学　位　論　文　内　容　の　要　旨

博士の専攻分野の名称　　博士（工学）　　氏名　張　維楊

学　位　論　文　題　名

Study on improved implementation of a transmitter in BB84 quantum key distribution system
（BB84 量子鍵配送システムの送信機実装の改善に関する研究）

Since its proposal in 1984, quantum key distribution (QKD) has been extensively developed in theory and implementation. QKD allows two distant parties, Alice and Bob, to share secure cryptographic keys, even in the presence of an eavesdropper, Eve. The performance of QKD systems has improved in recent years. For example, ultrafast QKD systems operating with above-gigahertz clock speeds provide secure key distribution at several hundred kilobits per second over 50 km transmissions. Moreover, systems installed on fiber networks can continuously operate for months. Despite such remarkable achievements, QKD systems have not been widely deployed in mainstream networks.

One of the main obstacles for QKD adoption is the lack of security certifications for practical devices. Although the unconditional security of the BB84 protocol for QKD has been proved theoretically, the proof requires several conditions to be satisfied. Among them, the transmitter should encode the information on the photon states without introducing errors, but this premise may not be fully satisfied in practice due to device imperfections.

Most high-speed QKD systems implementing the phase-encoding BB84 protocol use modulators based on lithium niobate for phase and intensity modulation controlled by electric signals during state preparation. Although the lithium niobate modulators are suitable for conventional optical communication systems, high-speed QKD systems can be adversely affected by imperfect modulation. In fact, the state preparation flaw, that is, the difference between the modulated and ideal states, arises from degraded electrical signals applied to the modulators. Although signal degradation due to practical bandwidth-limited devices is common in high-speed systems, it substantially increases the error rate in QKD systems compared to conventional light-wave communication systems, given the analog nature of quantum states. Moreover, discrepancy between prepared quantum states and theoretical quantum states caused by imperfection of device, especially the phase modulator which will be discussed in this article, severely decreases the key generation rate given the increased channel loss. Therefore, modulation devices should be more tolerant to degraded electric signals for realizing security certified ultrafast QKD systems. Although a loss-robust protocol is recently available, it requires to constrain the state errors into a small range to provide high key generation rate. In this article, we propose using a dual parallel modulator (DPM) to mitigate the state preparation flaw. We show that the DPM allows to generate QKD states that are robust to inaccurate voltage signals. We quantitatively define the state preparation flaw with fidelity between conjugated-basis states to relate the corresponding density matrices. Then, we examine the mechanism of state preparation flaw in conventional modulators and introduce the proposed DPM approach. We describe the method and results of state characterization using state tomography. Then, we estimate the state preparation flaw caused by varying the supply

voltage based on the results of state tomography. We also calculate the secure key generation rate and show that this rate is not affected by degraded modulation signals in the proposed approach.

Another obstacle is that QKD systems require amount of random numbers during its operation. The random number generation should be reliable, economical and practical. As new generation cryptographic scheme, quantum key distribution is based on quantum mechanics. Therefore, random number generators (RNG) likewise based on nature of quantum process comes to front. Unlike pseudo-RNG based on competitional algorithms, quantum random number generator (QRNG) has true randomness obtained via quantum process involving inherent randomness. QRNG is divided into three types, trusted device QRNG, self-testing QRNG, semi-self-testing QRNG. Among three types, the trusted device QRNG, also called practical QRNG has been developed rapidly because of its convenience and low cost. With a well-designed post-process, the trusted device QRNG is information-theoretically secure and meets the security requirements of most applications.

In the trusted device QRNG, many quantum processes are used to build practical QRNG, including photon number, vacuum fluctuation of quantum state, phase fluctuation of amplified spontaneous emission, intensity fluctuation of amplified spontaneous emission and so on. Among the above, phase noise, or phase fluctuation of amplified spontaneous emission, which is quantum mechanical by nature, is one of the major schemes adopted as random source. Because it has high generation rate and requires relatively simple implementation setup.

Traditionally, QRNG based on phase noise requires a light source and a self-delayed interferometer. These two devices are commonly implemented in BB84 QKD systems. If we can build QRNG with equipment in QKD system, it will cut more cost and reduce the risk of information leak during random number transmission from external QRNGs. Therefore, in this study, we propose a QRNG based on a transmitter of a time-bin BB84 QKD system. It uses the laser diode (LD) in QKD system as the phase noise source and Asymmetrical Mach-Zehnder interferometers (AMZI) in QKD system as the time-delay device. In addition, a Faraday mirror, a photo detector, an analog to digital converter (ADC) and a computer are used as the measurement part. With extraction and feedback process, we can generate random number at several GHz rate in theory, and supply to the QKD system in real time. However, it is difficult to use the AMZI in a high-speed QKD system, because a long-time delay ($\tilde{1}$0ns) is required in a common QRNG based on phase noise to reduce the effects of potential phase correlation between light emission from the laser. Such long-time delay could not be supplied by the interferometer in a real QKD system, because a short time delay (400-1600 ps) interferometer is necessary in high transmission speed QKD system. We found that the phase noise randomness from the gain switched LD depends on the operating condition. We optimized the laser operating condition to maximize the phase randomness and obtained a high generation rate. We could build a QRNG system with simple implementation and obtained the high random number generation rate that matched the requirement for QKD system. We tested random numbers from our QRNG and obtained successful results. We implemented a feedback system to improve the randomness, and optimized it by using test results to improve the tradeoff between QRNG generation rate and randomness.