p^{\max}(\mu)}{p^{\min}(\mu)}\chi_{\text{Hol}}((\zeta Y)_1^{\text{inf},\Sigma},p,\eta,d)\right)-\text{leak}(\text{Err}_\mu^{\text{tot}})\right\}.$$

Formula (135) contains the integral fraction of the single-photon component $Y_1^{\mathrm{inf},\Sigma}$ and the integral ratio $(\zeta Y))_1^{\mathrm{inf},\Sigma}$. In fact, this means that the partial ratios in the argument of $\chi_{\mathrm{Hol}}(\zeta_1, p, d, \eta)$ in formulas (134) and (135) should be replaced by the mean values:

$$\zeta_1 \to (\zeta Y)_1^{\mathrm{inf},\Sigma}. \tag{136}$$

These quantities are expressed in the modified decoy state method in terms of the observed quantities—the count rate on the receiver side for states with different average numbers of photons. Recall that this is the length of the secret key in one basis. In order to obtain the key length over all bases, it is necessary to apply once again the convexity of the functions in (135).

10. ESTIMATION OF THE SECRET KEY LENGTH OVER ALL BASES

Let us estimate the length of the secret key over all bases. Now, the quantities in (135) must be supplied with the subscript of a basis $b = L, R$; we obtain

$$\ell^{\Sigma} = \sum_{b=L,R} \ell(b) = \sum_{b=L,R} \left\{ p^{\min}(\mu) e^{-2\mu} (2\mu) Y_1^{\mathrm{inf},\Sigma}(b) \times \left(1 - \frac{p^{\max}(\mu)}{p^{\min}(\mu)} \chi_{\mathrm{Hol}}((\zeta Y)_1^{\mathrm{inf},\Sigma}(b), p, \eta, d) \right) \right\} - P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}} \sum_{b=L,R} \frac{P_\mu^{\mathrm{inf,tot}}(b)}{P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}}} \mathrm{leak}(\mathrm{Err}_\mu^{\mathrm{tot}}(b)), \tag{137}$$

where

$$P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}} = \sum_{b=L,R} P_\mu^{\mathrm{inf,tot}}(b).$$

Using the convexity of the functions $\mathrm{leak}(\mathrm{Err}_\mu^{\mathrm{tot}}(b))$ and $\chi_{\mathrm{Hol}}(\zeta, p, \eta, d)$, we find

$$\mathrm{leak}\left(\sum_{b=L,R} \frac{P_\mu^{\mathrm{inf,tot}}(b)}{P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}}} \mathrm{Err}_\mu^{\mathrm{tot}}(b) \right) \geq \sum_{b=L,R} \frac{P_\mu^{\mathrm{inf,tot}}(b)}{P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}}} \mathrm{leak}(\mathrm{Err}_\mu^{\mathrm{tot}}(b)), \tag{138}$$

$$\mathrm{Err}_\mu^{\Sigma\mathrm{tot}} = \sum_{b=L,R} \frac{P_\mu^{\mathrm{inf,tot}}(b)}{P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}}} \mathrm{Err}_\mu^{\mathrm{tot}}(b),$$

$$\chi_{\mathrm{Hol}}\left(\sum_{b=L,R} (\zeta Y)_1^{\mathrm{inf},\Sigma}(b), p, \eta, d \right) \geq \sum_{b=L,R} \frac{Y_1^{\mathrm{inf},\Sigma}(b)}{Y_1^{\mathrm{inf},\Sigma\mathrm{tot}}} \chi_{\mathrm{Hol}}((\zeta Y)_1^{\mathrm{inf},\Sigma}(b), p, \eta, d).$$

Finally we obtain

$$\ell^{\Sigma} = P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}} \left\{ \frac{e^{-2\mu}(2\mu) p^{\min}(\mu) Y_1^{\mathrm{inf},\Sigma\mathrm{tot}}}{P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}}} \times \left(1 - \frac{p^{\max}(\mu)}{p^{\min}(\mu)} \chi_{\mathrm{Hol}}((\zeta Y)_1^{\mathrm{inf},\Sigma\mathrm{tot}}, p, \eta, d) \right) - \mathrm{leak}(\mathrm{Err}_\mu^{\Sigma\mathrm{tot}}) \right\}, \tag{139}$$

where

$$(\zeta Y)_1^{\mathrm{inf},\Sigma\mathrm{tot}} = \sum_{b=L,R} \frac{Y_1^{\mathrm{inf},\Sigma}(b)(\zeta Y)_1^{\mathrm{inf},\Sigma}(b)}{Y_1^{\mathrm{inf},\Sigma\mathrm{tot}}},$$

$$Y_1^{\mathrm{inf},\Sigma\mathrm{tot}} = \sum_{b=L,R} Y_1^{\mathrm{inf},\Sigma}(b).$$

11. DISCUSSION OF THE RESULTS

Formula (139) gives the length of the secret key in bits per detected message over all bases. The length of the key per detected message over all bases is expressed in terms of the average values of the observed parameters on the receiver side. These parameters are as follows.

1. The total error probability $\mathrm{Err}_\mu^{\Sigma\mathrm{tot}}$ in information time windows averaged over all bases. This quantity can be determined both by disclosing a part of the sequence of detected messages and actually, provided that the error correction occurs immediately without preliminary estimation of the error probability. In this case, the fraction of corrected positions in the asymptotic limit immediately gives the quantity $\mathrm{Err}_\mu^{\Sigma\mathrm{tot}}$.

2. The total probability of detected messages $P_\mu^{\mathrm{inf},\Sigma\mathrm{tot}}$ over all bases.

3. The total probability of detection of the single-photon component of states, $Y_1^{\mathrm{inf},\Sigma\mathrm{tot}}$, in information time windows over all bases. This quantity is estimated in terms of the quantities, observed on the receiver side, for information messages and the messages with decoy states.

4. The total averaged probability of detection of the single-photon component of the states $(\zeta Y)_1^{\mathrm{inf},\Sigma\mathrm{tot}}$ over all bases in the control time windows. This quantity is estimated in terms of observed quantities for information messages and the messages with decoy states.

5. The quantities $p^{\max}(\mu)$ and $p^{\min}(\mu)$, which determine the maximum and minimum probabilities of distinguishing the probing states reflected from the intensity modulator, depend on the specific experimental implementation of the quantum cryptography system, and must be determined/calculated in special studies.

6. The quantity η, which determines the minimum overlap (maximum distinguishability) of the probing

states reflected from the phase modulator on the receiver side, should also be measured/calculated in special studies and determined for the specific implementation of the system.

7. The quantities p and d, which describe the probability of distinguishing quantum states in side channels associated with the passive detection of electromagnetic radiation and backward radiation of avalanche detectors, should be determined experimentally and also depend on the specific implementation of the system.

The upper bound for the information leakage to the eavesdropper under an attack on information states in a quantum communication channel can be obtained, at least for single-photon states, without resorting to any model considerations, but relying only on the fundamental limitations of quantum theory, for example, on the entropy uncertainty relations [3], since the type of information states sent to the communication channel is known. The situation with states in side channels is fundamentally different. The introduction of side channels of information leakage and quantum states in them cannot be done without some model considerations. The structure of quantum states in side channels is not known exactly. Theoretically, the structure of quantum states in side channels for each specific implementation of a quantum cryptography system can be determined by quantum tomography. However, this is only speculative. In practice, this is impossible due to the huge number of degrees of freedom of the system. For example, the exact type of side electromagnetic radiation from electronic equipment is unknown due to the macroscopically large number of degrees of freedom. Therefore, model considerations are required. Above, we considered the models of binary quantum channels for side radiation. The method proposed allows one to consider any other types of side channels on a regular basis. Moreover, according to the above consideration, the exact form of the states themselves is not required; it suffices to know the upper bound of the distinguishability of states, which is a simpler experimental problem.

We have considered the asymptotic limit of long transmitted sequences. The consideration of the finite length of transmitted sequences is a more or less standard problem on the fluctuations of observed quantities due to the finite length of the sequences, which is a standard problem in the classical probability theory.

ACKNOWLEDGMENTS

I am grateful to my colleagues from the Academy of Cryptography of the Russian Federation for discussions and support, as well as to I.M. Arbekov and S.P. Kulik for numerous interesting discussions and remarks that helped to improve the article.

FUNDING

This work was supported by the Russian Science Foundation, project no. 16-12-00015 (continued).

REFERENCES

1. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Comp., Systems and Signal Processing, Bangalore, India, 1984*, p. 175.
2. R. Renner, PhD Thesis (ETH Zürich, 2005); arXiv:quant-ph/0512258.
3. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, arXiv: 1103.4130v2 (2011); Nat. Commun. **3**, 1 (2012).
4. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
5. Won-Young Hwang, arXiv:[quant-ph]/0211153.
6. Xiang-Bin Wang, Phys. Rev. Lett. **94**, 230503 (2005).
7. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Phys. Rev. Lett. **94**, 230504 (2005).
8. Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, arXiv: [quant-ph]/0503005.
9. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
10. S. N. Molotkov, J. Exp. Theor. Phys. **106**, 1 (2008).
11. S. N. Molotkov, Laser Phys. Lett. **16**, 035203 (2019).
12. A. S. Holevo, Probl. Inf. Transmis. **9**, 177 (1973).
13. A. S. Kholevo, Usp. Mat. Nauk **53**, 193 (1998).
14. A. S. Holevo, *Quantum Systems, Channels, Information*, Vol. 16 of *de Gruyter Studies in Mathematical Physics* (MTsNMO, Moscow 2010; Walter de Gruyter, Berlin, 2013).

Translated by I. Nikitin