Security of Key Distribution While Transmissing via an Optical Fibre with Depolarization and Absorption

Anna Sotnikova, George Miroshnichenko
National Research University of
Informational Technologies, Mechanics and Optics
Saint-Petersburg, Russia
oirt@yandex.ru, gpmirosh@gmail.com

Abstract

New direction of modern information science (science about transfer method, storage and data processing) is optical quantum informations technologies.

Properties of the optical fibre (OF), used as an information channel, are very well known. Classical information is transmissed via OF with characteristics of an electromagnetic wave modulation, such as amplitude, intensity, phase, polarization. Nowadays, single-mode OF with slight absorption is developed, which will find wide application at long distance optical communication systems with high speed information transmission per bit. Mechanical and thermal influences on OF reduce apparition of interaction between orthogonal polarization modes, deforming type of transmissing waves polarization. In a general way, coefficient of waves connection depend on frequencies. This dependence reduce apparition of polarization modes dispersion, that is dependence wave velocity in OF on its polarization.

In quantum communications protocols quantum information is transmissed via OF, which is encoded in photon’s states- qubits. Nowadays there are some practical schemes of quantum cryptography.

Theoretically, single photon’s stations are used in a quantum cryptography plant. In present entanglement photon’s sources, probability of two photon’s pair generation is substantially lower than probability of biphoton generation. Therefore quantum cryptography systems based on EPR-protocol are the closest to the ideal systems.

In this research, distortion of quantum information (encoded in polarization photon’s states while transmitting them via OF in quantum cryptography plant) specifics is investigated. Quantum key distribution is realized by entanglement polarization biphoton stations. For key encoding is used quantum protocol BB84. Errors in the “sifted” key depend on possible interception of information, apparatus imperfection and noise in quantum channel. In literature degree of security key distributed is defined by parameter- rate of errors appearance quantum bits – QBER [1-3].

QBER depends from different factors, such as physical characteristics of quantum channel, transmitter and receiver, as well as from strategy of interception. In particular, QBER depends on relative error in the “sifted” key.

In this research, we find the average relative error (QBER) for variation of OB parameters in the sifted quantum key using BB84 protocol distribution with polarizing coding of the information.

It is possible to reduce QBER significantly, even when random OB parameters are widely dispersed.

For identifying the protocol working conditions at large distances we use the polarizing palpation effect, most clearly expressed when average value of OB parameters surpass their variation.

In conclusion, the correct choice of OB manufacturing technology will lower QBER to the critical level of 0.11, below which the distributed key can be applied for cryptographical purposes.

REFERENCES

[1] S. Castelletto, I. P. Degiovanni, M. L. Rastello. Quantum and classical noise in practical quantum-cryptography systems based on polarization-entangled photons. Phys. Rev. A 67, 022305, (2003).

[2] Nicolas Gisin, Gregoire Ribordy, Wolfgan Tittel, Hugo Zbinden. Quantum cryptography // Rev. Mod. Phys. V.74, P.145 -195, (2002).

[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, 1301, (2009).