Field experiment on a robust hierarchical metropolitan quantum cryptography network

October 16 2009

Key Laboratory of Quantum Information (CAS), University of Science and Technology of China has recently demonstrated a metropolitan Quantum Cryptography Network (QCN) for Government Administration in Wuhu, China. The project is reported in Volume 54, Issue 17 (September, 2009) of the *Chinese Science Bulletin* authored by Fang-xing Xu et al.

During the process of economic globalization, information security has become more and more important for both organizations and individuals. The secure communication is the basic requirement for all the confidential solutions to defend illegal eavesdropping and tampering. However, the security of a majority of classical cryptography is based on the complexity of the cipher algorithms and the development of distributed computing and specific hacking chips. Especially the quantum computer has become as a serious threat to classical cryptography nowadays. Consequently, a brand-new generation of quantum cryptography is refined as the urgent demand of secure communication.

Quantum cryptography can distribute secret keys by encrypting the information in a quantum system, such as photons. It is founded on the principles of fundamental physics rather than assumptions about the resources available to a potential adversary, which is provably secure against any attack by eavesdroppers allowed by quantum mechanics. Combined with the quantum key distribution (QKD) and the "one-time pad" algorithm, quantum cryptography can establish unconditional

secure communication between legal users, for now and the future. Moreover, in the process of QKD industrialization, networking is a milestone for the popularization of quantum cryptography service, especially a robust QCN compatible with the classical optical network which is a potential solution for the fast inflation of user number and unforeseen emergent demands of communication.

Aiming at that, the Key Laboratory of Quantum Information (KLQI) built this brand-new quantum cryptography network. Compared with the prior network projects, Wuhu QCN implements hierarchical structure with multi-levels and contains three different existing networking techniques. Nodes with different priorities and demands are set in the central backbone net or the subnet, and choose suitable networking technique. All the QKD links are based on the BB84 protocol with decoy state method which can promise the security level for the communication. Meanwhile, QKD software that all nodes run, application programs for encrypting text messages, sound and video are developed as well.

As the authors said in the paper that "In the process of QKD industrialization, the stability of the QKD system and the networking techniques are two heavy cruxes.", the Wuhu QCN implements the Faraday-Michelson Interferometer (FMI) system, an unidirectional QKD scheme with the strict proof of its security and stability which can auto-compensate the influence of the birefringence in the transmitting channel that will jeopardize the performance of QKD system. Several field demonstrations of KLQI group including Beijing-Tianjin QKD experiment (2004), four-port star type network in Beijing (2007) and the Wuhu quantum cryptography network for Government administration (2009) clearly show 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 quantum router, active optical switch routing and trusted relay to construct a hierarchical and extendable structure. A full-mesh backbone network is built with a quantum router in the center to supply a no-congestion communication between all the gateways simultaneously, 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 implement of this hierarchical framework is a big step toward the actualization of practical large-scale quantum cryptography network.

How to implement quantum cryptography into the practical utility is an essential problem as well. As a solution to 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 extend, Wuhu cryptography network is quite a creative and interesting attempt on the electronic administration. Massive data traffic of government confidential files and personal information obviously has 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.

It is the ultimate goal for all the security researchers to eliminate "Hackers" and "Trojan horses". Quantum cryptography as the earliest utility of quantum mechanism can supply an unconditional secure communication to benefit people. In the practical realization, QKD scheme's stability and key rate are not the only two important issues.

Especially with the urgent and inflating demand of emergent quantum cryptographic service, networking and routing techniques should be taken into serious consideration, as well as the application mode of QCN. The hierarchical metropolitan QCN field in Wuhu cannot only serve public secure communication with QKD but also act as a test bed to research those problems in realizations and applications of QCN in depth.

More information: Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. *Chinese Science Bulletin*, 2009, 54: 2991-2997, doi: 10.1007/s11434-009-0526-3

Source: Science in China Press