ISSN 0030-400X, Optics and Spectroscopy, 2011, Vol. 111, No. 5, pp. 685–688. © Pleiades Publishing, Ltd., 2011.
Original Russian Text © D.B. Horoshko, D.I. Pustakhod, S.Ya. Kilin, 2011, published in Optika i Spektroskopiya, 2011, Vol. 111, No. 5, pp. 719–723.

Time-Shift Quantum Key Distribution: Sensitivity to Losses[1]

D. B. Horoshko[a, b], D. I. Pustakhod[a], and S. Ya. Kilin[a]

[a] *Stepanov Institute of Physics, National Academy of Sciences, Minsk, 220072 Belarus*
[b] *Laboratoire PhLAM, Université de Lille 1, Villeneuve d'Ascq, 59655 France*
e-mail: horoshko@ifanbel.bas-net.by; d.pustakhod@ifanbel.bas-net.by; kilin@ifanbel.bas-net.by

Received April 18, 2011

Abstract—The sensitivity to losses of a recently proposed protocol of time-shift quantum key distribution with the use of decoy states is studied. An attack with discrimination of all states is analyzed. It is established that the use of decoy states ensures the security of the protocol at a high level of losses up to 11.7 dB.

DOI: 10.1134/S0030400X11110129

1. INTRODUCTION

Quantum key distribution (QKD) is a technique that provides creation of two identical random strings of symbols (a cryptographic key) for two remote users, with guarantees that the third party, a possible eavesdropper, has a negligibly small quantity of information [1]. The most important part of this process is sending quantum systems (optical pulses) along a quantum communication channel (optical fiber or open space) from one user to the other. The unconditional security of QKD protocols is based on the impossibility of cloning the state of an individual quantum system [2], which is followed by the inevitability of distortions of the quantum carrier's state during an attempt to read out the information recorded on it. However, a quantum, as well as a classical, quantum communication channel is susceptible to two sources of distortions: noises and losses. This, in principle, permits an eavesdropper to mask his invasion. Thus, the analysis of the sensitivity of the QKD protocol to noises and losses is necessary in determining the conditions of a reliable work of the protocol.

During the last quarter of the last century, a large amount of different QKD schemes were developed and implemented [1]. The search for new and simpler methods for coding information in a quantum communication line resulted in a method of coding information through a time interval of photon emission [3–6]. In practice this means that time shifts are introduced into light pulses that are sent into the communication line. This method of time-shift coding has the advantage of relative simplicity in the construction of the sending and receiving equipment and a low level of errors in the transmitted data. However, the QKD protocols that have been developed based on this method are not free from drawbacks that can threaten protection from eavesdropping. The recently proposed time-shift QKD protocol using decoy states [7] has a high degree of protection with insignificant complication of the construction. Some attacks on the proposed protocol were analyzed, and the limit values of noise parameters at which a secure distribution of the key is possible were found. It was also demonstrated that the use of decoy states eliminates the 50% restriction on losses in the signal channel that is inherent to the two-state protocol.

In this work the sensitivity of the proposed protocol to losses in the quantum communication line is analyzed and the maximally admissible level of the losses is established. The QKD protocol that was proposed in [7] is reported in Section 2 with insignificant modifications. In Section 3 the structure of quantum states that are used for sending information is analyzed. In Section 4 the maximally admissible level of losses is established.

2. PROTOCOL

Information Coding

Information from the sending party to the receiving party (below, Alice and Bob, respectively) is transmitted by sending light pulses along an optical fiber which plays the role of a quantum communication channel. The schematic diagram of the setup is presented in Fig. 1 and is explained in the course of this section. Information is sent cycle by cycle, and, in every cycle with duration T_L, one of four signals is sent to the quantum channel: a reference pulse, signal pulses "0" and "1," or a decoy pulse (Fig. 2).

Reference pulses (Fig. 2a) are used for synchronization of the clocks of the transmitting and receiving

[1] The essentials of the paper were reported at the 13th International Conference on Quantum Optics and Quantum Information (May 28–June 1, 2010, Kyiv, Ukraine).

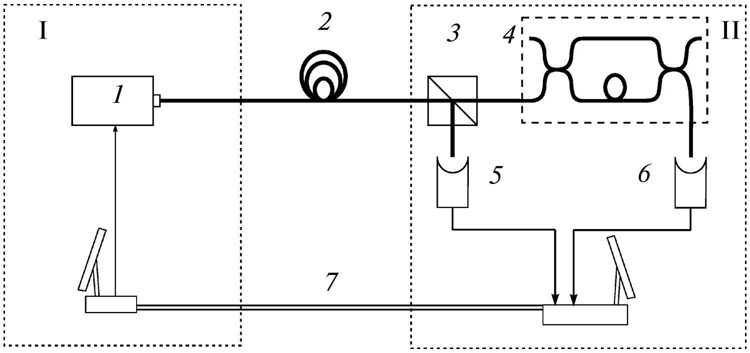

Fig. 1. Schematic diagram of the setup for the implementation of the time-shift QKD protocol. I is the transmitting station (Alice) and II is the receiving station (Bob). (*1*) Laser source of light pulses, (*2*) fiber optical communication line (quantum channel), (*3*) fiber beamsplitter, (*4*) fiber interferometer with a delay in one arm, (*5*) signal photodetector, (*6*) check photodetector, and (*7*) classical communication channel.

stations. They contain a large number of photons, and their temporal position is known to the users and the potential enemy beforehand.

For the signal pulses, rectangular coherent pulses with duration $T = 2T_L/3$ containing $\mu < 1$ photons on average are used. When the "0" value is transmitted, a pulse the beginning of which coincides with the beginning of the cycle is generated (Fig. 2b); during the transmission of "1," the pulse is shifted to a half of its length $T/2$ (Fig. 2c). Alice, also randomly, inserts into the sequence the decoy pulses that are used to check the coherence of the sent pulses and detect eavesdropping. The duration of the pulses is equal to the duration of the cycle, i.e., $3T/2$, and the photon flux is two-thirds of the flux of the signal pulses (Fig. 2d). Thus, the decoy pulses also contain μ photons on the average (this is the difference from the protocol that was considered in [7]). When the information exchange via the quantum channel is over, Alice, using the classical communication channel, sends to Bob the numbers of the cycles into which the decoy pulses were inserted.

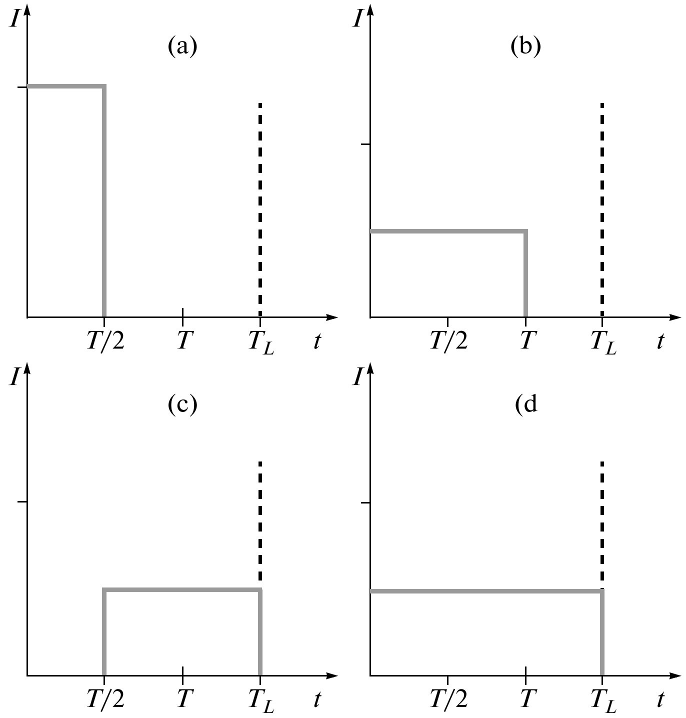

Fig. 2. Light pulses used for sending information in a quantum channel: (a) reference pulse, (b) signal pulse "0," (c) signal pulse "1," and (d) decoy pulse.

Information Decoding

At the receiving party (Bob), the light flux is divided into two equal parts by a beamsplitter. One part is directed to the signal detector and the other to the coherence checking block containing an interferometer. The signal detector operates in the mode of photon counting and records the times of photons falling on it. After the synchronization of the generators on the base of strong reference pulses for each photon detected in the signal cycle, Bob calculates the time of its detection with respect to the beginning of the cycle. Bob divides the whole cycle into three windows with duration $T/2$ each and decodes the obtained sequence in the following way: if the detection time lies in the first ([0, $T/2$]) or in the third ([T, $3T/2$]) windows, then the received photon is considered as informative with the value "0" or "1," respectively. If the time of photon detection lies in the second window ([$T/2$, T]), this count is not taken into consideration. When the communication session is over, Bob reports the numbers of cycles with informative values to Alice and she retains only the values that were sent in these cycles. Thus, Alice and Bob form the so-called "sifted sequences," from which the cryptographic key will be then obtained by means of the classical postprocessing.

The second half of the beam is directed to the coherence checking block which includes an unbalanced Mach–Zehnder interferometer and a detector which checks one of its outputs. The difference of the optical length of the path between the interferometer arms δl is approximately $vT/2$, where v is the speed of light in the optical fiber. This means that a pulse with duration T or $2T/3$ is divided in the interferometer into two halves passing along the long and short arms and the front part of one half of the pulse interferes with the rear part of the other half. The exact value of δl depends on temperature and smoothly varies in time. In connection with this, the difference of phases between the interfering halves of the pulse also varies, which leads to a periodic change of the signal at the output of the interferometer, where the minimums and maximums correspond to the destructive and constructive interference, respectively. After Alice announces via a classical channel the numbers of cycles in which the decoy pulses were sent, Bob calculates for these pulses the number of photons N_P at the check detector in the second and third temporal windows for a certain summation time T_S. The summation time should be much less than the characteristic time of the phase change of the interferometer. If this condition is satisfied, the variation of N_P in time will be an interference pattern reflecting the degree of coherence of decoy pulses coming to Bob's station. The visibility of this pattern will be always below 1, and with its drop below the value $V_0 = 0.67$ the protocol ceases to be secure [7].

3. STRUCTURE OF STATES OF THE INFORMATION CARRIER

In the limit of a small average number of photons, the quantum state of the pulse of a field that is created by sharp opening and closing of the shutter placed in the path of a monochromatic plane-polarized light beam that is characterized by the photon flux F, frequency ω_0, and phase ϕ and that propagates in the direction of the x axis is given by the following expression [7]:

$$|\psi(t, t_0, T_P, F, \phi)\rangle = \sqrt{1 - FT_P}|0\rangle \\ - ie^{i\phi}\sqrt{\frac{Fc}{2\pi}} \int_{t_0}^{t_0+T_P} d\tau e^{-i\omega_0(\tau - t_0)} \int_{-\infty}^{\infty} dk e^{-ikc(t-\tau)} a_k^+|0\rangle, \tag{1}$$

where t is the current time instant, t_0 is the time at which the front edge of the pulse meets the point $x = 0$, T_P is the pulse duration, $|0\rangle$ is the vacuum state of all field modes, and a_k^+ is the creation operator of a photon with a wave vector k satisfying the commutative relation $[a_k, a_{k'}^+] = \delta(k - k')$. It is easy to find that the average number of photons in a pulse is $\mu = FT_P$.

Using formula (1) two signal states and the decoy state of the protocol that was described above can be written in the form

$$|\psi_0\rangle = \sqrt{1-\mu}|0\rangle + \sqrt{\mu/2}(|1\rangle + |2\rangle), \tag{2}$$

$$|\psi_1\rangle = \sqrt{1-\mu}|0\rangle + \sqrt{\mu/2}(|2\rangle + |3\rangle), \tag{3}$$

$$|\psi_d\rangle = \sqrt{1-\mu}|0\rangle + \sqrt{\mu/3}(|1\rangle + |2\rangle + |3\rangle), \tag{4}$$

where the states $|1\rangle$, $|2\rangle$, and $|3\rangle$ are the single-photon part of state (1):

$$|n\rangle = -ie^{i\phi}\sqrt{\frac{c}{\pi T}} \int_{t_n}^{t_n+T/2} d\tau e^{-i\omega_0(\tau - t_n)} \int_{-\infty}^{\infty} dk e^{-ikc(t-\tau)} a_k^+|0\rangle, \tag{5}$$

with similar pulse durations $T/2$ and initial instants taking the values $t_1 = 0$, $t_2 = T/2$, and $t_3 = T$; the time is counted from the beginning of the cycle. This means that they describe a photon localized in the first, second, or third window, respectively. One can easily see that all four states $\{|n\rangle, n = 0, 1, 2, 3\}$ are normalized and mutually orthogonal. This follows that the states (2), (3), and (4) are linearly independent.

4. ATTACK WITH DISCRIMINATION OF STATES

Since three states of a quantum information carrier are linearly independent vectors in the space of states, these states can be subjected to the so-called measurement of unambiguous discrimination [8]. The measurement of this type is used when it is known that the system is in one of N linearly independent states. This measurement has $N + 1$ outcomes; N of them correspond to the detection of one of possible states with conditional probabilities $\{p_m, m = 1, \ldots, N\}$ and one more outcome is indefinite; i.e., it does not correspond to any knowledge about the state of the system.

If QKD is implemented using a quantum channel with a sufficiently low transmission coefficient in the intensity η, the unambiguous discrimination of states permits an enemy (traditionally called Eve) to organize the following attack. Eve replaces the quantum channel with losses by a more perfect channel having negligibly small losses. Then at one of the points of this channel, Eve subjects the pulses that go from Alice (except reference ones) to the unambiguous discrimination with equal conditional probabilities of detection of all three states $p_m = \mu\eta$. In the case of successful detection of the state of the pulse, $\{|\psi_m\rangle, m = 0, 1, d\}$, Eve sends to Bob a pulse occupying the same temporal windows but containing exactly one photon, i.e., the state

$$|\varphi_m\rangle = \mu^{-1/2}(1 - |0\rangle\langle 0|)|\psi_m\rangle. \tag{6}$$

If this operation requires some time, the reference pulses are delayed for the same time. In the case of an indefinite result, Eve does not send anything to Bob. As a result individual photons come to Bob's station in the corresponding windows with the average rate $\mu\eta$, like in the absence of interception. Thus, remaining invisible, Eve completely supervises the exchange of states in the quantum channel and, as a consequence, the generated key.

Certainly, the described attack is possible only upon sufficiently high losses of the quantum channel, namely, when $\mu\eta$ becomes less or equal to the maximal probability $p_{\max}$ of the "equally probable" discrimination of three states $\{|\psi_m\rangle,\ m = 0, 1, d\}$. Let us find this value.

By virtue of the fact that all three discriminated states (2), (3), and (4) have the same vacuum component, Eve can first project the state of the pulse on a single-photon subspace, which will have the probability of a success μ, and then discriminate three states $|\varphi_m\rangle$, which lie in the single-photon subspace and are linearly independent. Since we are interested in the procedure of the "equally probable" discrimination at which the conditional probability of obtaining the outcome m in the measurement of the state $|\varphi_m\rangle$ does not depend on m ($P_m = P$), the maximal value P can be found analytically [8] as a reciprocal of the maximal eigenvalue $\lambda_{\max}$ of the operator

$$\Lambda = \sum_{m=1}^{3} \frac{|\varphi_m^{\perp}\rangle\langle\varphi_m^{\perp}|}{|\langle\varphi_m^{\perp}|\varphi_m\rangle|^2}, \tag{7}$$

where $|\varphi_m^{\perp}\rangle$ is the state orthogonal to two states $\{|\varphi_l\rangle,\ l \neq m\}$ in the linear span of all three discriminated states. Using Eqs. (2), (3), (4), and (6), we find

$$|\varphi_0^{\perp}\rangle = (-|2\rangle + |3\rangle)/\sqrt{2}, \tag{8}$$

$$|\varphi_1^{\perp}\rangle = (|1\rangle - |2\rangle)/\sqrt{2}, \tag{9}$$

$$|\varphi_d^{\perp}\rangle = (|1\rangle - |2\rangle + |3\rangle)/\sqrt{2}. \tag{10}$$

By substituting these expressions into (7) and solving the characteristic equation for the 3 × 3-matrix, we obtain, after some computations, $\lambda_{\max} = (15 + \sqrt{201})/2 \approx 14.6$. Thus, the maximal value of the conditional probability of detecting the state $|\varphi_m\rangle$ is $P_{\max} = 1/\lambda_{\max} \approx 0.068$. Taking into account that the probability of successful projection on a single-photon subspace is μ, we obtain for the described attack that $p_{\max} = \mu P_{\max} \approx 0.068\mu$. Thus, Eve completely takes over the control of the quantum channel if the channel transmission is $\eta = 6.8\%$, i.e., if the signal is attenuated at the level of 11.7 dB, which corresponds to the distance of 58.5 km with the use of a standard telecommunication fiber with losses of 0.2 dB/km.

5. CONCLUSIONS

In this work the sensitivity of the time-shift QKD protocol with the use of decoy states to the losses in the quantum communication channel was studied and it was shown that the protocol becomes insecure at losses above 11.7 dB. This value is much higher than the limit of 3 dB that occurs with the use of only two signal states and does not permit one to implement the QKD scheme at distances that exceed 15 km. Further studies in this direction may be connected with the use of linearly dependent states of optical pulses that exclude the possibility of errorless discrimination of all states at any level of losses.

ACKNOWLEDGMENTS

The work was supported by the Belarusian Republic Foundation for Fundamental Research (project no. F10R-123), as well as by a project of the Seventh Framework Program of the European Commission (HIDEAS FP7-ICT-221906).

REFERENCES

1. S. Ya. Kilin, Usp. Fiz. Nauk **169**, 507 (1999).
2. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
3. S. N. Molotkov, JETP Lett. **79** (9), 445 (2004).
4. S. N. Molotkov, JETP Lett. **79** (8), 563 (2004).
5. T. Debuisschert and W. Boucher, Phys. Rev. A **70**, 042306 (2004).
6. W. Boucher and T. Debuisschert, Phys. Rev. A **72**, 062325 (2005).
7. D. B. Horoshko, D. I. Pustakhod, and S. Ya. Kilin, Opt. Spectrosc. **108** (3), 336 (2010).
8. A. Chefles, Phys. Lett. A **239**, 339 (1998).

Translated by A. Nikol'skii