ISSN 0021-3640, JETP Letters, 2020, Vol. 112, No. 6, pp. 383–392. © Pleiades Publishing, Inc., 2020.
Russian Text © The Author(s), 2020, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2020, Vol. 112, No. 6, pp. 401–411.

QUANTUM INFORMATICS

On a New Attack on Quantum Key Distribution: Joint Unambiguous Measurements of Probe States and the PNS Attack on Information States

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

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

Received August 11, 2020; revised August 15, 2020; accepted August 16, 2020

A new attack on the quantum key distribution is proposed involving joint collective unambiguous measurements of reflected probe states from an intensity modulator and photon number splitting (PNS) measurements, i.e., nondestructive measurements of the number of information photons in the quantum communication channel. This attack does not change the relative statistics of photocounts of states with different numbers of photons, does not lead to errors on the receiver side, and, thereby, is not detected by any of known methods, including the modified decoy state method. The attack results only in additional losses in the communication channel, which are not "controlled" by the decoy state method. The dependence of introduced losses on the intensity of reflected probe states is estimated. The critical level of losses depends on a particular physical implementation of the quantum cryptography system, which determines the upper bound of the intensity of reflected probe states. The knowledge of this bound is fundamentally necessary to ensure the security of keys. The fact that the attack does not lead to errors on the receiver side and does not change the relative statistics of photocounts but only results in additional losses, which depend on the intensity according to the distinguishability of reflected probe states, *does not mean* that this attack transforms quantum cryptography systems from the type of cryptographic systems where the security of keys is guaranteed by fundamental quantum mechanical laws to the type of systems where this security is guaranteed by technical restrictions. Even in the presence of side channels of information leakage, the security of keys is still guaranteed by fundamental quantum mechanical restrictions on the distinguishability of states. A low level of distinguishability ("intensity") of quantum states in side channels is naturally reached by technical tools.

DOI: 10.1134/S0021364020180095

1. INTRODUCTION

The development of methods for unauthorized information disclosure accompanies the development of methods for transmission and protection of information. In the classical region, information carriers are electromagnetic signals, which are transmitted either through open space or through cable or fiber optic communication channels. Unauthorized information disclosure for classical signals is possible both from cable communication channels and from fiber optic communication channels.

To obtain information, the direct access to a communication channel is not necessarily needed because the operation of transmitter and receiver equipment results in side electromagnetic radiation, which can be detected. The detection of side electromagnetic radiation can compromise the operation of electronic cryptographic equipment. Various types of interfaces between individual components of equipment also result in compromising side radiation.

There are other side channels of information leakage such as electromagnetic radiation and optical radiation (electromagnetic radiation in the optical range), as well as acoustic, ultrasonic, and mechanical channels, which can lead to information leakage without direct access to a source of information. Usually, a large set of methods and experimental devices in this field are not widely reported. Some aspects of the detection of side signals in classical cryptographic systems, as well as some historical examples, can be found, e.g., in [1–7].

When the optic signal intensity is reduced to a single-photon level, the signal becomes quantum and this leads to a qualitatively new situation. In contrast to the intense classical optical signal transmitted through a fiber optic communication channel, eavesdropping attempts to measure an unknown state in a quantum

communication channel result in perturbation of a quantum state and errors on the receiver side [8]. For this reason, the detection of any attack on the quantum communication channel is guaranteed by the fundamental quantum laws. Furthermore, fundamental quantum-mechanical restrictions allow relating the observed level of perturbation of quantum states (level of errors) observed on the receiver side to the upper bound of information leakage [9–11]. This is the foundation of quantum cryptography, i.e., quantum secret key distribution.

In this sense, quantum cryptography systems are protected against attacks directly on the communication channel. Moreover, it is assumed that the communication channel is directly accessible for active eavesdropping.

The currently achieved understanding of attacks on quantum states in the quantum communication channel, i.e., attempts at retrieval of transmitted key information, is sufficiently deep. There are methods to take into account that a source of quantum states is not strictly single-photon, losses in the communication channel, non-unit quantum efficiency of single-photon detectors, etc. Quantum cryptography ensures the unconditional security of keys with respect to attacks on the quantum communication channel, which is based only on fundamental quantum-mechanical laws.

Quantum cryptography systems are complex devices including numerous active fiber optic components such as phase modulators, intensity modulators, polarization controllers, and controlling electronics with various external and internal interfaces. The operation of electronics and electronically controlled active fiber optic elements leads to side radiation, which carries information on distributed keys.

The situation in quantum cryptography is more delicate than that in classical cryptographic systems. Quantum cryptography systems are open systems because the eavesdropper can obtain information on distributed keys not only from detected side radiation but also by actively probing the state of fiber elements (phase modulators, intensity modulators, polarization controllers, etc.) through the fiber optic communication channel.

Without understanding and inclusion of information leakage through side channels, it is impossible to exactly analyze the security of keys in real quantum cryptography systems. Another fundamental difference of side channels in quantum cryptography from side channels in classical systems is that states in side channels cannot be considered classically. The eavesdropper can measure information quantum states and states in side channels simultaneously; consequently, the fully quantum consideration is necessary.

The complete set of methods of including attacks on equipment and taking into account side channels of information leakage is currently under active study. Unlike classical cryptographic systems, the study of information leakage through side channels began only recently [12–20].

A source of information states in real systems provides weakened coherent states with Poisson photon number statistics and is not strictly single-photon. The secret key is composed only of a single-photon component of coherent states. Conservatively in favor of the eavesdropper (Eve), it is accepted that information contained in multiphoton components of states with the number of photons $k > 1$ is known to Eve. The fraction of the single-photon component on the receiver side is estimated by the modified decoy state method (see details in [21–23]). In the absence of side channels of information leakage, the most general attack on the single-photon component of states is a unitary attack. Such an optimal attack can be constructed explicitly for the BB84 protocol [24, 25]. Since the multiphoton components of states are "given" (assumed to be known) to the eavesdropper, the further goal is reduced to the construction of an attack on a single-photon component with allowance for side leakage channels.

It is fundamentally important for the decoy state method that, without additional information, Eve does not know from what state and with what average number of photons a component with a given number of photons k originates. The distortion of the single-photon component in messages belonging to coherent states with various intensities distorts the relative observed total count rate, i.e., statistics on the receiver side for messages where states with various intensities were sent. Change in the relative total count rate makes it possible to estimate the fraction of the single-photon component and error in it on the receiver side.

Everything stated above is valid when Eve does not have additional information on a state sent to the quantum communication channel in each message and on its intensity (average photon number).

In the presence of side signals, assumptions underlying the decoy state method are violated. Actively probing the state of the intensity modulator, Eve obtains additional information on the intensity of the transmitted state.

Measurements of the probe states reflected from the intensity modulator give additional information on the intensity of the transmitted state in each message. Two types of measurements are possible:

- measurements minimizing the error of distinguishing reflected states,
- unambiguous measurements (UMs).

Measurements of the first type allow distinguishing quantum states but with a certain error probability. Measurements of the second type distinguish states with certainty if a *conclusive* outcome is obtained. Upon an inconclusive outcome, usually denoted as ?, nothing is known about the state. When distinguishing N states, a measurement of the first type has N out-

comes. A measurement of the second type has $N+1$ outcomes, i.e., N conclusive and one inconclusive. It is noteworthy that the necessary and sufficient condition for the possibility of UMs is the linear independence of a set of N states [26–33], which is fulfilled for reflected states (see below).

An attack on distributed keys in the case of measurements of the first type is detected by the decoy state method because this attack changes the Poisson count statistics. However, the standard decoy state method [21–23] should be significantly modified, as done in [17, 18].

A new attack described in this work involves the active probing of the intensity modulator, UMs of reflected states, and a PNS attack with the nondestructive measurement of the number of photons in information states in the quantum communication channel, which has not yet been considered, as far as I know.

With this attack, Eve *knows the entire key*, does not generate errors on the receiver side, and does not change the photocount statistics on the receiver side in messages corresponding to coherent states with various intensities (average number of photons).

This attack cannot be detected by the decoy state method because it does not change the observed relative statistics of counts of states with various intensities on the receiver side. The attack only reduces the general rate of photocounts, i.e., only increases observed losses without change in statistics in Fock components of states with different numbers of photons.

It is important that total losses in the communication channel are not explicitly involved in the decoy state method [17, 21–23]; i.e., neither the standard [21–23] nor the modified decoy state method [17, 18] requires tracking total losses.

Since the proposed attack results only in additional losses, i.e., reduction of the count rate on the receiver side, and does not generate errors and does not violate the statistics of counts, it is important to know the level of losses generated by this attack.

More precisely, the attack is not detected by known methods and is efficient, i.e., undetectable if the level of losses generated by this attack is no less than a certain value.

The aim of this work is to estimate the critical observed level of losses, i.e., decrease in the photocount rate at which this attack becomes possible.

2. DESCRIPTION OF THE ATTACK

The idea of the attack is quite simple. Quantum cryptography systems with phase encoding on the receiver side involve active elements—phase and intensity modulators. If the state of the phase modulator is known, the transmitted key bit is known. If the state of the intensity modulator is known, the intensity (and average number of photons) of the coherent state in it is known. If Eve certainly knowns the states of both active elements, Eve knows the entire transmitted key.

Since quantum cryptography systems are open systems, Eve not only has access to the quantum communication channel, but also can actively probe states of the active elements through the fiber optic communication channel by sending probe radiation and, then, measuring the reflected state.

The degree of distinguishability of states reflected from active elements of the transmitted station depends on the intensity of reflected states. Intense, classical states are certainly distinguishable. The intensity of information states sent from the transmitter station is controlled by the transmitter, whereas the intensity of reflected states is controlled by Eve. The more intense the probe signals sent by Eve, the more intense the reflected probe states.

To know the upper bound of the intensity of reflected states, it is necessary to know the upper bound of the intensity of input probe states, which is dictated by the melting of optic fiber [34–36]. In other words, the intensity of input states cannot be larger than the critical value at which the fiber is melted [34–36].

The upper bound of the intensity of reflected states at the known upper bound of the intensity of input states can be controlled by using optical insulators, which weaken output reflected states to the necessary level. This level is assumed to be known and determines the probability of distinguishability of output probe states.

The further consideration implies the application of the BB84 protocol, as the most widely used. The phase modulator can be in four states corresponding to the values $x = 0$ and 1 in the direct, $b = +$, and conjugate, $b = \times$, bases. Let $|\psi_{x_b}\rangle_{\mathrm{PM}}$ be states reflected from the phase modulator corresponding to these four values.

The decoy state method [17, 23] usually involves states with three different intensities (average numbers of photons) μ, ν_1, and ν_2, which correspond to three different states of the intensity modulator. Let $|\psi_\xi\rangle_{\mathrm{MI}}$ be states reflected from the intensity modulator for three intensities (average numbers of photons) $\xi = \mu, \nu_1$, and ν_2. There are 12 reflected states in the side active probing channel:

$$|\psi_{x_b\xi}\rangle_{\mathrm{PMMI}} = |\psi_{x_b}\rangle_{\mathrm{PM}} \otimes |\psi_\xi\rangle_{\mathrm{MI}}. \quad (1)$$

If coherent states are used in practice as input probe states, the state at the output to the communication channel after reflection from an active optical element will be a coherent state with the shifted phase depending on the state of the active element and with a different intensity. In favor of Eve, reflected states are assumed pure because they have large distinguishabil-

ity. Under these assumptions, reflected states can be represented in the form

$$|\alpha_{x_b\xi}\rangle_{\mathrm{PMMI}} = |\alpha_{x_b}\rangle_{\mathrm{PM}} \otimes |\alpha_\xi\rangle_{\mathrm{MI}},$$
$$x_b = \{0+, 1+, 0\times, 1\times\}, \quad \xi = \{\mu, \nu_1, \nu_2\}. \tag{2}$$

2.1. Direct Distinguishing of States in Side Channel

The first strategy is reduced to direct distinguishing of 12 reflected probe states specified by Eqs. (1) and (2) by means of UMs. However, this strategy is not the best because UMs give a conclusive outcome with a low probability since 12 states should be distinguished.

This strategy provides a conclusive outcome with a probability of about $\mathrm{Pr}_{\mathrm{OK}} \approx \mu_{\max}^{11}$, where $\mu_{\max} = \max_{x_b,\xi}\{|\alpha_{x_b,\xi}|^2\}$ is the maximum average number of photons in reflected states.

It is assumed that the average number of photons in reflected states in the case of the use of optical insulators does not exceed the average number of photons in reflected states in information states $\mu \approx 0.2$–0.5, $\mu_{\max} < \max_\xi\{\xi\} = \mu \approx 0.2$–$0.5$. Under this attack, the probability of distinguishing the intensity of transmitted information states and values of the key bit is negligible; correspondingly, the attack in this form results in overly large losses. The following strategy will be efficient.

2.2. Measurement of the Intensity of States Reflected from the Intensity Modulator and the PNS Attack on Information States in the Quantum Communication Channel

The aim of Eve is to know the transmitted bit without generating errors and to avoid the detection by the decoy state method. To the last aim, Eve should know which of the states with the intensity μ, ν_1, or ν_2 is sent in each message.

Attack: Performing UMs, Eve distinguishes the states $|\alpha_\mu\rangle_{\mathrm{MI}}$, $|\alpha_{\nu_1}\rangle_{\mathrm{MI}}$, and $|\alpha_{\nu_2}\rangle_{\mathrm{MI}}$. If the outcome of the measurement is inconclusive, the message is blocked.

If the outcome is conclusive, the state $|\alpha_\mu\rangle_{\mathrm{MI}}$, $|\alpha_{\nu_1}\rangle_{\mathrm{MI}}$, or $|\alpha_{\nu_2}\rangle_{\mathrm{MI}}$ is known. Then, Eve performs nondestructive measurements of the number of photons in information states, i.e., PNS attack. If a message with the number of photons $k < 3$ is detected, it is blocked. If the number of photons detected in information states is $k \geq 3$, UMs of information states are performed.

The necessary and sufficient condition for the possibility of UMs is the linear independence of states [31]. If the basis in the BB84 protocol with phase encoding is unknown, it is necessary to distinguish four states. Four states in messages with three photons have the form

$$|\Phi_k^x\rangle = \sqrt{\frac{3!}{2^3}}\sum_{m=0}^{3} e^{i\varphi_x m}\frac{|m\rangle_1 \otimes |k-m\rangle_2}{\sqrt{m!(k-m)!}}; \tag{3}$$

i.e., four states specified by Eq. (3) become linearly independent beginning with three-photon messages.

Indeed, the basis vectors in the Fock subspace with three photons ($k = 3$) in two time windows are

$$|3\rangle_1|0\rangle_2, \quad |2\rangle_1|1\rangle_2, \quad |1\rangle_1|2\rangle_2, \quad |0\rangle_1|3\rangle_2.$$

Information states at $k = 3$ in two bases are given by three vectors (see Eq. (3)):

$$\text{basis} + \begin{cases} 0+ \to \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 + \frac{1}{\sqrt{2!}}|2\rangle_1|1\rangle_2 + \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 + \frac{1}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \\ 1+ \to \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 + \frac{1}{\sqrt{2!}}|2\rangle_1|1\rangle_2 - \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 - \frac{1}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \end{cases},$$

$$\text{basis} \times \begin{cases} 0\times \to \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 + \frac{i}{\sqrt{2!}}|2\rangle_1|1\rangle_2 - \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 - \frac{i}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \\ 1\times \to \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 - \frac{i}{\sqrt{2!}}|2\rangle_1|1\rangle_2 - \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 + \frac{i}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \end{cases}.$$

The Fock subspace for the single-photon component of states is two-dimensional; the number of information states is still four; consequently, they are linearly dependent. The subspace with two photons is three-dimensional; the number of information states is still four; therefore, they are linearly dependent. Hence, UMs of information states are possible only beginning with the three-photon component of states.

The probability $\mathrm{Pr}_\xi(k \geq 3)$, $\xi = \mu, \nu_1, \nu_2$ of the presence of messages with three or more photons in the quantum communication channel depends on the intensity of the information coherent state, i.e., the

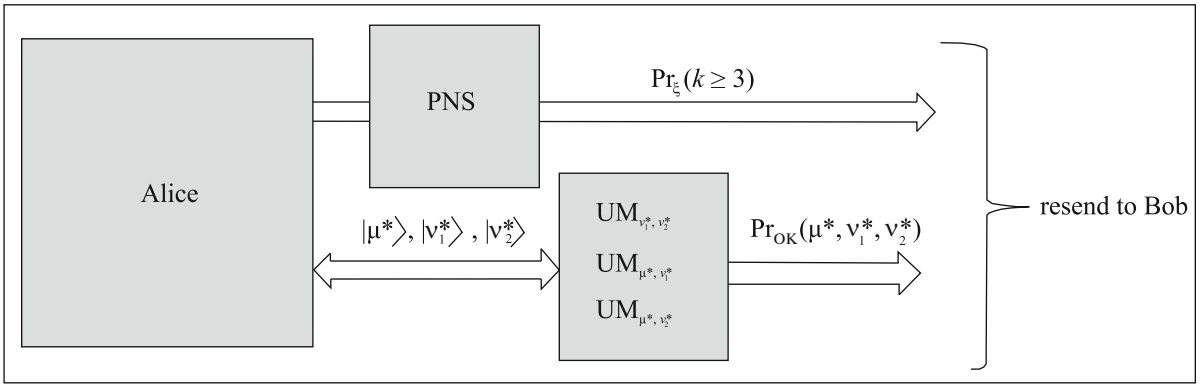

Fig. 1. Schematic diagram of the attack with unambiguous measurements of reflected states and PNS measurements of information states.

average number of photons in it μ, ν_1, or ν_2. This probability is given by the formula

$$\Pr_\xi(k \geq 3) = e^{-2\xi}\sum_{k=3}^{\infty}\frac{(2\xi)^k}{k!} \leq \xi^3. \quad (4)$$

To know the transmitted key bit, Eve should have messages with the number of photons $k \geq 3$ for messages with any intensity. Consequently, the probability of success is determined by the minimum probability of finding three or more photons in messages with different average number of photons $\xi = \mu$, ν_1, and ν_2. Taking into account the hierarchy of intensities $\mu > \nu_1 > \nu_2$, the minimum probability is found in the form

$$\Pr_{\min}(k \geq 3) = \min_{\xi = (\mu, \nu_1, \nu_2)}\left\{e^{-2\xi}\sum_{k=3}^{\infty}\frac{(2\xi)^k}{k!}\right\} \leq (\nu_2)^3. \quad (5)$$

After UMs of three-photon states, Eve knows the transmitted bit. If the outcome of UMs of information states is inconclusive, the message is blocked.

The PNS attack with subsequent UMs of information states and removal of inconclusive outcomes without knowledge to what message and with what average number of photons the three-photon state belongs distorts the statistics of photocounts in messages with different average numbers of photons μ, ν_1, and ν_2, which is detected by the decoy state method.

However, Eve has access to states reflected from the intensity modulator. Unambiguous measurements of these states at the conclusive outcome after the PNS attack and UMs of information states allow Eve, at the conclusive outcome for reflected states, to know both the information bit and the intensity (μ, ν_1, or ν_2) in this message.

As a result, at two successive conclusive outcomes, Eve knows the entire information on transmitted states, i.e., the key bit and the intensity (μ, ν_1, or ν_2). All other messages where the outcome is inconclusive in PNS and UMs of either information states or states reflected from the intensity modulator are blocked.

The minimum probability of a conclusive outcome when distinguishing states reflected from the intensity modulator can be estimated now. Optimal UMs for two pure states are known [29–31]. There are some results on distinguishing more than two pure and mixed states. To obtain particular numerical values, it is necessary to know the exact structure of quantum states and to use numerical minimization.

To estimate the probability of conclusive outcomes and the corresponding losses induced in this attack, it is more convenient to use exact analytical results to distinguish two states and to use cascade unambiguous measurements, where a pair of states are distinguished at each step, to distinguish three states (see Fig. 1). This method does not require numerical minimization.

2.3. Cascade Measurements of Probe States

Cascade UMs for distinguishing three states reflected from the intensity modulator, which are briefly denoted as $|\mu^*\rangle$, $|\nu_1^*\rangle$, and $|\nu_2^*\rangle$, contain two steps. At the first step, two states $|\nu_1^*\rangle$ and $|\nu_2^*\rangle$ are distinguished; more precisely, the third state is excluded at one of two conclusive outcomes. For example, after the exclusion of the state $|\nu_1^*\rangle$ at the first step, the states $|\mu^*\rangle$ and $|\nu_1^*\rangle$ remain undistinguished. After the exclusion of the state $|\nu_2^*\rangle$ at the first step, the states $|\mu^*\rangle$ and $|\nu_2^*\rangle$ remain determined and are distinguished at the second step of UMs (see Fig. 2). At the second step of UMs, two pairs of states (Fig. 2) $|\mu^*\rangle$ and $|\nu_1^*\rangle$ or $|\mu^*\rangle$ and $|\nu_2^*\rangle$ are distinguished.

The first step involves the measurement $UM_{\nu_1^*,\nu_2^*}$ (Fig. 2), which is given by the decomposition of unity

$$I = \mathcal{P}^{\perp}_{\nu_1^*} + \mathcal{P}^{\perp}_{\nu_2^*} + \mathcal{P}^{?}_{\nu_1^*,\nu_2^*}, \quad (6)$$

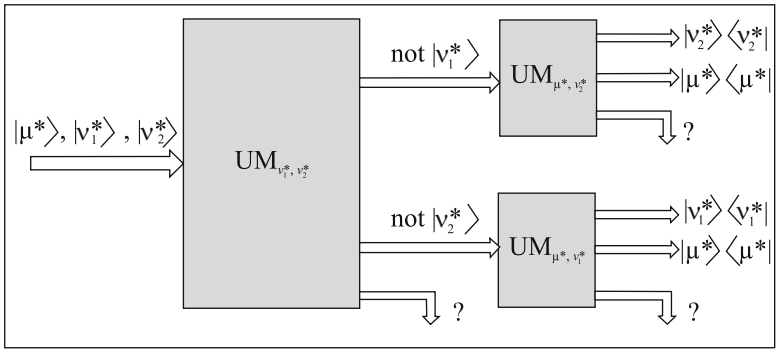

Fig. 2. Schematic diagram of the second unambiguous measurement cascade.

where

$$\mathcal{P}^{\perp}_{\nu_1^*} = \frac{I - |\nu_1^*\rangle\langle\nu_1^*|}{1 + |\langle\nu_1^*|\nu_2^*\rangle|}, \quad \mathcal{P}^{\perp}_{\nu_2^*} = \frac{I - |\nu_2^*\rangle\langle\nu_2^*|}{1 + |\langle\nu_1^*|\nu_2^*\rangle|}, \qquad (7)$$
$$\mathcal{P}^{?}_{\nu_1^*,\nu_2^*} = I - \mathcal{P}^{\perp}_{\nu_1^*} - \mathcal{P}^{\perp}_{\nu_2^*},$$

and I is the identity operator. The operator-valued measures $\mathcal{P}^{\perp}_{\nu_1^*}$ and $\mathcal{P}^{\perp}_{\nu_2^*}$ in Eqs. (6) and (7) up to normalization are projectors; i.e., $(\mathcal{P}^{\perp}_{\nu_1^*,\nu_1^*})^2 \propto \mathcal{P}^{\perp}_{\nu_2^*,\nu_2^*}$, which will be required below.

The probabilities of the conclusive outcome and states at the output on the first cascade have the form

$$UM_{\nu_1^*,\nu_2^*}\begin{cases} \text{not } |\nu_1^*\rangle \to \begin{cases} \Pr(|\nu_2^*| \text{ not } |\nu_1^*\rangle) = 1 - |\langle\nu_2^*|\nu_1^*\rangle|, \text{ output state } |\nu_2^*\rangle\langle\nu_2| \\ \Pr(|\mu^*| \text{ not } |\nu_1^*\rangle) = \dfrac{1 - |\langle\mu^*|\nu_1^*\rangle|}{1 + |\langle\nu_2^*|\nu_1^*\rangle|}, \text{ output state } |\mu^*\rangle\langle\mu^*| \end{cases} \to UM_{\mu^*,\nu_2^*} \\ \text{not } |\nu_2^*\rangle \to \begin{cases} \Pr(|\nu_1^*| \text{ not } |\nu_2^*\rangle) = 1 - |\langle\nu_2^*|\nu_1^*\rangle|, \text{ output state } |\nu_1^*\rangle\langle\nu_1^*| \\ \Pr(|\mu^*| \text{ not } |\nu_2^*\rangle) = \dfrac{1 - |\langle\mu^*|\nu_2^*\rangle|}{1 + |\langle\nu_2^*|\nu_1^*\rangle|}, \text{ output state } |\mu^*\rangle\langle\mu^*| \end{cases} \to UM_{\mu^*,\nu_1^*}. \end{cases} \qquad (8)$$

In view of Eq. (8), the probability of the conclusive outcome at the first step satisfies the inequality

$$\Pr_{OK}^{(1)} \le \min\{\Pr(|\mu^*| \text{ not } |\nu_1^*\rangle), \Pr(|\nu_1^*| \text{ not } |\nu_2^*\rangle), \Pr(|\nu_2^*| \text{ not } |\nu_1^*\rangle)\}. \qquad (9)$$

The second cascade of UMs (Fig. 2) is chosen depending on the outcome at the first step. One of two measurements is chosen; each measurement is specified a specific unity decomposition. When the outcome at the first step is (not $|\nu_1^*\rangle$), the measurement UM_{μ^*,ν_2^*} chosen in the second cascade is given by the decomposition of unity (Fig. 2)

$$I = \mathcal{P}^{\perp}_{\mu^*} + \mathcal{P}^{\perp}_{\nu_2^*} + \mathcal{P}^{?}_{\mu^*,\nu_2^*}, \qquad (10)$$

where

$$\mathcal{P}^{\perp}_{\mu^*} = \frac{I - |\mu^*\rangle\langle\mu^*|}{1 + |\langle\mu^*|\nu_2^*\rangle|}, \quad \mathcal{P}^{\perp}_{\nu_2^*} = \frac{I - |\nu_2^*\rangle\langle\nu_2^*|}{1 + |\langle\mu^*|\nu_2^*\rangle|}, \qquad (11)$$
$$\mathcal{P}^{?}_{\mu^*,\nu_2^*} = I - \mathcal{P}^{\perp}_{\mu^*} - \mathcal{P}^{\perp}_{\nu_2^*},$$

$$UM_{\mu^*,\nu_2^*}\begin{cases} \text{not } |\mu^*\rangle \to \Pr(|\nu_2^*| \text{ not } |\mu^*\rangle) = 1 - |\langle\mu^*|\nu_2^*\rangle|, & \text{output state } |\nu_2^*\rangle\langle\nu_2^*| \\ \text{not } |\nu_2^*\rangle \to \Pr(|\mu^*| \text{ not } |\nu_2^*\rangle) = 1 - |\langle\mu^*|\nu_2^*\rangle|, & \text{output state } |\mu^*\rangle\langle\mu^*|. \end{cases} \qquad (12)$$

If the outcome at the first step is (not $|\nu_2^*\rangle$), the measurement UM_{μ^*,ν_1^*} in the second cascade is given by the decomposition of unity (Fig. 2)

$$I = \mathcal{P}^{\perp}_{\mu^*} + \mathcal{P}^{\perp}_{\nu_1^*} + \mathcal{P}^{?}_{\mu^*,\nu_1^*}, \qquad (13)$$

where

$$\mathcal{P}^{\perp}_{\mu^*} = \frac{I - |\mu^*\rangle\langle\mu^*|}{1 + |\langle\mu^*|\nu_1^*\rangle|}, \quad \mathcal{P}^{\perp}_{\nu_1^*} = \frac{I - |\nu_1^*\rangle\langle\nu_2^*|}{1 + |\langle\mu^*|\nu_1^*\rangle|}, \quad \mathcal{P}^{?}_{\mu^*,\nu_1^*} = I - \mathcal{P}^{\perp}_{\mu^*} - \mathcal{P}^{\perp}_{\nu_1^*}, \tag{14}$$

$$\mathrm{UM}_{\mu^*,\nu_1^*} \begin{cases} \text{not } |\mu^*\rangle \to \Pr(|\nu_1^*\rangle| \text{ not } |\mu^*\rangle) = 1 - |\langle\nu_1^*|\mu^*\rangle|, & \text{output state } |\nu_1^*\rangle\langle\nu_1^*| \\ \text{not } |\nu_1^*\rangle \to \Pr(|\mu^*\rangle| \text{ not } |\nu_1^*\rangle) = 1 - |\langle\nu_1^*|\mu^*\rangle|, & \text{output state } |\mu^*\rangle\langle\mu^*|. \end{cases} \tag{15}$$

In view of Eqs. (10)–(15), the probability of the conclusive outcome at the second step satisfies the inequality

$$\Pr_{\mathrm{OK}}^{(2)} \le \min\Big\{\Pr(|\mu^*\rangle| \text{ not } |\nu_1^*\rangle), \Pr(|\nu_1^*\rangle| \text{ not } |\mu^*\rangle), \Pr(|\mu^*\rangle| \text{ not } |\nu_2^*\rangle), \Pr(|\nu_2^*\rangle| \text{ not } |\mu^*\rangle)\Big\}. \tag{16}$$

The resulting probability of the conclusive outcome in two cascades when measuring states reflected from the intensity modulator is no more than

$$\Pr_{\mathrm{OK}}(\min) = \Pr_{\mathrm{OK}}^{(1)}\Pr_{\mathrm{OK}}^{(2)}. \tag{17}$$

Under the assumption that reflected states are coherent, having different phases and average numbers of photons $\xi, \xi' \ll 1$, it follows from Eqs. (8), (12), and (15) that $1 - |\langle\xi|\xi'\rangle|^2 = 1 - e^{-|\xi - \xi'|^2} \le |\xi - \xi'|$, where $\xi, \xi' = \mu^*, \nu_1^*, \nu_2^*$.[1] In view of the natural hierarchy $\mu^* > \nu_1^* > \nu_2^*$ of the intensities of reflected states, the following estimate is obtained:

$$\Pr_{\mathrm{OK}}(\min) \le \mu^*\nu_1^*(\nu_2^*)^2. \tag{18}$$

2.4. Final Stage of the Attack—Resending of States to the Receiver Side

In messages where conclusive outcomes are obtained for reflected states and information states in the quantum communication channel, Eve knows both the information bit and the average number of photons in the state in this message.

All messages with the joint conclusive outcome are divided into three sets. The first, second, and third sets include messages where sent states have the average numbers of photons μ, ν_1, and ν_2, respectively. In all these messages, Eve also knows the transmitted key bit.

How can Eve use this attack so that errors do not appear on the receiver side and the relative statistics of photocounts in messages with different average number of photons does not change?

We recall that, if a coherent state with the *average number of photons* ξ passes through the communication channel with the transmission coefficient T and, correspondingly, with losses $1 - T$, states immediately at the input of the receiver side will have the form

$$\rho^x(\xi) \to \rho^x(\xi T) = e^{-2\xi T}\sum_{k=0}^{\infty}\frac{(2\xi T)^k}{k!}|\Phi_k^x\rangle\langle\Phi_k^x|. \tag{19}$$

Here, $T = 10^{-\frac{\delta L}{10}}$ is the transmission coefficient through the communication channel, where L is the length of the communication channel and δ is the relative loss coefficient. Correspondingly, the probability of components of states with a nonzero number of photons *at the input of the receiver side* is

$$Q(\xi T) = e^{-2\xi T}\sum_{k=1}^{\infty}\frac{(2\xi T)^k}{k!} = 1 - e^{-2\xi T}. \tag{20}$$

In other words, Eq. (20) is the probability that each component $|\Phi_k^x\rangle\langle\Phi_k^x|$ with the number of photons $k = 0,1\ldots$ reaches the input of the receiver side without distortions after the passage through the channel with losses. This probability is given by the expression

$$e^{-2\xi T}\frac{(2\xi T)^k}{k!}. \tag{21}$$

Let T_μ, T_{ν_1}, and T_{ν_2} be the transparencies of the channel satisfying the equalities

$$\Pr_{\mathrm{OK}}(\min)\mathrm{P}_\mu(k \ge 3) = Q(\mu T_\mu) \approx 2\mu T, \tag{22}$$

$$\Pr_{\mathrm{OK}}(\min)\mathrm{P}_{\nu_1}(k \ge 3) = Q(\nu_1 T_{\nu_1}) \approx 2\nu_1 T, \tag{23}$$

$$\Pr_{\mathrm{OK}}(\min)\mathrm{P}_{\nu_2}(k \ge 3) = Q(\nu_2 T_{\nu_2}) \approx 2\nu_2 T. \tag{24}$$

These formulas give the probability of the joint conclusive outcome for distinguishing states, the average number of photons in a given message, and the probability of determining the transmitted key bit. Informally, this is the fraction of messages with the average number of photons at different $\xi = \mu, \nu_1, \nu_2$ at which Eve knows the entire information on these messages.

Further, the minimum transmission coefficient T_ξ is selected from Eqs. (22)–(24)

$$T_{\min} = \min_{\xi\in\{\mu,\nu_1,\nu_2\}}\{T_\xi\} = \min_{\xi\in\{\mu,\nu_1,\nu_2\}}\left\{\frac{1}{\xi}Q^{-1}\big(\Pr_{\mathrm{OK}}(\min)\ \mathrm{P}_\xi(k \ge 3)\big)\right\}, \tag{25}$$

where $Q^{-1}(...)$ is the function inverse to $Q(...)$.

[1] Do not confuse the notation of the coherent state $|\xi\rangle$ with the average number of photons ξ.

Let $\xi = \nu_2$ for definiteness; then,

$$\begin{aligned} \mathrm{Pr}_{\mathrm{OK}}(\min)\mathrm{P}_{\mu}(k \geq 3) &\geq Q(\mu T_{\min}), \\ \mathrm{Pr}_{\mathrm{OK}}(\min)\mathrm{P}_{\nu_1}(k \geq 3) &\geq Q(\nu_1 T_{\min}), \\ \mathrm{Pr}_{\mathrm{OK}}(\min)\mathrm{P}_{\nu_2}(k \geq 3) &= Q(\nu_2 T_{\min}). \end{aligned} \tag{26}$$

Informally, Eqs. (26) specify the sizes of sets of messages with μ, ν_1, and ν_2 where Eve knows the entire information, i.e., the average number of photons and the transmitted key bit.

If $\xi = \mu$, in the fraction of messages

$$\frac{Q(\mu T_{\min})}{\mathrm{Pr}_{\mathrm{OK}}(\min)\mathrm{P}_{\mu}(k \geq 3)} \tag{27}$$

with the joint conclusive outcome, Eve *sends* states

$$|\Phi_k^x\rangle_{\mathrm{BB}}\langle\Phi_k^x| \tag{28}$$

with the necessary probabilities

$$e^{-2\mu T_{\min}} \frac{(2\mu T_{\min})^k}{k!}, \quad k \geq 1, \tag{29}$$

directly to the input of the receiver station (Bob, see Fig. 1). In the fraction of messages

$$1 - \frac{Q(\mu T_{\min})}{\mathrm{Pr}_{\mathrm{OK}}(\min)\mathrm{P}_{\mu}(k \geq 3)}, \tag{30}$$

Eve sends nothing to Bob (see Fig. 1) even if the joint conclusive outcome is obtained. In other words, the fraction of messages with the joint conclusive outcome from Eqs. (22) and (23) is excessive. The size of the set of messages with the joint conclusive outcome for messages with μ is larger than that required for inequalities (26) to be satisfied.

Eve acts similarly for messages with ν_1, where the joint conclusive outcome is obtained. In messages with ν_2, Eve delivers all messages with the joint conclusive outcome to the input of the receiver side.

As a result, states appearing *at the input of the receiver side* at any $\xi = \mu$, ν_1, and ν_2 are specified by the density matrices

$$\rho^x(\xi T_{\min}) = e^{-2\xi T_{\min}} \sum_{k=0}^{\infty} \frac{(2\xi T_{\min})^k}{k!} |\Phi_k^x\rangle_{\mathrm{BB}}\langle\Phi_k^x|, \quad \xi = \mu, \nu_1, \nu_2. \tag{31}$$

States at the input of the receiver side look like undistorted states transmitted through the channel with the transparency $T_{\min}$. In this case, the relative and internal Poisson statistics of states in the number of photons and Fock states themselves remain undistorted, and all states look like states transmitted through the same ideal channel with losses $1 - T_{\min}$. As a result, Bob sees undistorted states with undistorted internal and relative Poisson statistics for states with different ξ values at the input of the receiver side. We recall that the decoy state method does not follow losses and, therefore, cannot detect this attack.

2.5. Some Numerical Estimates

We make numerical estimates of losses generated by this attack. The observed losses depend on the average number of photons in probe states reflected from the intensity modulator. Let the average number of photons in reflected states, when the state of the intensity modulator corresponds to messages of information states with the average number of photons μ, be $\mu^* = 0.1$. Correspondingly, $\nu_1^* = 0.01$ and $\nu_2^* = 0.01$ for information messages with ν_1 and ν_2, respectively. In view of Eqs. (24) and (27), the transmission coefficient T_{Eve} (loss coefficient $1 - T_{Eve}$) under this attack satisfies the inequalities

$$\begin{aligned} \mathrm{Pr}_{\mathrm{OK}}(\min)\mathrm{Pr}_{\min}(k \geq 3) &\leq \nu_2 T_{\mathrm{Eve}}, \\ T_{\mathrm{Eve}} &\leq \mu^* \nu_1^* \nu_2^* \approx 10^{-5}. \end{aligned} \tag{32}$$

We recall that the probability of passage of the communication channel with the length $L = 100$ km and standard losses in the single-mode optic fiber $\delta = 0.2$ dB/km is $T_{100} = 10^{-\frac{\delta L}{10}} = 10^{-2}$, which is three orders of magnitude larger than that at this attack and used to estimate the intensity of reflected probe states. The lower the intensity of reflected states, the higher the losses introduced at this attack. A low intensity of reflected probe states can be ensured by using unilateral optical isolators at the output of the transmitter station. The attenuation coefficient of optical isolators will be determined by a particular technical implementation of a quantum cryptography system.

3. CONCLUSIONS

Quantum cryptography systems were proposed for quantum key distribution, where security is guaranteed by fundamental quantum mechanical constraints on the distinguishability of states. More precisely, the cloning of an unknown quantum state with *unit probability* is forbidden by the *no-cloning* theorem [37], which is an elegant reformulation of the fundamental Heisenberg–Robertson uncertainty relation [38, 39]. In application to quantum cryptography, this forbiddenness means that the eavesdropper cannot make a copy of an information state (correspondingly, any number of copies if one could be made) for eavesdropping measurements. The Heisenberg–Robertson uncertainty relation expresses the mathematical fact that a pair of uncommuted observables (Hermitian operators) cannot have a common system of eigenvectors. Therefore, any attacks on a quantum communication channel will inevitably generate errors on the receiver side.

The next fundamental fact is that quantum theory makes it possible to obtain the upper fundamental bound of information leakage to the eavesdropper at a given observed error on the receiver side. This fundamental bound can be obtained from entropy uncer-

tainty relations [11], which also follow from the noncommutativity of observables.

Everything stated above concerns single-photon states. Since a strictly single-photon source of information states is currently absent, real systems involve quasi-one-photon states of laser radiation, i.e., strongly weakened coherent states, which are superpositions of states with different Fock numbers of photons. The secret key is formed only from the single-photon component of states reaching the receiver side. The entire information contained in multiphoton components of states is assumed to be known to the eavesdropper (given to the eavesdropper). The decoy state method [21–23] allows estimating the fraction of the single-photon component reaching the receiver side.

Thus, deep understanding of attacks on information states in the quantum communication channel has been already achieved. However, quantum cryptography systems are open; i.e., the eavesdropper has access not only to the quantum communication channel but also to side information leakage channels and can actively probe optical components of the system—phase and intensity modulators—whose state carries information on the transmitted key. The measurement of probe states by the eavesdropper does not lead to errors on the receiver side because they do not perturb information states and is an additional information "bonus" for the eavesdropper.

The security of keys in quantum cryptography cannot be analyzed without the inclusion of information leakage through side channels.

In this work, a new attack on quantum cryptography systems is proposed involving a joint attack on information quantum states (PNS attack) and an attack with unambiguous measurements of reflected probe states from an intensity modulator in the side channel. This attack is not detected by known methods because it does not change the relative statistics of photocounts in the decoy state method, but it results only in additional losses in the quantum communication channel, which are not detected by the decoy state method. Moreover, it was previously believed that it is unnecessary to follow losses in the communication channel because they do not directly affect security if the decoy state method is used.

The consideration in this work shows that the inclusion of information leakage through side channels requires the inclusion of losses in the quantum communication channel to estimate the length of the secret key. Our estimates give the level of losses at a known maximum intensity of reflected probe states at which the eavesdropper knows the whole key, does not generate errors on the receiver side, and is not detected if general losses in the communication channel are not controlled. At the level of losses below a critical value, the eavesdropper will inevitably produce either errors or changes in the relative statistics of photocounts on the receiver side.

We again emphasize that the critical level of losses depends on a particular physical implementation of the quantum cryptography system, which determines the upper bound of the intensity of reflected probe states. The knowledge of this bound is fundamentally necessary to ensure the security of keys. In particular, if the system should guarantee the security of keys in a 100-km-long communication channel (the transmission coefficient $T = 10^{-2}$), and its physical implementation is such that the intensity of reflected states under the attack described above leads to critical losses of about the same value (the transmission coefficient $T_{\text{Eve}} = 10^{-2}$) or larger, the system cannot guarantee the security of transmitted keys; i.e., the eavesdropper is not detected.

The detection of the attack is ensured not by the quantum key distribution protocol but by the physical implementation of the system, which should be such that this eavesdropping attack generates losses noticeably exceeding losses in the communication channel with the length at which the system should operate.

To conclude, in order to avoid misunderstanding, it is noteworthy that the inclusion of side channels of information leakage does not transform quantum cryptography systems from the type of cryptographic systems where the security of keys is guaranteed by fundamental quantum mechanical laws to the type of systems where this security is guaranteed by technical restrictions. Even in the presence of side channels of information leakage, the security of keys is still guaranteed by fundamental quantum mechanical restrictions on the distinguishability of states.

The intensity (average number of photons) in information states, which are quasi-single-photon and single-photon ideally, emitted from the transmitter station is also reached by the weakening of the initial signal to a necessary level by means of technical tools. At a given intensity of signals, their maximum allowable, best possible distinguishability is dictated by quantum mechanics. The same is true for states in side channels. The upper bound of the intensity of states in side channels is reached by technical tools, i.e., by the implementation of the system that gives the upper bound of the distinguishability of states, which is also determined by the fundamental quantum-mechanical constraints.

ACKNOWLEDGMENTS

I am grateful to I.M. Arbekov, K.A. Balygin, S.P. Kulik, and A.N. Klimov for numerous stimulating discussions and to my colleagues at the Academy of Cryptography of the Russian Federation for stimulating discussions, remarks, and support.

FUNDING

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

REFERENCES

1. A. O. Bauer, in *The History of Military Communications, Proceedings of the 5th Annual Colloquium, Bournemouth Univ., September 24, 1999*.
2. Engineer Pamphlet EP 1110-3-2 (U. S. Army Corps of Engineers, Publ. Depot, Hyattsville, 1990).
3. W. van Eck, Comput. Secur. **4**, 269 (1985).
4. P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*, in *Proceedings of the 19th International Conference on Cryptology (CRYPTO'99),* Lect. Notes Comput. Sci. **1666**, 388 (1999).
5. P. Wright, *SpyCatcher: The Candid Autobiography of a Senior Intelligence Officer* (William Heinemann, Australia, 1987).
6. P. Smulders, Comput. Secur. **9**, 53 (1990).
7. M. G. Kuhn, Tech. Report No. UCAM-CL-TR-577 (Cambridge Univ. Press, Cambridge, 2003), p. 577.
8. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computer Systems and Signal Processing* (IEEE, 1984), p. 175.
9. R. Renner, PhD Thesis (ETH, Zürich, 2005); arXiv: 0512258.
10. J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
11. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
12. M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015); arXiv: 1506.01989.
13. K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).
14. W. Wang, K. Tamaki, and M. Curty, New J. Phys. **20**, 083027 (2018).
15. S. N. Molotkov, Laser Phys. Lett. **17**, 015203 (2020).
16. S. N. Molotkov, K. A. Balygin, A. N. Klimov, and S. P. Kulik, Laser Phys. **29**, 124001 (2019).
17. S. N. Molotkov and K. A. Balygin, Laser Phys. **30**, 065201 (2020).
18. S. N. Molotkov, J. Exp. Theor. Phys. **130**, 809 (2020).
19. S. N. Molotkov, JETP Lett. **111**, 653 (2020).
20. S. N. Molotkov, JETP Lett. **111**, 506 (2020).
21. W.-Y. Hwang, arXiv: 0211153 [quant-ph].
22. X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
23. H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, arXiv: 0503005 [quant-ph].
24. S. N. Molotkov, J. Exp. Theor. Phys. **126**, 741 (2018).
25. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
26. A. Chefles, Phys. Lett. A **239**, 339 (1998).
27. I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
28. D. Dieks, Phys. Lett. A **126**, 303 (1988).
29. G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
30. A. Peres and D. R. Terno, J. Phys. A **31**, 7105 (1998).
31. U. Herzog, Phys. Rev. A **75**, 052309 (2007).
32. T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301 (2003).
33. P. Raynal and N. Lütkenhaus, Phys. Rev. A **72**, 022342 (2005).
34. S. W. Allison, G. T. Gillies, D. W. Magnuson, and T. S. Pagano, Appl. Opt. **24**, 1 (1985).
35. L. W. Tutt and T. F. Boggess, Prog. Quantum Electron. **17**, 299 (1993).
36. R. M. Wood, *Laser-Induced Damage of Optical Materials* (Institute of Physics Publishing, Bristol, 2003).
37. W. K. Wooters and W. H. Zurek, Nature (London, U.K.) **299**, 802 (1982).
38. W. Heisenberg, Z. Phys. **43**, 172 (1927).
39. H. P. Robertson, Phys. Rev. **34**, 163 (1929).

Translated by R. Tyapaev