Chinese Science Bulletin

Real applications of quantum communications in China

LI ChengZu

Department of Physics, National University of Defense Technology, Changsha 410073, China

The first metropolitan quantum cryptography network for government administration, which is named "Q-Government", has recently been field tested in Wuhu, Anhui Province by researchers of Key Laboratory of Quantum Information (CAS)[1]. Based on quantum cryptography, the network can guarantee the unconditional security for information transmission in an open channel.

Information security has become more and more important during the process of knowledge-based economic globalization. For both organizations and individuals, the anti-wiretapping and anti-tamper secure communication is the basic guarantee for all of the confidential solutions. However, the security of major classical cryptography realizations, including the private-key cryptosystem and the public-key cryptosystem, is based on the computational complexity of the cipher algorithm. At present, the rapid developments of distributed computing, ASIC design and especially the quantum computer and quantum algorithm have brought out unprecedented challenges to classical cryptography. The cases of sensitive information leakage, hacking and cracking are increasing. Consequently, a brand-new generation of quantum cryptography is refined as an urgent demand of secure communication.

Quantum cryptography exploits the quantum state as the information carriers, such as photons, to distribute secret keys remotely. The basic principles of quantum mechanics ensure that any attacking or tampering behavior of eavesdroppers will be perceived by legitimate users. Combined with the quantum key distribution and the "one-time pad" algorithm, quantum cryptography can establish unconditional secure communication between legal users, for now and the future.

In the process of QKD industrialization, the stability of the QKD system and the network techniques are two heavy cruxes. The Wuhu quantum cryptography network implements the Faraday-Michelson Interferometer (FMI) system, a unidirectional QKD scheme with the strict proof of its security and stability, which has the proprietary intellectual property rights. The significance of the FMI system is that it can auto-compensate the influence of the birefringence in the transmitting channel that will jeopardize the performance of QKD system. Several field demonstrations including Beijing-Tianjin QKD experiment at 2004, four-port star type network in Beijing at 2007 and the Wuhu quantum cryptography network for government administration at 2009, have clearly shown that the stability and robustness of this QKD basic device is sufficient for practical implementations.

Networking is a milestone for the popularization of quantum cryptography service. However, the no-clone theorem of quantum system makes data traffic difficult to route in the net while guaranteeing the security of the protocol. The Wuhu cryptography network assembles the widely-used techniques of wavelength routing, active optical switch routing and trusted relay to construct a hierarchical structure. A full-mesh backbone network is built with a quantum router in the center to supply a no-congestion communication among all the gateways, while the quantum switch based on the time multiplexing can achieve a balance for subnets between network efficiency and speed. In addition, trusted relay is a compromising method to extend the scale of the network as long as a practical quantum repeater is still missing. The whole implementation of this hierarchical framework is a key step toward the actualization of practical large-

doi: 10.1007/s11434-009-0523-6
email: czli@nudt.edu.cn

Citation: Li C Z. Real applications of quantum communications in China. Chinese Sci Bull, 2009, 54: 2976−2977, doi: 10.1007/s11434-009-0523-6

scale quantum cryptography network.

It is also an essential problem how to implement quantum cryptography into the practical utility. As a solution of the basic question to distribute secure key in the classical cryptography, quantum cryptography and quantum key distribution have a splendid prospective in the Internet and communication network for secure telephony, confidential fax and VPN, etc. To some extent, Wuhu cryptography network is quite a creative and interesting attempt to the electronic administration. Massive data traffic of government confidential files and personal information obviously have the right to increase the secure level to "quantum" unconditional secure level. In the future, quantum cryptography will become widely-spread as the sustainable development of secure media communication with instant video, sound and text message improves rapidly.

To eliminate "Hackers" and "Trojan horses" is one of the ultimate goals for all the security researchers, even though it seems next to impossible for classical cryptography so far. Quantum cryptography combined with the existing cryptosystems represents a milestone in the path of seeking unconditional security. Nevertheless, while the priest climbs a post, the devil climbs ten. The battle in the field of information security never ends. The safety depends not only on the cryptographic techniques, but also on the administration and the security awareness of users.

1 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chinese Sci Bull, 2009, 54: 2991－2997