Security conditions for sub-carrier wave quantum key distribution protocol in errorless channel

A Gaidash, A Kozubov, V Chistyakov, G Miroshnichenko, V Egorov, A Gleim
ITMO University, Saint-Petersburg 197101, Russia

Abstract. Article deals with security criterion for sub-carrier wave quantum key distribution (SCW QKD) protocol in errorless channel. SCW QKD is promising type of QKD system in a field of telecommunications due to its compatibility and very efficient using of channel spectral bandwidth. Corresponding expression of security condition was derived for the first time in this work.

1. Introduction
Quantum key distribution (QKD) system allows share secure symmetric key between two users by transmitting single photons encoded in non-orthogonal basis sets [1]. According to the laws of quantum physics, it is impossible for a third party to measure these states without disturbing them and introducing errors, so that legitimate users of such systems cannot share key due to the reduction of its length to zero when error rates reaches critical value during post-processing [2].

One of the practical approaches to the implementation of QKD, with particular potential for optical network implementation, is based on subcarrier wave generation (SCW) [3]. Its main feature lies in a method of single photon generation in which the signal photons are not emitted directly by a source but are generated on subcarrier frequencies, or sidebands, as a result of phase modulation of a classical field on the central frequency, or carrier wave. Advantages of this type of QKD system include a simplification of phase shift matching in the transmitter (Alice) and receiver (Bob) modules with absence of complicated distributed interferometry schemes. Perhaps one of the most valuable features of SCW QKD systems is the exceptionally efficient use of the quantum channel bandwidth (up to 40%, which is one order higher than in other QKD systems) and the ready capability of signal multiplexing of added subcarriers on the same carrier source.

To the best of our knowledge there still no strict mathematical security proof for such a promising protocol. Here we present the first attempt to do so proposing security estimations in errorless channel with losses.

2. Mathematical model
Let us consider firstly the principal scheme of the most danger collective zero-error quantum memory assisted beam-splitting attack as you can see in figure 1. Alice connected to the Bob through optical fiber while illegitimate user (Eve) replaces their channel with ideal one and uses adjustable beam splitter to fake initial loss in the ideal channel. Thus Eve collects the entire “lost” signal. Then she stores all the quantum states in the quantum memory carrying out measurements after reconciliation.

In order to derive expression of the secure key fraction we should consider transmission capacity for Alice-Eve (AE) channel. Therefore, we should consider initial state $u$ prepared by Alice at first
modulator as following, however without central mode since it does not carry any phase-coded information:

$$|u(\varphi_A)\rangle = \prod_{n \neq 0} |\alpha \cdot \exp(-i\varphi_A n) \cdot d^S_{0,n}(\beta)\rangle$$

where $\varphi_A$ is Alice’s phase choice, $\alpha$ is coherent state, $d^S_{n,k}(\beta)$ is d-Wigner matrix, $S$ is number of interacting modes in modulator, $\beta$ is coefficient related to modulation index.

$$|\alpha \cdot \exp(-i\varphi_A n) \cdot d^S_{0,n}(\beta)\rangle$$

(1)

where

$$\varphi_A$$

is Alice’s phase choice,

$$\alpha$$

is coherent state,

$$d^S_{n,k}(\beta)$$

is d-Wigner matrix,

$$S$$

is number of interacting modes in modulator,

$$\beta$$

coefficient related to modulation index.

Figure 1. Principal scheme describes Eve’s strategy of replacing initial channel with ideal one in a way that she collects the entire “lost” signal while Bob receive expected part of signal. Here $\eta$ denotes “losses” modeled by Eve, $\gamma$ denotes “transmissivity”, BS denotes adjustable beam-splitter.

Here we use quantum theory of mode-bounded EOM [4] due to useful properties of d-Wigner matrix in later calculation. Next useful expression was derived for overlapping of states with different phases ($0$ and $\pi$) as following for AE channels:

$$\psi = \langle u(0)|u(\pi)\rangle = \langle u(\pi)|u(0)\rangle = \exp\left(-|\alpha|^2 \cdot \eta \cdot \left[1 - d^S_{0,0}(2\beta)\right]\right).$$

(2)

We should note that whether there is two or four state protocol Eve only needs to distinguish states within one basis (with relative phases $0$ and $\pi$) since she operates with them after reconciliation. Hence one can derive Holevo bound for two state SCW QKD protocol in arbitrary errorless channel as follows:

$$X = 1 - \frac{1+\psi}{2} \log_2(1 + \psi) - \frac{1-\psi}{2} \log_2(1 - \psi)$$

(3)

Secure key can be generated in case when secret key fraction $r$ is positive as follows:

$$r = 1 - X = \frac{1+\psi}{2} \log_2(1 + \psi) + \frac{1-\psi}{2} \log_2(1 - \psi) > 0$$

(4)

3. Conclusion

This work dedicated to strict mathematical proof of SCW QKD two states protocol security. The main security condition proposed here for the first time taking into consideration errorless channel and quantum theory of mode-bounded EOM. However, in order to complete security proof one should for instance consider origins of error appearance together with its correction process in the Alice-Bob channel; it will be covered in later papers.

Acknowledgments

This work was financially supported by the Ministry of Education and Science of Russian Federation (project № 114.578.21.0112, RFMEFI57815X0112).

References

[1] Bennett C, Brassard G 1984 Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175

[2] Wootters W, Zurek W 1982 Nature 299 802

[3] Gleim A, et al. 2016 Optics express 24 2619

[4] Miroshnichenko G, Gleim A 2015 arXiv preprint 1504.01632.
Erratum: Security conditions for sub-carrier wave quantum key distribution protocol in errorless channel

J. Phys.: Conf. Ser. 917 (2017) 062014

A Gaidash, A Kozubov, V Chistyakov, G Miroshnichenko, V Egorov, A Gleim

Department of Photonics and Optical Information Technology, ITMO University, Saint Petersburg 197101, Russia

viegrov@corp.ifmo.ru

Our paper «Security conditions for sub-carrier wave quantum key distribution protocol in errorless channel» published in Journal of Physics: Conf. Series 917 (2017) 062014 contains the following misprints we would like to correct:

1. On page 2, line 10 should be as follows: «Here we use quantum theory of mode-bounded electro-optic modulator (EOM) [4] due to useful properties of d-Wigner matrix in later calculation».

1. The Acknowledgments section must be read as follows: This work was financially supported by the Ministry of Education and Science of Russian Federation (project № 14.578.21.0112, RFMEFI57815X0112).