ISSN 1063-7397, Russian Microelectronics, 2006, Vol. 35, No. 1, pp. 31–36. © Pleiades Publishing, Inc., 2006.
Original Russian Text ©V.L. Kurochkin, I.I. Ryabtsev, I.G. Neizvestny, 2006, published in Mikroelektronika, 2006, Vol. 35, No. 1, pp. 37–43.

Quantum Cryptography and Quantum-Key Distribution with Single Photons

V. L. Kurochkin, I. I. Ryabtsev, and I. G. Neizvestny

Institute of Semiconductor Physics, Siberian Division, Russian Academy of Sciences, Novosibirsk, Russia
e-mail: kurochkin@isp.nsc.ru

Received September 5, 2005

Abstract—A brief overview of the current status of quantum cryptography is given. The results are presented of our preliminary experiments with free-space quantum-key distribution by means of single linearly polarized photons with coded polarization states according to the BB84 protocol, for which purpose a quantum-cryptography communication system is designed. Single photons are detected with a 50% probability using specially designed high-speed photodetectors based on silicon avalanche photodiodes, operated in Geiger mode with active avalanche quenching. A key generation rate of 3.8 kbit/s is obtained, the mean photon number per pulse being 0.2.

DOI: 10.1134/S1063739706010045

1. INTRODUCTION

Quantum cryptography is a new field of research in telecommunications whose ultimate goal is to ensure absolute security of data communications over fiber or free-space optical channels [1]. The problem is that the most common cryptographic technique, Rivest–Shamir–Adleman (RSA) encryption, presupposes that no one knows a fast algorithm for factorizing large integers. However, it is possible that such an algorithm will emerge in the near future; in fact, it has been devised for quantum computers [2], although these are still at an exploratory stage.

The idea behind quantum cryptography is to create a secret quantum key during the transmission of single photons from a sending to a receiving party, commonly called Alice and Bob, respectively [1]. The security against eavesdropping by a third party called Eve comes from laws of quantum mechanics: (1) Any measurement of the state of a quantum entity changes this state. (2) It is not possible to reliably identify an unknown state of a quantum entity by a single measurement [3]. Consequently, any attempted attack on the data transmission will unavoidably cause an irreversible change in the quantum states of data-carrying single photons, providing unambiguous evidence of the attack.

The first quantum-cryptography protocol, commonly known as the BB84, was proposed in 1984 by Bennett and Brassard [4]. In broad terms, a quantum key is created as follows. Alice produces single linearly polarized photons whose polarization can have one of the four possible orientations 0°, +45°, +90°, and –45°, which make up a rectilinear (0°, +90°) and a diagonal (+45°, –45°) basis. Alice and Bob have an agreement as to which logical value is to be assigned to each polarization; for example, polarizations of 0° and +45° may correspond to logical zero, and polarizations of +90° and –45° to logical one. During a communication session, Alice sends a sequence of single photons whose polarizations are chosen at random. Bob detects the photons and chooses at random a polarization measurement basis for each of them, using a polarization beam splitter. Over an additional, open channel, Bob then informs Alice which basis he has taken for the measurement but does not communicate the result. Eve cannot gain anything from the situation because any detected photon may correspond to 0 or 1. In reply to Bob's message, Alice informs Bob whether or not he chose the appropriate polarization measurement basis for each detected photon. Finally, Alice and Bob accept only the measurement results that have been obtained in identical bases. A unique random sequence of 0's and 1's is thus created that constitutes a secret binary quantum key.

Quantum cryptography has been an active field of research and development since the first successful implementation of the BB84 protocol [5]. Quantum-key distribution (QKD) was first effected to a distance of 30 cm [5]. Currently, a range of over 20 km is achieved in the atmosphere [6], and plans are under way for ground-to-satellite QKD [7].

The BB84 protocol allows photon states to be coded in terms of polarization, phase, frequency, etc. [1]. Polarization coding is mostly used in free-space channels. With optical fiber, phase rather than polarization coding is the most common technique on account of severe polarization distortions. It is set up by a phase modulator inserted into one leg of an optical-fiber

Mach–Zehnder interferometer. The best experimental results were achieved with a plug-and-play self-cancellation scheme first implemented by Stucki *et al.* [8] and further developed by Kosaka *et al.* [9] and Kimura *et al.* [10]. This scheme works as follows. On Bob's side, short laser pulses containing many photons are first passed through two legs of a Mach–Zehnder interferometer. This has a delay line in one of the legs to split an input pulse in two. One of them has its phase shifted by a phase modulator. The pulses are then transmitted over a quantum channel formed by a single-mode fiber several tens of kilometers long. On Alice's side, the pulses are first reflected by a Faraday mirror providing self-cancellation of polarization distortion by the channel, the first pulse is passed through a phase modulator, and both pulses are attenuated to the single-photon level and sent to Bob. The scheme has been tested successfully at a range of 150 km [10]. On the other hand, it is vulnerable to the Trojan-horse attack by Eve [1].

In addition to the BB84 protocol, other procedures have been proposed, involving two [11] or six [12] basis states. Moreover, Ekert [13] advanced a radically new conception of QKD in which a quantum key is created by means of entangled photon pairs; it is based on the Einstein–Podolsky–Rosen thought experiment [14]. A successful test of this scheme through an intracity line has recently been reported [15].

Quantum cryptography proved so attractive both in concept and in application potential that different teams immediately embarked on its implementation. An extensive review of theoretical and experimental research in this field up to 2002 was given by Gisin *et al.* [1]. More recently, some new concepts of quantum communication channel were proposed, and many experiments were conducted with the aim of increasing QKD range. As an example, we cite works by Molotkov [16, 17] on relativistic quantum cryptography. Also, Yelin and Wang [18] proposed a time–frequency coding scheme, and Inoue *et al.* [19, 20] devised a QKD technique that uses the phase shift between two successive single photons.

2. EXPERIMENTAL SETUP

This paper reports on experimental demonstrations of free-space QKD with polarization coding of single photons by the BB84 protocol, for which purpose a quantum-cryptography communication system was built. The aim was to investigate methods for the generation of single photons in a given polarization state, their detection, and original-state identification. The experiments included simulation of unauthorized photon interception in the quantum channel. Evidence was obtained that such interception can be detected.

The communication system consists of a transmitting and a receiving unit shown in Figs. 1 and 2, respectively. The transmitting unit is based on four ILPN-210 semiconductor lasers (*2*) producing pulses with different polarizations:0°, +45°, 90°, and –45°. The four laser beams are combined into a single beam by mirrors (*5*) and attenuated by an absorbing filter (*6*) at the output. Computer-controlled current sources (*1*) provide a modulated injection current to generate laser pulses 8–10 ns wide at a wavelength of about 830 nm. Peltier cooling elements (*3*) ensure a stable operating temperature.

The communication channel is an air-filled enclosed space 70 cm long (impervious to external light).

In the receiving unit (Fig. 2), an input beam is split in two by a semitransparent mirror (*1*). The transmitted beam is passed through a Glan-prism polarization beam splitter (*3*), which guides photons of polarization 0° or +90° to appropriate photodetectors (*4*); polarization separation is done to 10^4 or better. Photons of polarization +45° or –45° can reach either photodetector with equal probabilities, 50%. The beam reflected from the semitransparent mirror is passed through a half-wave plate ($\lambda/2$) that rotates the polarization through 45° so that photons of polarization +45° or –45° can be separated by a second Glan-prism polarization beam splitter and guided to appropriate photodetectors. Photons of polarization 0° or +90° can reach either of these photodetectors with equal probabilities.

In the transmitting unit the laser power is selected such that most of the output pulses contain a single photon. The number of photons per pulse is known to have a Poisson distribution. In quantum cryptography a pulsed signal is considered to be a single-photon signal if the mean number $\bar{n}$ of photons per pulse is 0.1 to 0.2 [1]. For example, $\bar{n} = 0.1$ implies that the number of two-photon pulses is 5% of that of single-photon ones, and the percentage of three-photon pulses is 0.16%; consequently, nine out of every ten pulses have no photons. A transmitted photon of any polarization can reach any of three photodetectors: one of them corresponds to the photon's basis, and the rest correspond to the other basis, being accessible with equal probabilities (the complementary photodetector designated for the photon's basis is inaccessible due to the Glan prism). The proportion of multiphoton pulses can be evaluated during transmission on the basis of a Poisson distribution by taking signals from all the four photodetectors simultaneously and counting coincident signals. A desired mean number of photons per pulse is achieved by adjusting the output powers of the lasers one by one.

The single-photon nature of confidential transmission places heavy demands on the performance of the photodetectors, which serve as fast single-photon counters. They must have high quantum efficiency and low noise as well as high counting rate. Free-space QKD systems operate in the wavelength band 800–900 nm, an optical window of the atmosphere [6, 21]. The best single-photon detectors currently available are silicon avalanche photodiodes.

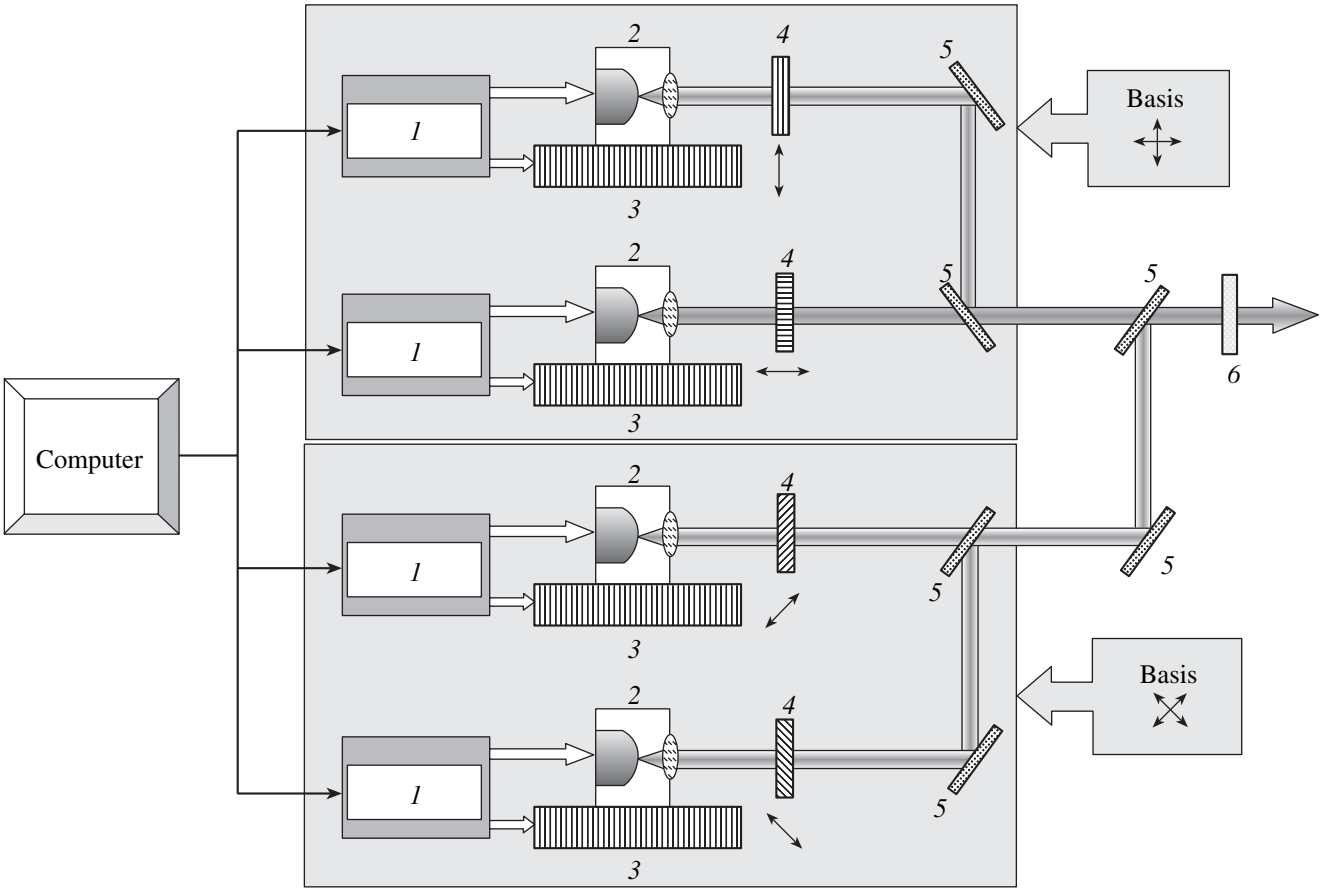

Fig. 1. Transmitting unit of the experimental QKD system with single linearly polarized photons: (*1*) computer-controlled laser-current sources, (*2*) semiconductor lasers, (*3*) Peltier cooling elements, (*4*) polarizers (Glan prisms), (*5*) mirrors, and (*6*) absorbing filter.

We selected EG&G's C30902S avalanche photodiodes, which are among the most sensitive models for the 800-nm band. They were employed in specially designed single-photon counters with active avalanche quenching [22, 23], offering a maximum count rate of 5 MHz and an output pulse width of 8–10 ns. Photon counting is realized by operating the photodiodes in Geiger mode, in which a single photon can induce a charge-carrier avalanche if the photodiode is biased to above the breakdown voltage V_{br}. The gain of such photodiodes can reach 10^5. The signal from a photodiode's load resistance (50 Ω) is boosted by an amplifier and fed into a pulse former that is implemented in transistor–transistor-logic (TTL) technology and serves as an interface to a computer. Peltier cooling elements are used to maintain the operating temperature at –20°C in order to reduce the photodiode's noise. The rate F of noise pulses depends on the temperature and the excess bias voltage above the photodiode breakdown level, $V - V_{br}$. Figure 3 shows a measured variation of F with $(V - V_{br})$ at –20°C. The saturation segment corresponds to the maximum probability of photon detection, whose rated value is 50% for a wavelength of 830 nm.

In contrast to other designs [22, 23], our photodetector circuit is provided with active current-limiting capability to protect the photodiode from breakdown under intense illumination, which may render C30902S photodiodes inoperative; different modes of current limitation are possible. The height of the avalanche-quenching pulse is adjustable over the range 5–25 V. The circuit also provides signal-level discrimination and includes time-gating capability; the gate pulse is adjustable for delay and width, the minimum width being 30 ns. The output signals of the photodetector can be fed into analog and digital instruments (oscilloscopes, computers, etc.). Figure 4 depicts the measured dependence of photodetector output pulse rate on laser-pulse repetition rate for different laser intensities, with the maximum count rate set to 2.5 MHz.

A quantum key is generated as follows. Clock pulses are generated in the transmitting unit at a rate equal to the laser pulse rate, which is set by the computer. Each clock pulse is sent to the receiving unit for synchronization purposes. At the same time, another

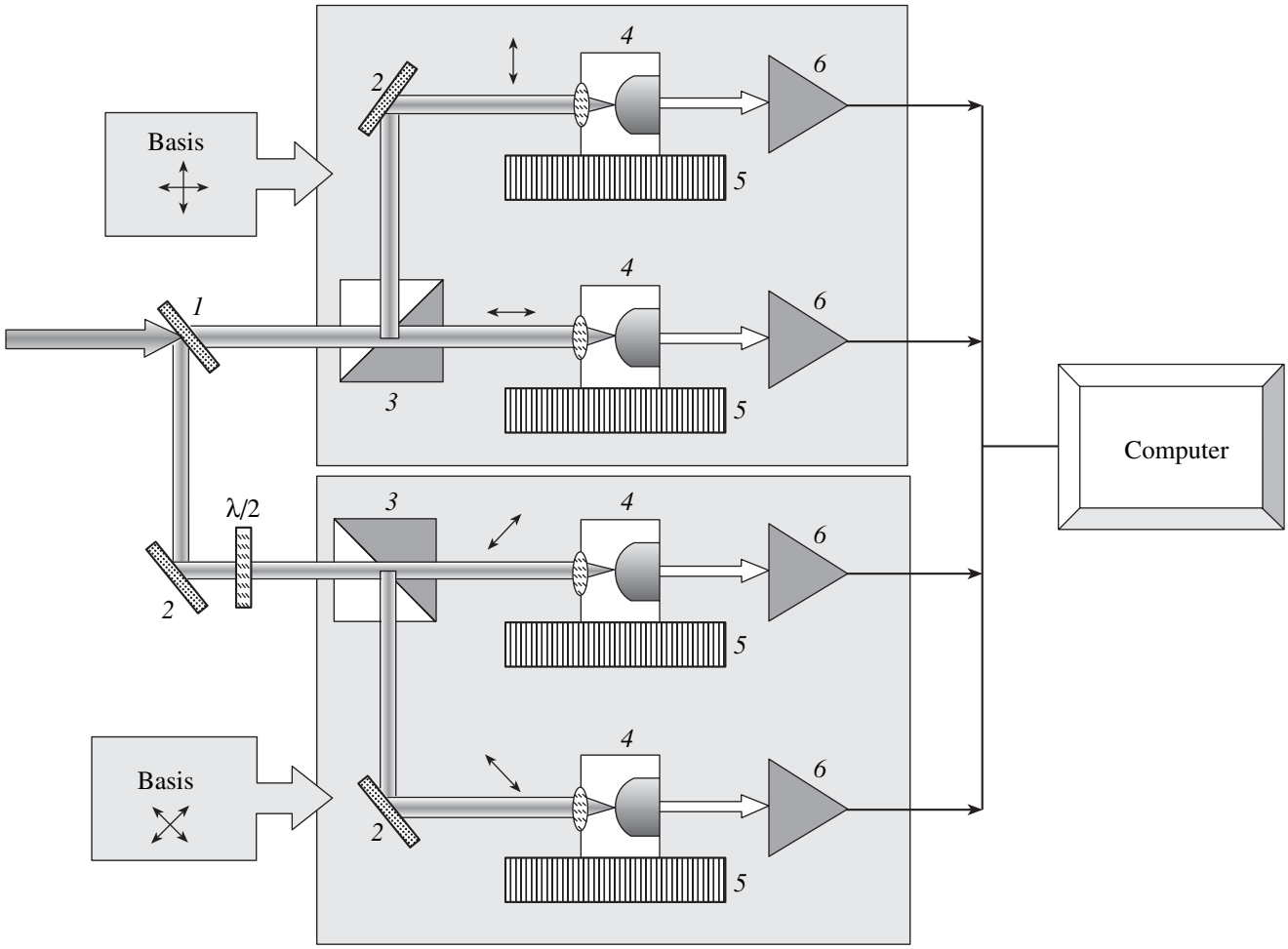

Fig. 2. Receiving unit of the experimental QKD system: (*1*) semitransparent-miror beam splitter, (*2*) mirrors, (*3*) Glan-prism polarization beam splitters, (*4*) avalanche photodiodes with converging lenses, (*5*) Peltier cooling elements, (*6*) active-quenching amplifiers, and (λ/2) half-wave plate.

pulse makes one of the four lasers, selected with a random-number generator, produce a light pulse 8–10 ns wide. In response to a clock pulse, the receiving unit produces a 20-ns gate pulse to define a period during which photodetector output pulses can be accepted. This method enables us to reject most of the dark-current noise. More specifically, it reduces the noise-pulse rate to about 100 per 10^6 clock pulses as against about 3 kHz at $V - V_{br} = 20$ V (Fig. 3).

Thus, photodetector pulses are counted only during laser pulses. For every photodetector pulse accepted, the sequence number of the corresponding clock pulse is stored in the receiver's computer and a signal pulse is sent to the transmitter, which then stores the number and identifies the laser that emitted during the clock period concerned. However, it is not necessary to perform this procedure over the whole session because the mean number of photons per pulse is much less than unity. If the respective polarization measurement bases (rectilinear or diagonal) for the two sides are the same, the measurement results are assigned the next sequence number and added to the key being created; otherwise, they are rejected. A secret key of given length is thus produced according to the BB84 protocol.

3. QKD EXPERIMENTAL RESULTS

At the first stage, we ascertained main performance parameters of the experimental system and conducted preliminary experiments with QKD. The most important parameter is the ultimate rate of quantum-key creation. It is determined by the laser pulse rate; the mean photon number per pulse, $\bar{n}$; and the maximum speed of response of the photodetectors.

Typical QKD characteristics are as follows. At $\bar{n} \approx 0.1$, a quantum key 21 303 bit long was generated during 10^6 clock periods, with 209 bits (0.98%) identified as wrong (the corresponding bits at Alice and Bob differed in value). At $\bar{n} \approx 0.2$, QKD under similar conditions yielded a 38 578-bit key with 371 bits (0.96%) identified as wrong. The clock rate being 100 kHz, key

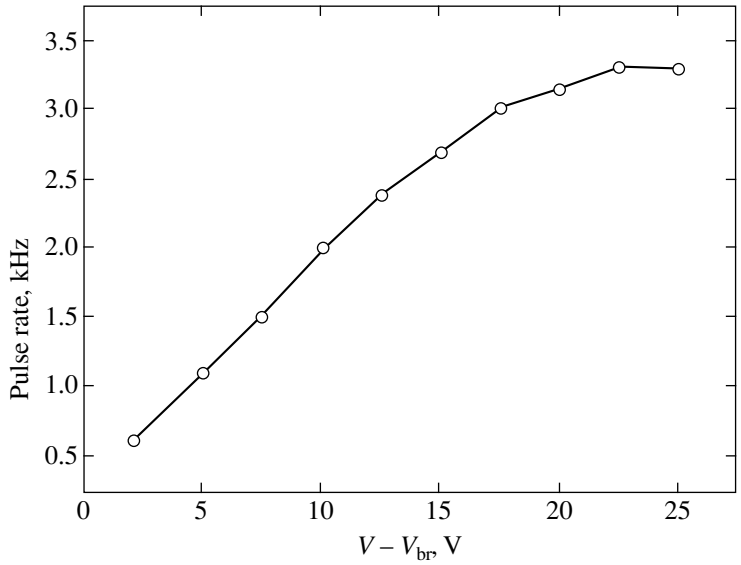

Fig. 3. Noise-pulse rate vs. excess bias voltage above the breakdown level for the C30902S photodiode operated at –20°C.

generation occurred at rates of 2.1 and 3.8 kbit/s, respectively. The low error rates compared with experiments in the atmosphere [21] should be due to the channel being free from external interference and attenuation.

The key-generation rate was limited by the rate of exchange through the ISA interface between the transmitting or receiving unit and its computer. This type of interface permitted a maximum clock rate of about 100 kHz. We plan to change to the PCI interface to raise the clock rate to 10 MHz and to accelerate key generation by two orders of magnitude.

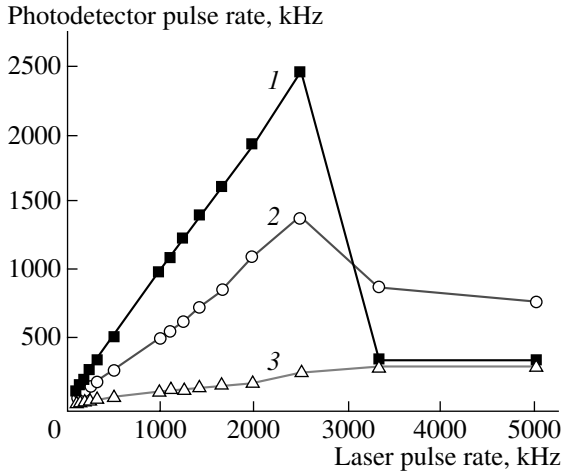

Fig. 4. Photodetector output pulse rate measured against laser pulse rate for different laser intensities, with the maximum count rate set to 2.5 MHz. Graph *1* refers to a laser intensity so high that the photodetector operation probability is close to 100%. Graph *2* is obtained at a moderate intensity when the operation probability is 50%. Graph *3* corresponds to a low intensity at which the operation probability is 10%, the mean photon number per pulse being 0.1.

The second stage was a test to determine whether the system was able to detect unauthorized photon interception in the quantum channel. The test procedure was as follows. Alice and Bob make a comparison of a randomly chosen portion of a key received via the insecure channel. If there has been no interception, the keys generated by Alice and Bob agree within an accuracy limited by the photodetector noise in Bob's station (false detections). Eve is assumed to intercept photons, measure their polarization, and send photons of the same polarization to Bob so as to conceal the attack. Since she does not know the polarization basis chosen by Alice, her measurements should have a mean error of 25%, resulting in mismatch between the keys formed by Alice and Bob. The test confirmed this value of mean measurement error by Eve, providing conclusive evidence that unauthorized interception can be detected.

4. CONCLUSIONS

Quantum cryptography is the most developed area of quantum information science from a practical point of view. Its techniques and algorithms enable QKD to distances of tens of kilometers with absolute security. Free-space QKD can be implemented by means of single photons with coded states of polarization according to the BB84 protocol. Our preliminary experiments with this approach, using a specially designed communication system, have demonstrated the possibility of achieving fast key generation and detecting unauthorized photon interception in the quantum channel. Our future experimental studies will deal with long-distance QKD in free space or optical fiber.

ACKNOWLEDGMENTS

We are deeply grateful to K.A. Valiev for fruitful discussions and his unstinting support. This study was funded by the Russian Foundation for Basic Research under grant no. 04-07-90432 and by Presidium of the Russian Academy of Sciences within Project No. 21.

REFERENCES

1. Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., Quantum Cryptography, *Rev. Mod. Phys.*, 2002, vol. 74, pp. 145–175.
2. Shor, P.W., *Proc. 35th Symp. on Foundations of Computer Science*, Goldwasser, S., Ed., Los Alamitos, Calif.: IEEE Computer Society, 1994, pp. 124–134.
3. Wootters, W.K. and Zurek, W.H., A Single Quantum Cannot Be Cloned, *Nature*, 1982, vol. 299, pp. 802–803.
4. Bennett, C.H. and Brassard, G., in *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India*, New York: IEEE, 1984, pp. 175–179.
5. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J., Experimental Quantum Cryptography, *J. Cryptology*, 1992, vol. 5, pp. 3–28.
6. Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P.M., Tapster, P.R., and Rarity, J.G., Quantum Cryptography: A Step towards Global Key Distribution, *Nature*, 2002, vol. 419, p. 450.
7. Rarity, J.G., Tapster, P.M., Gorman, P.M., and Knight, P., Ground to Satellite Secure Key Exchange Using Quantum Cryptography, *New J. Phys.,* 2002, vol. 4, pp. 82.1–82.21.
8. Stucki, D., Gisin, N., Guinnard, O., and Ribordy, G., and Zbinden, H., Quantum Key Distribution over 67 km with a Plug&Play System, *New J. Phys.*, 2002, vol. 4, pp. 41.1–41.8.
9. Kosaka, H., Tomita, A., Nambu, Y., Kimura, T., and Nakamura, K., Single-Photon Interference Experiment over 100 km for Quantum Cryptography System Using Balanced Gated-Mode Photon Detector, *Electron. Lett.*, 2003, vol. 39, pp. 1199–1201.
10. Kimura, T., Nambu, Y., Hatanaka, T., Tomita, A., Kosaka, H., and Nakamura, K., Single-Photon Interference over 150-km Transmission Using Silica-Based Integrated-Optic Interferometers for Quantum Cryptography, arXiv: quant-ph/0403104.
11. Bennett, C.H., Quantum Cryptography Using any Two Nonorthogonal States, *Phys. Rev. Lett.*, 1992, vol. 68, pp. 3121–3124.
12. Brü, D., Optimal Eavesdropping in Quantum Cryptography with Six States, *Phys. Rev. Lett.*, 1998, vol. 81, pp. 3018–3021.
13. Ekert, A.K., Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.,* 1991, vol. 67, pp. 661–663.
14. Einstein, A., Podolsky, B., and Rosen, N., Can Quantum Mechanical Description of Physical Reality Be Considered Complete, *Phys. Rev.*, 1935, vol. 47, pp. 777–780.
15. Resch, K.J., Lindenthal, M., Blauensteiner, B., Böhm, H.R., Fedrizzi, A., Kurtsiefer, C., Poppe, A., Schmitt-Manderbach, T., Taraba, M., Ursin, R., Walther, P., Weier, H., Weinfurter, H., and Zeilinger, A., Distributing Entanglement and Single Photons through an Intra-city, Free-Space Quantum Channel, *Opt. Express*, 2005, vol. 13, pp. 202–209.
16. Molotkov, S.N., New Approach to Absolute Security in Relativistic Quantum Cryptography, *Zh. Eksp. Teor. Fiz.*, 2003, vol. 124, pp. 1172–1196.
17. Molotkov, S.N., Straightforward Delay Quantum-Cryptographic Scheme Based on an Optical-Fiber Mach–Zehnder Interferometer, *Pis'ma Zh. Eksp. Teor. Fiz.*, 2003, vol. 78, pp. 194–200.
18. Yelin, S.F. and Wang, B.C., Time-Frequency Bases for BB84 Protocol, arXiv: quant-ph/0309105.
19. Inoue, K., Waks, E., and Yamamoto, Y., Differential Phase Shift Quantum Key Distribution, *Phys. Rev. Lett.*, 2002, vol. 89, p. 037902.
20. Inoue, K., Waks, E., and Yamamoto, Y., Differential-Phase-Shift Quantum Key Distribution Using Coherent Light, *Phys. Rev. A*, 2003, vol. 68, p. 022317.
21. Hughes, R.J., Nordholt, J.E., Derkacs, D., and Peterson, C.G., Practical Free-Space Quantum Key Distribution over 10 km in Daylight and at Night, *New J. Phys.*, 2002, vol. 4, pp. 43.1–43.14.
22. Ghioni, M., Cova, S., Zappa, F., and Samori, C., Compact Active Quenching Circuit for Fast Photon Counting with Avalanche Photodiodes, *Rev. Sci. Instrum.,* 1996, vol. 67, pp. 3440–3448.
23. Cova, S., Ghioni, M., Laciata, A., Samori, C., and Zappa, F., Avalanche Photodiodes and Quenching Circuits for Single-Photon Detection, *Appl. Opt.*, 1996, vol. 35, pp. 1956–1976.