Practical security for subcarrier wave quantum key distribution against collective beam-splitting attack.

A.V. Kozubov[1], A.A. Gaidash[1], G.P. Miroshnichenko[1], D.B. Horoshko[2,3], A.V. Gleim[1,4]

[1] ITMO University, Department for Photonics and Optical Information Technology, 199034 Kadetskaya Line 3b, Saint Petersburg, Russia

[2] Univ. Lille, CNRS, UMR 8523, Physique des Lasers Atomes et Molécules (PhLAM), F-59000 Lille, France

[3] B. I. Stepanov Institute of Physics, NASB, Nezavisimosti Avenue 68, Minsk 220072, Belarus

[4] Kazan National Research Technical University KAI, 420111, Karl Marx str. 10, Kazan, Russia

Growing interest in quantum key distribution (QKD) in the last decade has led to emergence of a large number of experimental works dedicated to developing reliable QKD setups suitable for everyday operation in existing telecommunication networks. In [1] we suggested a novel subcarrier wave (SCW) QKD design capable of operating in optical links with losses up to 42 dB, which is also particularly promising in terms of robustness against external factors and multiplexing potential. The system uses a modification of BB84 phase protocol. However, the major results of [1] were experimental, while the performed security analysis was supplementary.

In order to ensure secure operation of a QKD system for real-life applications, one needs to consider possible eavesdropping strategies and define optimal parameters for the experimental setup. In this work we perform security analysis for SCW QKD [1,2] against one of the most powerful collective attacks on phase protocols: a collective beam-splitting attack [3].

In order to solve this task, we perform realistic description of different SCW QKD system components. It requires a coordinated solution of several problems using methods of quantum optics. First of all, we describe the process of photonic quantum state preparation and binary information encoding. For correct quantum bit error rate (QBER) estimation we construct a theory for photonic quantum state decoherence process during propagation in optical fibers. We also provide mathematical description of detection process and processing of classical binary bit strings.

It strongly should be mentioned that such security analysis has never been done for SCW QKD systems.The main results of this work are the following. Using data from [4] we obtained equations for input coherent state transformation by an electro-optical modulator, with using more accurate model and taking into account all possible sidebands and geometric sizes of the modulator. We then constructed formulas for sidebands detection probability using Markov's approximation, which take into consideration detection efficiency and a parameter defining dark count rate. We found also the Holevo bound for the accessible information in the Alice-Eve channel [5, 6] and made estimations for both for pure and mixed states. Moreover, the capacity of the SCW QKD channel (modelled as binary symmetric erasure channel) was investigated, taking phase errors into account. Error and uncertain results probabilities were calculated depending on the channel length. Finally, using the equations from [1, 2, 6, 7], we estimated secure key rate for different system parameters.

Using the obtained equations, we studied the dependence of secret key rate in SCW QKD setup depending on the device parameters and channel length. Notably, the results were achieved despite a relatively low phase change frequency of 100 MHz. As can be seen from the figure, detector dark count rate f remains the main limiting factor for the maximum QKD distance. The values used in the calculations (f = 0.01, 10, 10^3 Hz with quantum efficiency (QE) 20%) imply

using modern superconducting nanowire single photon detectors, which are available on the market [8].

These results are important for constructing long-distance QKD links and multiuser quantum networks using SCW QKD instrumentation: an ultra-high bandwidth approach to QKD compatible with existing optical fiber infrastructure.

Acknowledgements

This work was financially supported by Government of Russian Federation, Grant 074-U01 and by the Ministry of Education and Science of Russian Federation (project № 14.578.21.0112, contract № 02.G25.31.0229).

References

[1] A. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. Opt. Express, Vol. 24, No. 3, p.2619-2633, (2016)

[2] Matthieu Bloch and Steven W. McLaughlin, Jean-Marc Merolla, Frédéric Patois. Frequency-coded quantum key distribution. Opt. Lett., Vol. 32, No. 3, p. 301-303, (2007)

[3] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, Momtchil Peev. The security of practical quantum key distribution. Rev. Mod. Phys, V. 81, №3, p. 1301-1350, (2009)

[4] Miroshnichenko G P, Kiselev A D, Trifanov A I, Gleim A V 2016 arXiv:1605.05770v1

[5] Holevo A. S. Bounds for the quantity of information transmitted by a quantum communication channel //Problemy Peredachi Informatsii. – 1973. – T. 9. – №. 3. – C. 3-11.

[6] K. Inoue, E. Waks, and Y. Yamamoto. Differential-phase-shift quantum key distribution using coherent light. Phys. Rev., A 68, 022317, (2003)

[7] B. Korzh, N. Walenta, R. Houlmann, H. Zbinden. A high-speed multiprotocol quantum key distribution transmitter based on a dual-drive modulator. Optics Express, Vol. 21, Issue 17, pp. 19579-19592, (2013)

[8] Shcherbatenko, M., Lobanov, Y., Semenov, A., Kovalyuk, V., Korneev, A., Ozhegov, R., Kazakov A., Voronov B.M., Goltsman, G. N. Potential of a superconducting photon counter for heterodyne detection at the telecommunication wavelength. *Optics Express*, *24*(26), 30474-30484. (2016).