NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2013, 4 (2), P. 190–195

ANALYSIS OF A SIDEBANDS-BASED QUANTUM CRYPTOGRAPHY SYSTEM WITH DIFFERENT DETECTOR TYPES

V. I. Egorov[1], D. N. Vavulin[1], I. Z. Latypov[2], A. V. Gleim[1], A. V. Rupasov[1]

[1] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, Russia

[2] Zavoisky Physical-Technical Institute, Kazan, Russia

egorovvl@gmail.com, dima-vavulin@mail.ru

PACS 03.67.-a

We performed theoretical analysis of a sidebands-based quantum cryptography system with two types of detectors: an avalanche photodiode and a superconducting photon counter. The influence of detector parameters on eavesdropper "Intercept-resend" attack efficiency was investigated.

Keywords: quantum cryptography, intercept-resend, avalanche photodiodes, superconducting single photon detectors.

1. Introduction

Quantum cryptography is a method of secure communications based on using single-photons in the process of secret key generation [1]. Therefore, information security is granted on a physical level by the fundamentals of quantum physics. The principal advantage of this technology is its ability to allow legitimate users (Alice and Bob) to always detect eavesdropping in the secure channel based on the increase in error level during transmission. In practice, quantum key distribution security is limited by the amount of losses in communication channel and the quantum bit error rate (QBER). It is known that the eavesdropper (Eve) can conceal their activity under errors which inevitably appear during the key distribution process [2]. The QBER value is dependent upon both the optical scheme and device parameters. In particular, detector characteristics make the largest contribution, especially at shorter distances ($<$50 km). In these studies, two detector types: an avalanche photodiode (APD) and a superconducting single-photon detector (SSPD) were analyzed. APD-detectors are used in most quantum cryptography experiments [2]. Their main drawback is a high rate of dark counts, resulting in high QBER. Superconducting detectors [3] have high count rates and fewer dark counts, however, they are more operationally complex, requiring the use of liquid helium to maintain cryogenic temperatures (2–4 K).

Today many types of QKD systems are known [2]. Merolla et al. [4] suggested a method of quantum key distribution using sidebands modulation of light (SQKD). Among its advantages are simplicity of optical phase introduction, matching and maintenance, high bitrate and low error rate, achieved by unidirectionality and frequency separation of quantum and classical signals, as well as in principal, the possibility of implementing wavelength division multiplexing.

In this paper the informational characteristics of an SQKD system with APD and SSPD detectors (raw key generation rate and QBER) were investigated. We also performed theoretical analysis of the system's ability to resist Intercept-resend attacks [2], the efficiency of which was defined by its QBER value.

2. Experimental Setup

Figure 1 shows a schematic diagram of an SQKD system. The laser emitted monochromatic radiation. The spectrum of signal in frequency scale include only one component. In a sender block phase modulator PMA performed sinusoidal modulation on a high frequency from radio range. If the index of modulation is low enough, in addition to the central frequency, two sidebands will appear in the spectrum at PMA output (Fig. 1b). The spectral shift of the sidebands from the central frequency was equal to the modulation frequency. Optical phase shift of sidebands was determined by the phase of the modulating wave. The index of modulation can be chosen low enough so that the radiation on the sidebands can be regarded as a single stream of photons.

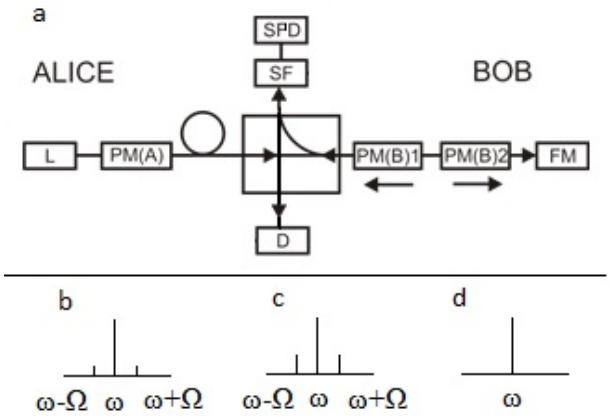

FIG. 1. Principal scheme of a sidebands-based quantum key distribution system (a). L — light source. PMA, PMB — phase modulators, FM — Faradey mirror, SF — spectral filter, D — detector, SPD — single photon detector. At the bottom — spectra of optical signals after modulation at the Alice block and Bob's block with relative phase shift 2π (c) and π (d)

The modulated optical signal, which consisted of central and side frequencies with a given relative phase was transmitted over the communication line to Bob's device, which contain ed similar modulators PMB1 and PMB2. Two modulators were necessary to compensate for polarization distortion in the optical system. At the receiving unit a phase shift was added without reference to the sender. The second modulation resulted in sideband amplitude changes depending on the relative phase shift of Alice and Bob. After passing through modulators the light was reflected off the Faraday mirror and passed to the spectral filter. This filter separated quantum and classical signal components, which were detected by a single photon counter SPD and detector D respectively. The SQKD system also included an optical subsystem of synchronization between the sender and the receiver (not shown on the figure).

3. Operational Parameters of the System with Different Detector Types

One of the main parameters of a quantum key distribution system is the ultimate raw key generation rate F_{raw}, which was, in our case, limited by the maximum detector count rate on the receiver side and is defined as:

$$F_{raw} = \frac{1}{2} f_{bit}\, \mu\, a_{\text{loss}}\, \eta,$$

where 1/2 refers to probability of coincidence between Alice and Bob modulator phase shifts in the B92 protocol [1]; f_{bit} is the phase change frequency (i.e. the frequency of signals sent by

the transmitter); μ — mean number of photons per pulse ($\mu \sim 0.2$), η — quantum efficiency of a single photon detector. Coefficient a_{loss} represents the probability of a photon to achieve the detector and is defined through the value of total optical losses in the channel α:

$$a_{\text{loss}} = 10^{-\alpha/10}.$$

For the investigated SQKD system, the total losses were defined as the sum of losses in optical fiber and other optical elements. The latter included losses on a multiplexer (1.2 dB), circulator (2.21 dB), Bob modulators (10 dB after two passes) and a Faraday mirror (0.6 dB), totalling 14.01 dB. The attenuation rate in single mode fiber (SMF-28) was assumed to be 0.2 dB/km.

Modeling was conducted for the following detector parameters: f_{bit} = 100 MHz, η = 10% (APD, IdQuantique [5]); f_{bit} = 100 MHz, η = 25% (APD, IdQuantique [5]); f_{bit} = 500 MHz, η = 16% (SSPD, Scontel [3]). Fig. 2 illustrates calculated values of raw key generation rate depending on fiber optics line length for the SSQKD system with APD and SSPD detectors.

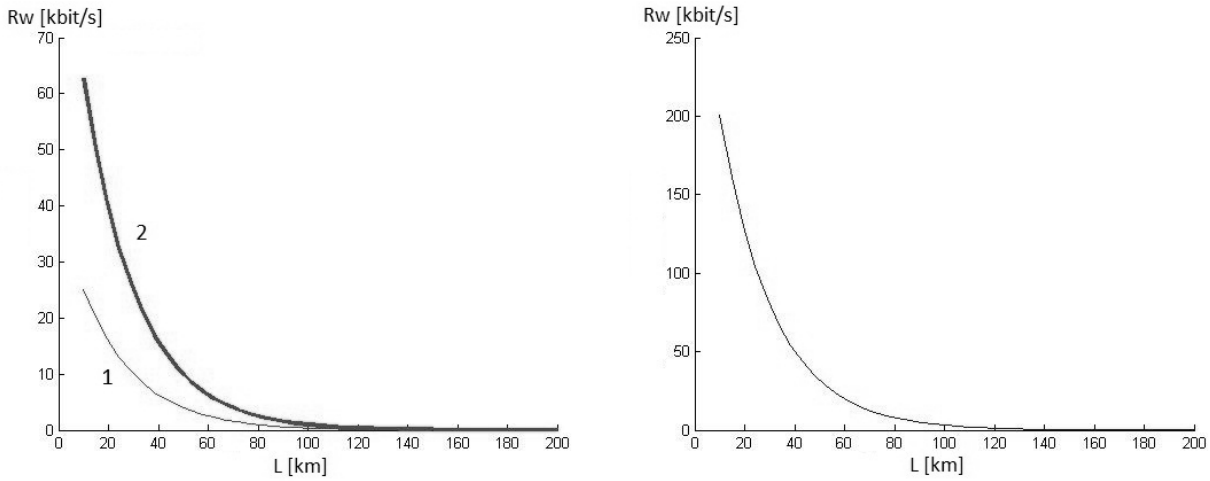

FIG. 2. Raw key generation rate in the SSQKD system with APD (a) and SSPD (b) detectors

Quantum bit error rate (QBER) is another important parameter of any QKD system. It is defined as:

$$QBER = \frac{F_{err}}{F_{raw} + F_{err}},$$

where F_{err} is the frequency of error bits that appear in the process of key distribution. This quantity consisted of two components: optical error frequency F_{opt} and detector dark count rate F_{dark}. For an SSPD detector, the F_{dark} value may be as low as 10 Hz [6], and for an APD — 1 kHz for η = 10% and 5 kHz for η = 25% [5]. Optical error frequency F_{opt} is defined as:

$$F_{opt} = F_{raw} \cdot p_{err},$$

where p_{err} is the optical error probability, that in the current setup, includes Fabry–Perot based filter noise ($1.85 \cdot 10^{-4}$), probability of error induced by Rayleigh reflection, back reflection, circulator directivity ($1.63 \cdot 10^{-3}$), and noise from multiplexer cross-coupling ($1.93 \cdot 10^{-3}$). Multiplexer errors decay in optical fiber. Computational results are given on Fig. 3.

One may notice that QBER suffers a slight decay in a system with an SSPD detector for communication line length 10–40 km. This is due to errors introduced by optical elements

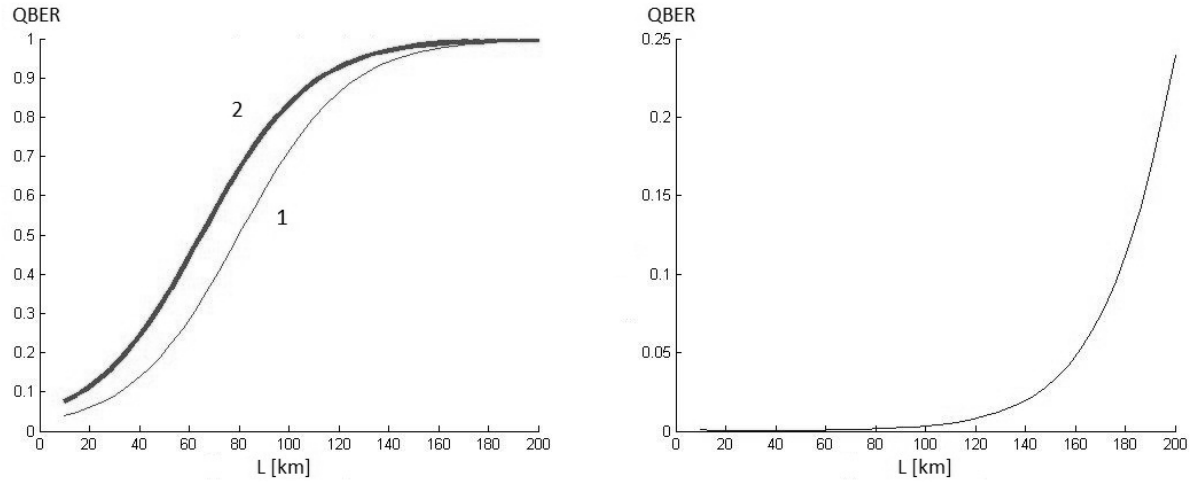

FIG. 3. QBER values in SQKD system with an APD (a) and SSPD (b) detectors

of Alice (they are represented by multiplexer errors in our model). This noise component is quickly attenuated over longer distances.

In order to estimate the efficiencies of different detectors, we introduced a parameter D_{Eff}, defining it as:

$$\mathrm{D_{Eff}} = \frac{\mathrm{QBER_{APD}} \,/\, \mathrm{QBER_{SSPD}}}{F_{raw}\ \mathrm{APD} \,/\, F_{raw}\ \mathrm{SSPD}}.$$

The curves for APD's with different quantum efficiencies are shown on Fig. 4. It can be seen that for optical channel length between 20 to 100 km, SSPD detectors demonstrated the most considerable advantage. In particular, at 60 km the signal-to-noise ratio of an SSPD is more than three orders of magnitude higher than for the studied APDs.

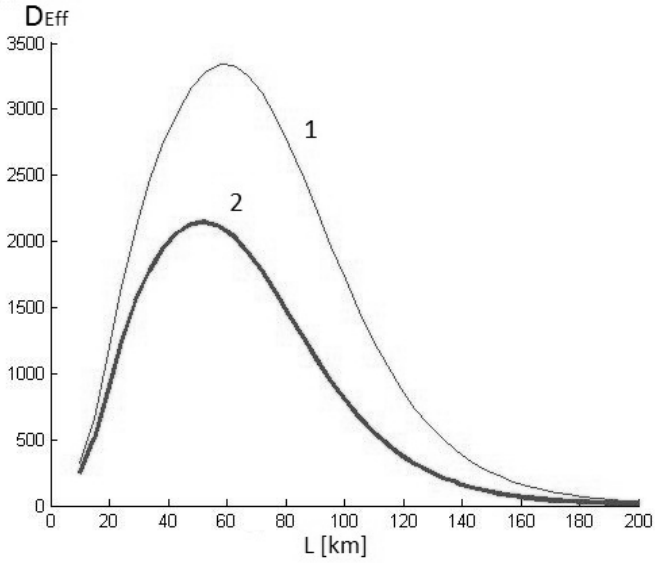

FIG. 4. Relative efficiency of SQKD systems with APD and SSPD detectors

TABLE 1. Probability analysis of Intercept-Resend strategy. Probabilities calculated for two symmetric cases are marked with an asterisk. Cases not shown are parenthesized

Phase used by Alice	0		π		0		π	
Phase used by Eve	0		π		π		0	
Probability of photon detection for Eve	$\mu/4$		$\mu/4$		0		0	
Phase detected by Eve	0		π		—		—	
Phase used by Eve for transmission	0		π		0	(π)	0	(π)
Probability of this event	$\mu/4$		$\mu/4$		$1/4 - \mu/8$*		$1/4 - \mu/8$*	
Phase used by Bob for detection	0	π	0	π	0	π	0	π
Probability of photon detection for Bob	$\mu^2/8$	0	0	$\mu^2/8$	$\mu/8 - \mu^2/16$*	0	$\mu/8 - \mu^2/16$*	0

4. "Intercept-resend" Attack Resistance

Intercept-resend eavesdropping strategy, e.g. when Eve imitates Bob's and Alice's behavior [1] is based upon the principal ability of an intruder to conceal their activity under optical errors, numerically estimated by the QBER value. Implementing this strategy, Eve connects to the quantum channel and measures the results of interference between prepared photons and Alice's pulses. If Eve receives a detector count, she sends a photon with the same phase value as the one used for measurement. Otherwise, if she doesn't receive a count, she sends a pulse with a random phase. Table 1 shows the probability analysis of this strategy. We assume that Eve possesses a detector with η = 100%, no dark counts and a light source equal to Alice with $\mu \sim 0.2$.

An important advantage of this strategy is the fact that Bob's total detection probability (μ/2 for B92 protocol) doesn't change. According to the table, the probability of a disagreement between Alice's and Bob's raw key bits is close to 50% for low μ. It is certain that such a high error rate is unsatisfactory, but Eve still possesses another opportunity. She may sacrifice information about the key, and therefore, linearly reduce the error rate. In order to do this, Eve can perform measurements with a certain rate. Thus, if we assume that random noise fluctuations are 50% of total noise rate, then Eve may stay undetected, adding an amount of errors bounded above by one-half of the QBER value:

$$\left(\frac{\mu}{4} - \frac{\mu^2}{8}\right) \Big/ \frac{\mu}{2} = QBER \cdot n,$$

where n represents the frequency of eavesdropping measurements. The number of bits received by Eve in this case may be estimated as:

$$N_{Eve} = \frac{F_{raw} \cdot t}{n} \cdot \left(\frac{\mu}{4} + \frac{\mu^2}{8}\right) \Big/ \frac{\mu}{2},$$

where t is transmission time. Table 2 shows calculated values for the investigated setup for 40 km fiber distance and $t = 10$ s.

Therefore, at the fiber length of 40 km, Eve is able to perform imperceptible eavesdropping for one of 4600 pulses in an SSPD based system, one of 13 pulses in an APD system with

TABLE 2. "Intercept-Resend" strategy efficiency for systems with different detector types

Detector type	F_{raw}, kbit/s	QBER	n	N_{Eve}, bits	Key fraction, %
SSPD	50.6	$3.9{\cdot}10^{-4}$	4615.4	60.5	0.01
APD, η=10 %	6.3	0.24	7.5	4620	7
APD, η=25 %	15.8	0.14	12.8	6788.6	4

η = 10 % and one of 7 in an APD system with η = 25 %. In ten seconds she will receive 61 (0,01%), 6789 (4%) and 4620 (7%) secret key bits respectively. It may be seen that for efficient detectors QBER grows more slowly than the detection rate, which makes these devices more suitable for QKD, especially at medium distances, which agrees with data from Fig. 4.

5. Conclusion

Thereby, the results of numerical simulations demonstrated the significantly higher efficiency of superconducting detectors relative to APDs for quantum cryptography systems. The values used in the calculations were based on data from the available specifications of commercial single-photon detectors. Both high detection rates and low dark counts of SSPD detectors make them more efficient for quantum cryptography application. The signal-to-noise ratio of an SSPD was found to be more than three orders of magnitude higher than that of the APD for setups with optical fiber several tens of kilometers long. Low dark count values in superconducting devices allowed increasing cryptographic security several times for lines of the same length and additionally facilitated the detection of Intercept-resend attacks. The use of APD made necessary the performance of reconciliation and privacy amplification procedures, [2] even for short optical communication line lengths. The data clearly demonstrated that APD's with higher quantum efficiencies (25% instead of 10%) provided higher security rates. Avalanche photodiodes can be used effectively in one-way cryptographic schemes (in particular, QKD using single-photon interference in sidebands of phase-modulated light for short communication channels (up to 30 km).

Acknowledgments

The study was supported by The Ministry of education and science of Russian Federation, project 14.B37.21.0248.

References

[1] C.H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, **68**, P. 3121–3124 (1992).

[2] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf et al. The security of practical quantum key distribution. *Rev. Mod. Phys.*, **81**, P. 1301–1350 (2009).

[3] G. N. Gol'tsman, O. Okunev, et al. Picosecond superconducting single-photon optical detector. *App. Phys. Lett.*, **79** (6), P. 705–707 (2001).

[4] J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, W.T. Rhodes. Single photon interference in sidebands of phase-modulated light for quantum cryptography. *Phys. Rev. Lett.*, **82**, P. 1656 (1999).

[5] IdQuantique id210 series datasheet. `http://www.idquantique.com`.

[6] A.V. Sergienko. Quantum optics: Beyond single-photon counting. *Nature photonics,* **2**, P. 268–269 (2008).