ISSN 1062-8738, Bulletin of the Russian Academy of Sciences. Physics, 2014, Vol. 78, No. 3, pp. 171–175. © Allerton Press, Inc., 2014.
Original Russian Text © A.V. Glejm, A.A. Anisimov, L.N. Asnis, Yu.B. Vakhtomin, A.V. Divochiy, V.I. Egorov, V.V. Kovalyuk, A.A. Korneev, S.M. Kynev, Yu.V. Nazarov, R.V. Ozhegov, A.V. Rupasov, K.V. Smirnov, M.A. Smirnov, G.N. Goltsman, S.A. Kozlov, 2014, published in Izvestiya Rossiiskoi Akademii Nauk. Seriya Fizicheskaya, 2014, Vol. 78, No. 3, pp. 266–270.

Quantum Key Distribution in an Optical Fiber at Distances of up to 200 km and a Bit Rate of 180 bit/s

A. V. Glejm[a], A. A. Anisimov[b], L. N. Asnis[a], Yu. B. Vakhtomin[c], A. V. Divochiy[c], V. I. Egorov[a], V. V. Kovalyuk[c], A. A. Korneev[d], S. M. Kynev[a], Yu. V. Nazarov[a], R. V. Ozhegov[c], A. V. Rupasov[a], K. V. Smirnov[c], M. A. Smirnov[a], G. N. Goltsman[d], and S. A. Kozlov[a]

[a] *National University of Information Technologies, Mechanics, and Optics Research, St. Petersburg, 197101 Russia*
[b] *National Scientific Research Institute of Radio Engineering and Electronics, Moscow, 119454 Russia*
[c] *ZAO Superconducting Nanotechnology, Moscow, 119021 Russia*
[d] *Moscow State Pedagogical University, Moscow, 119882 Russia*
e-mail: aglejm@yandex.ru; egorovvl@gmail.com

Abstract—An experimental demonstration of a subcarrier-wave quantum cryptography system with superconducting single-photon detectors (SSPDs) that distributes a secure key in a single-mode fiber at distance of 25 km with a bit rate of 800 kbit/s, a distance of 100 km with a bit rate of 19 kbit/s, and a distance of 200 km with a bit rate of 0.18 kbit/s is described.

DOI: 10.3103/S1062873814030095

INTRODUCTION

The problem of protecting confidential information transferred by public telecommunication channels nowadays is of great interest, due to new possibilities for decrypting information by means of classical high-speed computers and quantum computers, the latter of which are under intensive development. In 2010, for example, information encoded using a 768-bit RSA cryptographic key [1], the length of which was considered very secure, was decrypted using a classical computer. On the other hand, the 512 qubit quantum computer used in [2] allows us to predict that 1000 qubit quantum computers will be produced in the near future and make classical cryptographic protection obsolete in principle [3, 4]. One way to solve the problem of secure information transmission is to use quantum cryptography based on single photon technology [5, 6]. According to the fundamental laws of quantum physics, it is impossible to measure the physical values of a quantum system in an improper state without destroying it, so that a legitimate user of such systems can be sure to detect eavesdropping in a protected channel [7].

A practical problem in designing quantum cryptographic systems is to secure their connections to telecommunication networks. Subcarrier-wave quantum cryptography systems are specially designed to be compatible with fiber optic communication lines. High key distribution rates and low error rates are advantages of such systems, in which quantum signals are not generated directly by a source but are shifted to a side frequency as a result of phase-frequency modulation. Compatibility with optical networks is achieved through separation and unidirectionality of the quantum and classical signals. The theoretical foundations of such systems were presented in [8–12].

An experimental demonstration of a subcarrier-wave quantum cryptography system that distributes a secure key in a single-mode fiber at different distances is described in this work. The record key generation rate is achieved by using superconductor single-photon detectors (SSPDs) [13]. They are characterized by higher time resolution and considerably lower dark counts than in avalanche photodiodes at a wavelength of 1550 nm.

A SUBCARRIER-WAVE QUANTUM CRYPTOGRAPHY SYSTEM FOR SECURE KEY DISTRIBUTION

Figure 1 shows a block diagram of our system. A semiconductor laser generates a signal with a wavelength of 1550.12 nm. This radiation is modulated by phase modulator FM1, which is controlled by a signal arriving from an electronic control unit. As a result of phase modulation, two side frequencies separated from the carrier optical frequency by rate of the modulating radiofrequency signal of 4.4 GHz appear in radiation spectrum. Signal power at the side frequencies is controlled by varying the amplitude of the modulating signal. The modulated signal is then attenuated by attenuator AT. At the attenuator's output, the signal power at the side-frequencies corresponds to the mean photon number in a pulse 0.26. Each bit of the transmitted signal is encoded by introducing phase shift Φ_A into the modulating signal. The phase shift is controlled by the electronic control unit and is chosen arbitrarily from two possible values, 0 and π, for each bit.

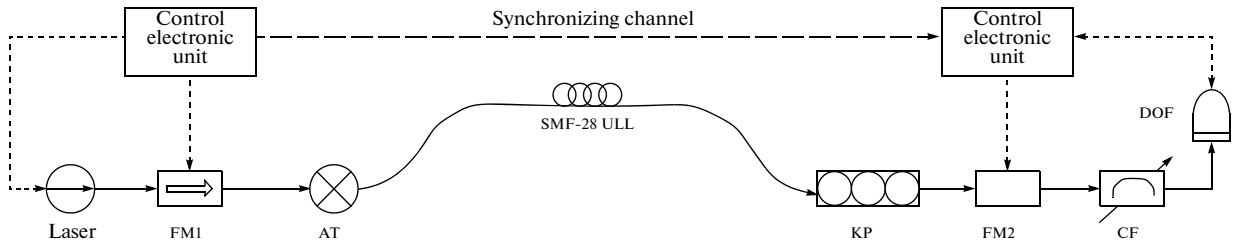

Fig. 1. Block diagram of our subcarrier-wave quantum cryptography system. FM1 and FM2 are phase modulators; AT is the attenuator, KP is the polarization controller; CF is the spectral filter; DOF is the semiconductor single-photons detector.

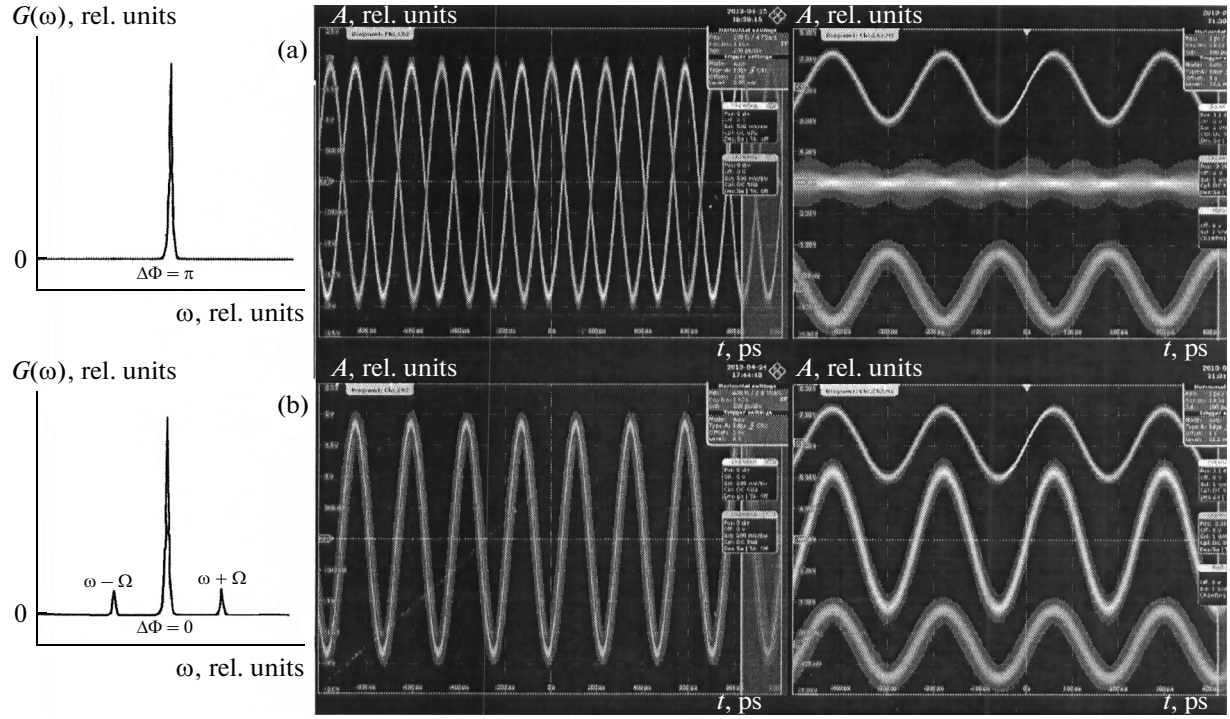

Fig. 2. Spectrum $G(\omega)$ and signal oscillogram under (a) destructive and (b) constructive interference.

The electronic control units in the transmitting and receiving modules are synchronized using a special waveform: a sine function with a frequency of 20 MHz, a gate pulse of 10 ns, and a frequency of 10 MHz. The first (start) gate pulse initiates key generation, and the subsequent gate pulses synchronize the recording of quantum counts in the buffer memories of the transmitting and receiving modules. A sinusoidal signal synchronizes the signal modulation generators in the transmitting and receiving modules. The synchronizing signal is transmitted by a coaxial cable.

The cryptographic key is generated according to the B92 protocol [13].

In the receiving unit, the quantum signal generated by the laser arrives at the optical-fiber polarization controller, phase modulator FM2, and spectral filter SF, connected in series. The spectral filter separates the side-frequency signal, which is detected by superconductor single photon detector DOF. At this stage, the signal is modulated once more. Phase modulator FM2 is controlled by the electronic control unit, and the bit sequence is encoded as in the transmitting unit. The modulation frequency is 100 MHz. Phase shift Φ_B is introduced into the modulating signal, and each bit shift (0 or π) is chosen arbitrarily from four possible values. The resulting power of the subcarrier wave depends on Φ_A and Φ_B. If $\Phi_A = \Phi_B$, constructive interference (Fig. 2a) is observed in the side-frequency optical signal, and the optical signal's power differs from zero. If $\Phi_A - \Phi_B = \pi$, destructive interference (Fig. 2b) is seen, and the registered power of the subcarrier wave corresponds to the dark noise of the single-photon detector.

The exchange of information needed for processing the measurement results is done in a public chan-

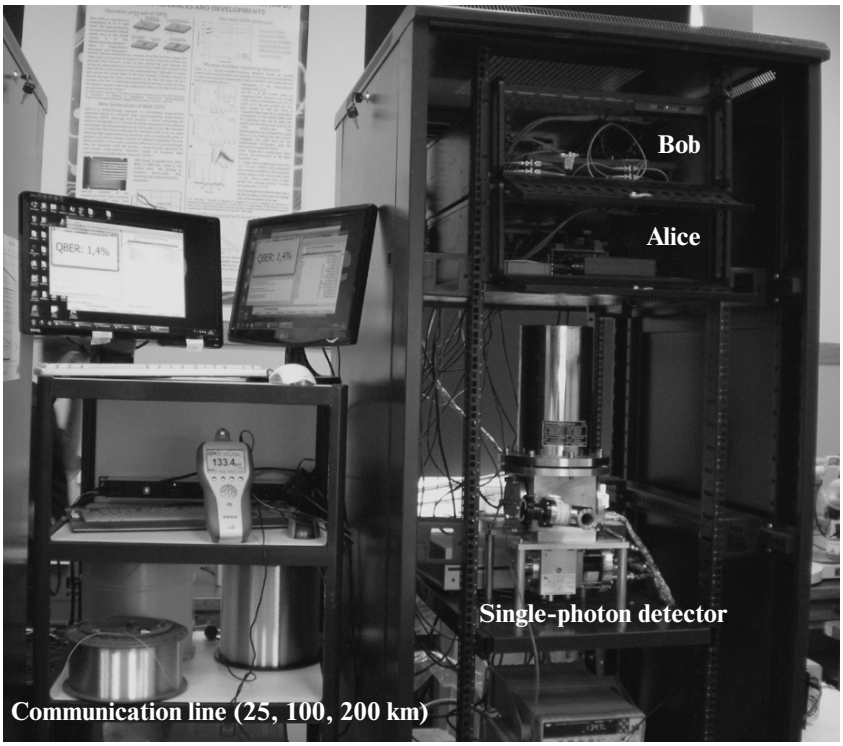

Fig. 3. Experimental setup of our subcarrier-wave quantum cryptography system. The figure shows the transmitting unit (Alice), the receiving unit (Bob), and the superconductor single-photon detector.

nel. The quantum signal is processed in the control electronic unit; as a result, the raw signal is generated simultaneously in the transmitting and receiving units. The error coefficient is calculated for the raw key, and legitimate users can conclude whether or not a third party is eavesdropping. If there is no eavesdropping, the errors are corrected, and a secret cryptographic key is generated in the transmitting and receiving units.

CRYPTOGRAPHIC KEY DISTRIBUTION IN AN OPTICAL FIBER

The cryptographic key in our system was generated under laboratory conditions (Fig. 3). The following parameters of the system were measured: generaton rate and the quantum bit error rate (QBER) at different distances: 25, 100 and 200 km. As a test line, we used a Corning SMF-28 ULL optical fiber without a buffer shell and with a certified loss of 0.17 dB/km.

The mean photon number in a pulse was the same in all experiments: 0.26. This value is determined by measuring the optical power at the input of the transmitting unit, according to the formula

$$n = \frac{P\lambda}{hckf},$$

where P is the optical power of radiation at the input of transmitting unit, $\lambda = 1550.12$ nm is the radiation wavelength at the central frequency, h is Planck's constant, c is the speed of light, $k = 40$ is the ratio between optical power at the carrier frequency and the side frequency (signal), and $f = 100$ MHz is the clock frequency of modulation. The contrast in the interference picture, i.e., the ratio between optical power under constructive interference (Fig. 2b) and optical power under destructive interference (Fig. 2a), is $K = 90$.

An Agilent 53131A counter was used to record the rate of key generation. The number of detectors counts per second was measured. The number of counts corresponded to the raw cryptographic key bitrate. In this work, we used a superconductor single-photon detector (SSPD) cooled to ~2.7 K by liquid helium in a closed-cycle unit. For optical radiation at a wavelength of 1550 nm, the quantum efficiency of the single photon detector was 16% with the rate of dark counts was not higher than 10 counts per second.

EFFICIENCY OF QUANTUM KEY DISTRIBUTION

Several calculated and experimental parameters were used to assess the efficiency of our telecommunications system. The main parameter was the Quantum Bit Error Rate of the system, QBER [15].

Experimental results for cryptographic key distribution over a subcarrier wave

Parameter	Measured value at a distance of		
	25 km	100 km	200 km
Key generation rate, kbit/s	800	19	0.18
QBER, %	0.4	0.45	1.5
Mean photon number per pulse	0.26		

QBER is defined as the ratio between error bits and the total number of received bits,

$$\mathrm{QBER} = \frac{N_{\mathrm{wrong}}}{N_{\mathrm{right}} + N_{\mathrm{wrong}}} = \frac{R_{\mathrm{err}}}{R_{\mathrm{err}} + R_{\mathrm{sift}}} \approx \frac{R_{\mathrm{err}}}{R_{\mathrm{sift}}}, \quad (1)$$

where R_{sift} (sifted key length) corresponds to counts when Alice and Bob (sender and receiver) bases coincide, and is equal to half of the raw key, R_{raw}:

$$R_{\mathrm{sift}} = \frac{1}{2} R_{\mathrm{raw}} = \frac{1}{2} q f_{\mathrm{rep}} \mu t_{\mathrm{link}} \eta, \quad (2)$$

where f_{rep} is the pulse repetition frequency; μ is the mean number of photons per pulse; t_{link} is the transfer coefficient, i.e., the probability of a photon reaching one of Bob's detectors; and η is the probability of a photon being detected, i.e., the quantum efficiency of detector. Factor $q \le 1$ (usually equal to 1 or 0.5 in different reports) is introduced into the system with phase encoding in order to account for noninterfering photons.

Let us examine different components of R_{err}. The first component characterizes photon reaching a wrong detector due to imperfect interference or depolarization, and we designate it as R_{opt}. Coefficient R_{opt} is determined by the product of R_{sift} and p_{opt}, which is the probability of photon striking a wrong detector,

$$R_{\mathrm{opt}} = R_{\mathrm{sift}} p_{\mathrm{opt}} = \frac{1}{2} q f_{\mathrm{rep}} \mu t_{\mathrm{link}} \eta p_{\mathrm{opt}}. \quad (3)$$

We can accept this component as an indicator of optical stability for our quantum cryptography system.

The second component R_{det} is determined as

$$R_{\mathrm{det}} = \frac{1}{2}\frac{1}{2} f_{\mathrm{rep}} p_{\mathrm{dark}} n, \quad (4)$$

where p_{dark} is the probability of dark photon recording in the time window of detector triggering, and n is the number of detectors in the system. By integrating both contributions, we can write QBER as

$$\mathrm{QBER} = \frac{R_{\mathrm{opt}} + R_{\mathrm{det}}}{R_{\mathrm{sift}}} = p_{\mathrm{opt}} + \frac{p_{\mathrm{dark}} n}{t_{\mathrm{link}} \eta 2 q \mu} = \mathrm{QBER}_{\mathrm{opt}} + \mathrm{QBER}_{\mathrm{det}}. \quad (5)$$

For systems with phase encoding,

$$\mathrm{QBER}_{\mathrm{opt}} = \frac{1 - V}{2}, \quad (6)$$

where V is the visibility of the interference picture.

The relationship between visibility and communication distance (L) can be written as

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} - I_{\min}} = \frac{\mu \times 10^{-\alpha L/10} \eta_{\mathrm{Bob}}}{\mu \times 10^{-\alpha L/10} \eta_{\mathrm{Bob}} + 2 p_{\mathrm{dark}}}, \quad (7)$$

where $10^{-\alpha L/10}$ describes signal attenuation in an optical fiber with length L; α is the attenuation coefficient of a single-mode fiber; and η_{Bob} is a coefficient that includes both the efficiency of photon detection and the photon losses due to Bob.

The second component,

$$\mathrm{QBER}_{\mathrm{det}} = \frac{n}{2 q \mu t_{\mathrm{link}} \eta} \frac{p_{\mathrm{dark}}}{} \quad (8)$$

increases with distance, since the rate of dark counting for photons is constant, while the bit rate and t_{link} diminish.

QBER can thus be written as

$$\mathrm{QBER} = \frac{p_{\mathrm{dark}}}{\mu 10^{-\alpha L/10} \eta_{\mathrm{Bob}} + 2 p_{\mathrm{dark}}} + \frac{n}{2 q \mu t_{\mathrm{link}} \eta} \frac{p_{\mathrm{dark}}}{}. \quad (9)$$

The experimental results are presented in the table. It can be seen that the quantum error coefficient is quite low for different lengths of communication lines (the limiting permissible value is 10%), allowing us to state that information is adequately protected in our subcarrier-wave quantum cryptography system.

CONCLUSIONS

An experimental setup for secure quantum key distribution using a subcarrier-wave quantum device was described. Signal transmission at side frequencies with powers corresponding to the mean number of photons in a pulse equal to 0.26 in a single-mode fiber at distances of 25, 100, and 200 km at bit rates of 800, 19, 0.18 kbit/s was demonstrated. To the best of our knowledge, the bitrates demonstrated at these distances are record for this type of system designed for telecommunication lines.

ACKNOWLEDGMENTS

This work was supported by the federal target program Investigations and Research in Topical Fields of the Russian Scientific Complex, 2007–2012 (state contract no. 16.513.11.3017).

REFERENCES

1. Aoki, K., Franke, J., Lenstra, A.K., et al., *Proc. 30th Annu. Conf. on Advances in Cryptology*, Santa Barbara, 2010, p. 333.
2. The D-Wave Two™ System. http://www.dwavesys.com/en/products-services.html. Accessed 15.08.2013.

3. Politi, A., Matthews, J.C.F., and O'Brien, J.L., *Science*, 2009, vol. 325, no. 5945, p. 1221.
4. Lu, C., Browne, D.E., Yandg, T., and Pan, J.-W., *Phys. Rev. Lett.,* 2007, vol. 99, p. 250504.
5. Bennett, C. and Brassard, G., *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, 1984, p. 175.
6. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., et al., *Rev. Mod. Phys.*, 2009, vol. 81, p. 1301.
7. Wootters, W.K. and Zurek, W.H., *Nature*, 1982, vol. 299, p. 802.
8. Mazurenko, Yu.T., Merolla, J.-M., and Goedgebuer, F.J., *Opt. Spektroskop.*, 1999, vol. 86, no. 2, p. 181.
9. Guerreau, O.L., Merolla, J.-M., Soujaeff, A., et al., *IEEE J. Select. Topics Quant. Electron.*, 2003, vol. 9, no. 6, p. 1533.
10. Cussey, J., Bloch, M., Merolla, J.-M., and McLaughlin, S.W., *Opt. Networks Technol. IFIP Int. Federat. Inf. Processing*, 2005, vol. 164, p. 390.
11. Bloch, M., McLaughlin, S.W., and Merolla, J.-M., *Opt. Lett.,* 2007, vol. 32, no. 3, p. 301.
12. Rupasov, A.V., Gleim, A.V., Egorov, V.I., and Mazurenko, Yu.T., *Nauch.-Tekhn. Vestn. Sankt-Peterburg. Gos. Univ. Inf. Tekhnol. Mekhan. Opt.*, 2011, no. 02(72), p. 95.
13. Gol'tsman, G.N., Okunev, O., Chulkova, G., et al., *Appl. Phys. Lett.,* 2001, vol. 79, no. 6, p. 705.
14. Bennett, C.H., *Phys. Rev. Lett.*, 1992, vol. 68, p. 3121
15. Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., *Rev. Mod. Phys.,* 2002, vol. 74, p. 145.

Translated by Yu. Zikeeva