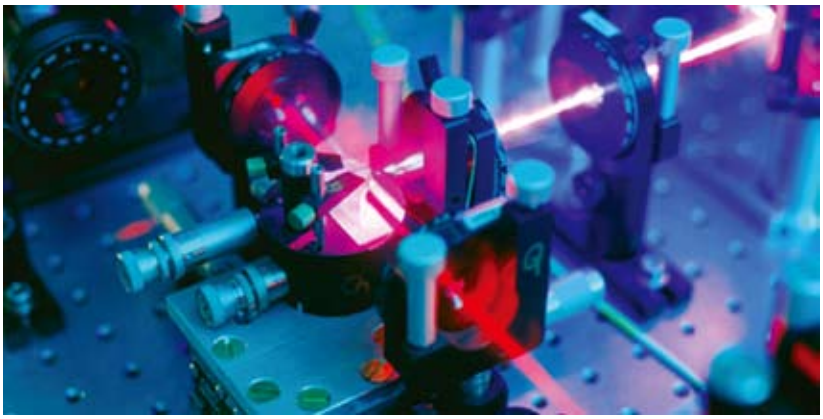
Quantum Key Distribution without Signal Disturbance Monitoring



Researchers from the CAS Key Laboratory of Quantum Information, University of Science and Technology of China have just achieved a significant progress in quantum key distribution research. Based on the self-developed active switching technology, they successfully conducted the world's longest – more than 90 km – round-robin differential phase shift (RRDPS) quantum key distribution experiment. The experiment results verified the feasibility of this novel protocol, and exhibited its potential advantage in practical scenarios. Their work was published in *Nature Photonics* under the title "Experimental demonstration of a quantum key distribution without signal disturbance monitoring".

Quantum key distribution (QKD) offers an optimal way for distant parties to share their secrets based on the laws of quantum physics. However, the imperfect characteristics of real-life systems and devices may compromise its practical security. In almost all of existing QKD protocols, some security parameters must be estimated or monitored to obtain the final secure key rate. Therefore, the signal disturbance may increase the system complexity, reduce the key generation efficiency, or cause vulnerabilities in practical QKD systems.

RRDPS protocol, proposed by T. Sasaki et al., doesn't require these parameters to bind the secure key rate. In this novel protocol, the sender divides the light pulses into a series of L-bit packets, and encodes the random signals as a superposition of time bins. The receiver randomly chooses the time delay to measure the interference results and its position. The possibility of eavesdropper to correctly guess the bit value correctly is very small when L is large, and the estimation of eavesdropping information is independent of the signal disturbance. Due to its independence with security parameters, RRDPS system is potentially applicable in complicated environments, while the implementation of a large L is a critical technical challenge.

By promoting the Faraday-Michelson interferometers with self-owned intellectual property rights and developing the high-speed optical active switching technology as well as the active phase compensating technology, Prof. HAN Zhengfu and his coworkers developed a high accuracy, high stability and low insertion loss interferometer, which can actively choose the time delay ranging from 1 to 64 bits to measure the quantum signals. With the help of the high-speed and low-noise InGaAs/InP detection unit, the whole system worked at 1 GHz repetition rate with the packet length of 65, and can obtain secure key bits under 90 km distance with the security parameter of 3×2^{-80} and taking the finite-key analysis into account.

It is the first active switching and the longest RRDPS experiment around the world. The stable interferometer is extendible and the experimental realization is excellent. The results demonstrated the feasibility of implementing long distance quantum key distribution without monitoring the signal disturbance, and exploited a new branch of practical QKD technologies.

This work was jointly supported by the Strategic Priority Research Program (B) of the Chinese Academy of Sciences, the National Basic Research Program of China and the National Natural Science Foundation of China.