Features of quantum key distribution system design

Mikhail Bobarov, Alina Borisova

JSC InfoTeCS, Moscow, Russia
*E-mail: Mikhail.Bobarov@infotecs.ru

In development of QKD system from the laboratory concept to its technical implementation as a product it is necessary to take into account both the features of the requirements for cryptographic protection of information, and the technical aspects of the QKD system implementation.

The requirements of cryptographic performance include, for example, the inability to fix any side effects of a useful signal from outside the QKD system, which imposes certain features on the choice of the elemental base of the electronic system.

Thus, in some QKD protocols implementations, the SPAD's clicks and the strobe signal (when operating in Geiger mode) can be dangerous for signal interception. Therefore, it is necessary to take into account that the diode strobe-generation circuit should work quickly enough and be low-noise. This is necessary to obtain adequate parameters of the SPAD and key generation rate.

From the cryptographic implementation point of view, the ideal solution would be a galvanic isolation between the control part of the circuit, the strobing part and the detector's part. However, the galvanic isolation of the control signals does not provide the necessary system performance parameters – key rate will be too low. A compromise option for the implementation of general requirements can be considered the use of ECL logic in the control part of the SPAD strobing. ECL logic has a drawback in the form of increased power consumption and increased heat dissipation, but it provides sufficient performance and it is low noise due to its specificity. Phase modulators, interferometers, attenuators, lasers, and single-photon detectors are the key optical elements in the majority of QKD systems [1]–[6]. Therefore, special demands are made on the quality of their operation. So the stability of the optical path difference of the interferometer has a direct impact on the parameters of the system: QBER, secret key rate. When designing equipment that will operate outside of laboratory conditions, it is necessary to ensure the constancy of the interferometer parameters in the entire range of operating conditions.

The optical path difference in fiber optic interferometers is provided, among other things, by the constant temperature of the fiber. Even a small change in the temperature of the interferometer during the secret key generation leads to an increase in QBER. To ensure temperature stability, the obvious solution is the passive method – thermal insulation of the interferometer. However, outside the laboratory environment, the use of only passive methods of temperature stabilization may not be enough, and in addition to them it is necessary to use active methods of temperature control of the interferometer.

Thus, the transition from the laboratory implementation of the QKD system to the finished product is a rather non-trivial task for the developers.

References

[1] *D. Lancho et al.*, QKD in standard optical telecommunications networks, International Conference on Quantum Communication and Quantum Networking, Springer, Berlin, Heidelberg, (2009).

[2] *E. O. Kiktenko et al.*, Demonstration of a quantum key distribution network in urban fiber-optic communication lines, Quantum Electronics, 47, N 9, (2017).

[3] *M. Fujiwara et al.*, Photon level crosstalk between parallel fibers installed in urban area, Optics express 18, (2010).

[4] *M. Sasaki et al.*, Field test of quantum key distribution in the Tokyo QKD Network, Optics express 19, N 11, (2011).

[5] *S. Wang et al.* Field and long-term demonstration of a wide area quantum key distribution network, Optics express, 22, N 18, (2014).

[6] *F. X. Xu et al*, Field experiment on a robust hierarchical metropolitan quantum cryptography network, Chinese Science Bulletin, 54, N 17, (2009).