

TRENDS IN THE DEVELOPMENT OF QUANTUM COMMUNICATIONS https://doi.org/10.1070/QEL17353

Development of quantum communications

Yu.V. Kurochkin

The relevance of research, development and implementation of quantum technologies has not been decreasing for many decades. The first stage of development and realisation of quantum technologies in practice made it possible to create lasers, high-speed optical communications, the Internet, nanophotonics, and many other applications that dramatically changed the world. In the past decades, we have been witnessing the rapid evolution of a new stage of quantum technologies, characterised by a desire to understand and apply the quantum properties of single atoms and photons. It is generally considered that quantum technologies are divided into three broad areas: quantum computing, quantum communications, and quantum sensors. Works in these areas are regularly reported in the Quantum Electronics journal.

This issue of the journal presents a selection of papers on the current trends in the development of quantum communications. Here we focus on quantum cryptography, or quantum key distribution. The central idea of the latter is based on the cloning prohibition theorem [1], which states that an arbitrary quantum state cannot be copied without introducing distortions. In practice it means that if information is transmitted via nonorthogonal single-photon states, an attempt to extract information will lead to a finite error rate. Quantum information theory, in turn, allows us to relate the upper bound on the fraction of eavesdropped information with the error rate [2]. Using single photons we distribute a key, i.e., a random sequence of bits that can then be used to secure information. If the error level indicates that the key was eavesdropped, then it is simply not used to transmit useful information. At the same time, the eavesdropper is considered to have the opportunity to use any future technologies that do not contradict the laws of quantum mechanics. This means that apart from being measured and transmitted, quantum states are allowed to be undergone nondestructive measurements [3] and conditional manipulations. The first and most commonly used protocol for transmitting information is BB84 [4], the advantage of which is the availability of rigorous proof of security. The existence of protocols with nonrigorous proof of security [5] opens up wide possibilities for the development of the theory of quantum communications. Optical implementations of even one protocol can vary greatly; for example, quantum states in optical fibre lines can be encoded both by polarisation [6] and by the phase [7] of photon quantum states, which opens up great scope for experimental work.

Government agencies, banks, telecommunications and energy companies are already using applied solutions based on quantum communications. Despite significant progress, significant restrictions still remain both in the qubit transmission range and in the rate of quantum key generation. These limitations are often fundamental, and to overcome them, new ideas and scientific developments are required. It is for this reason that quantum communications continue to be studied and developed at universities and research centres all over the world. The next stage of development can be quantum networks based on repeaters [8], through which a quantum signal will be transmitted over long distances via intermediate nodes without measurement. To implement such networks, an entanglement exchange protocol and quantum memory are required, in the development of which a significant scientific breakthrough has recently occurred [9]. This direction of development, in turn, requires new methods for preparing and measuring quantum states, including entangled states [10], and new proofs of the protocols security.

In recent years support of the development of quantum technologies at the state level has not only increased, but become targeted. For example, a Beijing–Shanghai quantum network has already been built in China, a large research support programme has been launched in the EU [11], quantum technologies in Russia are purposefully supported under the Digital Technologies federal project [12], and support programmes operate in England and the USA.

The published collection of papers is devoted mainly to theoretical research in the field of quantum information theory. Nevertheless, we tried not to ignore the experimental studies, which may be important for the implementation of quantum communication systems.

References

1. Wootters W.K., Zurek W.H. *Nature*, **299**, 802 (1982).
2. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dušek M., Lütkenhaus N., Peev M. *Rev. Modern Phys.*, **81** (3), 1301 (2009).
3. Fedorov I.A., Ulanov A.E., Kurochkin Y.V., Lvovsky A.I. *Optica*, **2** (2), 112 (2015).
4. Bennett C.H., Brassard G., in *Proceedings of International Conference on Computers, Systems & Signal Processing* (Bangalore, India: IEEE, 1984, p. 175).
5. Kurochkin Y. *Intern. Soc. Opt. Photon.*, 5833, 213 (2005).
6. Duplinskiy A., Ustimchik V., Kanapin A., Kurochkin V., Kurochkin Y. *Opt. Express*, **25** (23), 28886 (2017).
7. Dynes J., Yuan Z., Plews A., Takahashi R., Doi K., Tam W., Sharpe A., Kujiraoka M. *J. Lightwave Technol.*, **36** (16), 3427 (2018).
8. Duan L.M., Lukin M.D., Cirac J.I., Zoller P. *Nature*, **414** (6862), 413 (2001).
9. Bhaskar M.K., Riedinger R., Machielse B., Levonian D.S., Nguyen C.T., Knall E.N., Lukin M.D. *Nature*, **580**, 60 (2020).
10. Fedorov I.A., Ulanov A.E., Kurochkin Y.V., Lvovsky A.I. *Opt. Lett.*, **42** (1), 132 (2017).
11. https://qt.eu/.
12. https://digital.ac.gov.ru/support/#analytics.

Yu.V. Kurochkin International Centre for Quantum Optics and Quantum Technologies, ul. Novaya 100, 143025 Moscow, Skolkovo, Russia; e-mail: y.kurochkin@gmail.com

Received 10 April 2020
Kvantovaya Elektronika **50** (5) 425 (2020)
Translated by V.L. Derbov