Investigation the bit rate of quantum key using Si single photon detectors

A V Kolyako\textsuperscript{1,2} I G Neizvestny\textsuperscript{1,2}, V L Kurochkin\textsuperscript{1}

1 Institute of Semiconductor Physics, Siberian Division, Russian Academy of Sciences, Novosibirsk, 630090 Russia
2 Novosibirsk State Technical University, Novosibirsk, 630090 Russia

E-mail: kurochkin@isp.nsc.ru

Abstract. This work reports on the results of experimental investigations bit rate of quantum key distribution on a setup designed for quantum cryptography with single photons. Silicon avalanche photodiodes (C30902S) serve as single-photon detectors. The quantum key is transmitted with pulsed semiconductor lasers by coding polarization states of photons in two alternative nonorthogonal bases over free space.

1. Introduction

From the practical standpoint, quantum cryptography is today the most mature area of quantum informatics. Quantum cryptography allows for absolutely secure data transfer between legitimate users of communication lines. The security of data transfer, combined with the complete impossibility of unauthorized access, relies on fundamental laws of nature, unlike those cryptography approaches using mathematical methods, where the information basically may be decoded. In accordance with the mathematically proven Shannon statement [1], a message being transferred cannot be decoded if it is encoded by a random one-shot key whose length equals that of the message, provided that the key is known by legitimate users alone. However, the problem in this situation is how to transport the key to remote users. Generally speaking, classical communication methods cannot provide secure transfer of the key over accessible data channels, since there are techniques of inconspicuous listening with subsequent decoding.

The ideas of quantum physics and quantum informatics as applied to long-range data communication may be used to attack the problem of transfer of an absolutely random key through accessible data channels with security assurance. The absolute security provided by quantum cryptography follows from the forbidding of quantum physics that are imposed on a metering device: (i) it is impossible to extract information about nonorthogonal states without disturbance [2] and (ii) it is impossible to clone an unknown quantum state (the no-cloning theorem) [3]. From these forbidding, it follows that, if single quantum objects are employed as data carriers, any intervention into the data transfer process
undertaken by an unauthorized person will inevitably cause irreversible changes in the quantum states of the objects, from which the fact of intervention can be established.

Bennet and Brassard in 1984 [4] were the first to justify the principles of quantum cryptography and to devise a communications protocol. The first experimental demonstration of their concept [5] attracted much interest worldwide and gave an impetus to extensive research in this field. In [5], a key dissemination protocol was suggested, which was represented as a secured sequence of zeros and unities enciphered by single photons polarized in two mutually nonorthogonal bases. Later, this protocol was named BB84. In the first experimental setup [5], the distance between the transmitter and receiver (the length of the quantum channel) was 0.3 m. However, later on, rapid progress in the increase in the communication range was observed. At present, the record belongs to the group of the authors of [6], where the results on key distribution over a distance of 144 km are presented.

The important part of the quantum cryptography set up is single photon detector [7]. Single photon detection has large range of applications. It had become essential in broad range of research applications such as atmospheric monitoring, time resolved spectroscopy, quantum communications and investigation of quantum systems like single molecule. It has become an important instrument not only in physics but also in biology and chemistry. Quantum cryptography is the first in the history method which allows to guarantee the data transmission secrecy with the laws of physics. But for the good commercial application it should suit a number of conditions such as distance of communication, bit rate and stability. All these main parameters depend on the single photon detector operation. Specifically, it must offer a high quantum efficiency of measurement, a low noise, and a sufficiently high count rate. For the atmosphere transmission the silicon based avalanche photodiodes are used. This work reports on the results of experimental investigations bit rate of quantum key distribution on a setup designed for quantum cryptography. Silicon avalanche photodiodes (C30902S) serve as single-photon detectors.

2. Experimental setup

To research on the quantum key distribution over free space was create experimental set up [8,9]. The transmitting unit consists of four semiconductor lasers. Each laser generates light pulses with one of the four polarizations $0^\circ$, $45^\circ$, $90^\circ$ and $-45^\circ$. The laser beams are combined by a system of mirrors into one beam, which is attenuated by an absorbing filter at the exit and is directed through a 70-cm-long air gap toward the receiving unit. The semiconductor lasers with source supplies (modulated in current) operate in a pulsed mode with a pulse length of 8-10 ns. Each laser generates a coherent light pulse when a control pulse from a computer is fed into its power supply. The attenuated laser pulses arrive at the entrance of the receiving unit and are divided by a beam-splitting 50% mirror into two beams. The analysis of photons polarization was with help two Glan prism and four single-photon detectors.

The scheme of the receiving unit permits us to adjust the transmitting unit so that, after the exit attenuator, each laser pulse predominantly involves no more than one photon and the fraction of pulses containing two and more photons is insignificant. Under these conditions, the distribution of photons over the pulses obeys the Poisson statistics. In quantum cryptography, a signal is considered to be a single-photon signal if the mean number $n$ of photons per pulse falls in the range 0.1 - 0.4. In particular, at $n = 0.1$, the fraction of pulses containing two (three) photons is equal to 5% (0.16%) of the number of single-photon pulses. Actually, in this case, nine out of ten pulses contain no photons. A photon (with any polarization) sent by Alice can arrive at three photoreceivers, namely, at one photoreceiver in its own basis (the polarizing splitting prism does not transmit this photon to the second photoreceiver) and at two photoreceivers in the foreign basis with equal probability. In the case
when signals from all four photoreceivers are detected simultaneously and, in addition, the number of simultaneous operations of two and more photoreceivers is counted, the fraction of multiphoton pulses in the transmission can be calculated in terms of the Poisson statistics. The required mean number of photons in light pulses of the transmitting unit can be achieved by the sequential tuning of the laser power for each laser.

In our setup, the specially chosen silicon avalanche photodiodes C30902S (EG&G), which are the most sensitive photodiodes in the range of 0.8 μm, served as single-photon detectors. With the aim of counting single photons, the avalanche photodiodes were connected so that they operated in the Geiger mode, in which one photon can induce an avalanche of charge carriers. The photodiodes were connected in a passive avalanche quenching circuit. The ballast resistor (200 kΩ) limited the current in the avalanche photodiode. The signal was picked off the load resistor (50Ω), amplified by an amplifier 6, and fed into a shaper of standard TTL pulses for the interface with a computer. In order to decrease intrinsic noises, the photodiodes were cooled to –20°C with the use of Peltier semiconductor microcoolers. The quantum key was transmitted with pulsed semiconductor lasers by coding polarization states of photons in two alternative nonorthogonal bases (BB84 protocol).

3. Experimental results

In our experiments, the quantum key was generated as follows (protocol BB84). Alice’s computer sets the laser pulse repetition rate (clock frequency). For each clock period, a sync (strobe) is generated, which is sent to Bob for transmission–reception synchronization. Simultaneously with the strobe, another pulse is applied at random to one of the four lasers, which generates a 10-ns wide light pulse. A random number is created by an intelligent random-number generator, although generally it is preferable to use a noise generator to create a random number [7]. Having received the sync, Bob generates his own 20-ns wide strobe. The pulses from the photodetectors are recorded only during the strobe application. In this case, a major part of the intrinsic noise of the photodetector is eliminated. For example, at –20°C and a voltage excess of 20 V, the rate of noise pulses is about 3×10³ per second. At the same time, this value reduces to 100 per 10⁹ clock periods when time gating of the signals is employed. After amplification, the duration of the noise pulses and the pulses from the APD was found to be 8–10 ns. Pretuning of the delay between the strobe and the APD pulse (when the diode is triggered by a laser pulse from the transmitter) makes it possible to considerably improve the signal-to-noise ratio and reduce the error rate in the final code.

The pulse from the APD is regarded as bearing information only if it coincides in time with the laser pulse. Intrinsic noise pulses not appearing during the strobe did not fall on the counter. The data from the four photodetectors were read out by Bob’s computer under the control of the sync. In our setup, we used the same computer. Without loss in generality, such a design makes the experiment less hardware-intensive. When a pulse from any of the APDs came during the strobe, Bob remembered these data and the number of the sync and generated a signal for Alice by which she remembered the number of the sync and which of the lasers operated in that clock period. Since the mean number of photons in a light pulse was much less than unity, there was no need to remember the transfer process as a whole. Fifty percent mirror at the entrance randomly turns the photon to the vertical–horizontal or diagonal basis for recording. If Alice’s and Bob’s bases coincided, the measurements were assigned a successive serial number and filed to generate the key. Other wise, they were disregarded. According to the BB84 protocol, such a procedure generates a matched random secured key.

The bit rate of quantum key distribution depends on the clock frequency of laser pulse repetition, the number of photons per pulse, and the frequency characteristics of the avalanche photodiodes used. Sifted key generation rate is calculated by the following formula:
Here the $1/2$ factor is from sifting the key in the BB84 protocol, $f_L$ is laser repetition rate, $n$ is mean photon number per laser pulse, $\eta$ is quantum efficiency of SPCM, and $T$ is total transmission of the optical channel from Alice's output to Bob's detectors.

In our experiment, the rate of key generation was limited by the rate of data exchange between the computer and the receiving and transmitting units, which corresponded to a transmission clock frequency of 100 kHz. In the experiment, during the transmission with $\sim 0.1$ photon per pulse $10^6$ laser pulses, a key with a length of 12462 bits was generated; among the bits, only 812 (2.0%) were erroneous (the values of bits for Alice and Bob did not coincide – quantum bit error rate (QBER)). Table 1 shows the experimental data according to quantum key value of the average number of photons per pulse at a fixed quantum efficiency of 30%. Table 2 shows the error rate of the average number of photons per pulse at the quantum efficiency of 30%. During the transmission with $\sim 0.2$, the length of the key was 25336 bits, and QBER 174 bits (0.95%). For the used laser pulse repetition of 100 kHz, this corresponded to a key generation rate of $\sim 1.2$ kbits/s and 2.5 kbits/s.

### Table 1. Dependence of the quantum key distribution vs the average number of photons per pulse at a fixed quantum efficiency of 30%.

| Average number of photons | Amount of quantum key |
|---------------------------|-----------------------|
| 0.1                       | 12462                 |
| 0.2                       | 25336                 |
| 0.4                       | 44884                 |

### Table 2. Dependence of quantum bit error rate vs the average number of photons per pulse at 30% quantum efficiency.

| Average number of photons | QBER (%) |
|---------------------------|----------|
| 0.1                       | 2.0      |
| 0.2                       | 1.3      |
| 0.4                       | 0.9      |

### 4. Conclusion

To research on the quantum key distribution over free space was create experimental set up. The specially chosen silicon avalanche photodiodes C30902S (EG&G), which are the most sensitive photodiodes in the range of 0.8 $\mu$m, served as single-photon detectors. The key is transferred by pulsed semiconductor lasers, which encode the polarization state of the photons in two mutually nonorthogonal bases. The dependence of the bit rate quantum key and bit error rate vs of the average number of photons per pulse was investigated. When radiation propagates through the atmosphere, its polarization undergoes insignificant changes. Therefore, the polarization method of coding is used for organizing quantum channels over a free space, and, in the long view, the possibility of connection...
with orbital satellites is considered. The transmittance spectrum of the atmosphere has good transparency windows with wavelengths in the region of 0.8 μm. It is considered that the vertical optical density of the atmosphere is equivalent to a distance of about 8 km at normal conditions [7]; therefore, absorption losses of photons during the connection with the satellites are rather small. Further research in this field seems to be aimed at applying long-range atmospheric communication lines and increasing the data transfer rate.

Acknowledgments

This work was supported by RFBR (Grant No. 14-07-00809) and by the Siberian Branch of the Russian Academy of Sciences.

5. References

[1] Shannon C E 1949 Bell Syst. Tech. Jour 28 658.
[2] Bennet C H 1992 Phys. Rev. Lett 68 3121
[3] Wooters W K, Zurek W H 1982 Nature 299 802
[4] Bennet C H Brassard G 1984 Public Key Distribution and Coin Tossing Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, In-dia, December 1984 pp 175-179
[5] Bennet C H, Bessette F, Brassard G et.al. 1992 J.Cryptology 5 3
[6] Ursin R, Tiefenbacher F, Schmitt-Manderbach T et al. Nature Physics, 2007 3, 481
[7] Gisin N, Ribordy G, Title W et al. 2002 Rev. of Mod. Phys. 74 145
[8] Kurochkin V L Ryabtsev I I and I. G. Neizvestny I G 2005 Technical Physics 50 727
[9] Kurochkin V L Zverev A V Kurochkin Yu V Ryabtsev I I and I. G. Neizvestny 2011 Russian Microelectronics 40 245