学　位　論　文　内　容　の　要　旨

博士の専攻分野の名称　　博士（情報科学）　　氏名　葛　皓波

学　位　論　文　題　名

測定装置に依存しない量子鍵配送における時間同期に関する研究

（Study on measurement-device-independent quantum key distribution with time synchronization）

Modern cryptography can be divided into symmetric cryptography and asymmetric cryptography. The security of public key cryptography which belongs to asymmetric cryptography is based on computational complexity of its mathematical model. Communication is secured by proving that the reverse calculation of a mathematical problem is complex enough that decryption takes much longer than encryption. However, with the rapid development of quantum information technology such as quantum computer, computing power is greatly improved, so its security has been seriously threatened.

In order to deal with information security threat in new century, quantum cryptography based on physical laws is proposed and has been widely studied and applied in the world. Using quantum cryptography, any third party eavesdropping in the process of key transmission can be perceived. Combining with One-Time Pad encryption method which has been proved to be theoretically unconditional security, a theoretical unconditional secure communication system can be constructed. Quantum key distribution (QKD) and the first QKD protocol BB84 was proposed by Bennet and Brassard in 1984. Its system ensures theoretical unconditional security. However, the actual QKD system may have various security holes due to the inevitable errors and defects of the equipment. For example, detection efficiency mismatching attack and time-shift attack exploit the imperfection of the detector, and photon number splitting attack exploit the imperfection of the light source. In order to overcome photon number splitting attack on non-ideal single-photon source, decoy state method is proposed. With this theory, secure transmission distance and the generating efficiency of final key are greatly improved. Decoy state method has been recognized as a standard method to overcome photon number splitting attack.

For security holes caused by device imperfection, Acin et al. proposed device-independent QKD (DI-QKD). The advantage of this method is that it is possible to prove the unconditional security of a QKD system based on the Bell inequality without knowing the actual working state of the system. However, this scheme requires the single-photon detection efficiency to be close to 100

In 2012, Lo et al. proposed the measurement-device independent QKD (MDI-QKD). In this scheme, Alice and Bob send single photon pulses to a third party for the Bell state measurement (BSM). It can be immune to any detector side channel attacks. The system can be implemented with the lasers using the decoy state method. According to Lo et al., it is crucial that photons emitted by two independent lasers are indistinguishable. The MDI-QKD protocol is founded on the photon bunching effect of two indistinguishable photons at a 50:50 beam splitter (BS), and stable Hong-Ou-Mandel (HOM) interference should be observed. However, the fiber channel is susceptible to disturbances in real-world environments, and the effect of non-ideal visibility becomes particularly pronounced in

long-distance transmission. Therefore, it is imperative to elucidate the relationship between HOM interference visibility and the final key rate, and to establish methods for improving visibility. In practical compensation of the disturbance, it is of utmost importance to determine the desired accuracy to maintain the final key rate.

Our final goal is to provide an experimental scheme that ensures indistinguishablility of two photons. We first investigated the effect of two-photon interference visibility on the key generation rate under finite key lengths and the acceptable time delay between two Gaussian pulses at a 50:50 beam splitter for the decoy-state MDI-QKD protocol. Then, we propose a novel synchronization scheme for MDI-QKD aimed at mitigating the effect of temporal indistinguishability. We introduce a time synchronization scheme through disturbance compensation at the receiver, Charlie. Our experimental results demonstrate the feasibility of the frequency optical comb (OFC) scheme and the stability of precision control.

Chapter outlines are shown as follows.

Chapter 1: We review the development of quantum cryptography and quantum key distribution (QKD), and introduce the research background and the purpose of this study.

Chapter 2: We mainly introduce the principle of several common protocols for QKD. First, we introduce the first proposed BB84 protocol, which has been proved to be theoretically unconditionally secure. Subsequently, we introduce the realistic vulnerabilities of QKD systems and lead to some improved protocols for these problems.

Chapter 3: To address side-channel loopholes in QKD systems, we primarily focus on introducing the measurement-device-independent quantum key distribution (MDI-QKD) protocol. This section provides a detailed overview of the principles behind the MDI-QKD protocol. Additionally, we supplement this discussion with several commonly used encoding methods in practice.

Chapter 4: We emphasize a hitherto overlooked issue within MDI-QKD, involving the indistinguishability requirement for photons emitted by two independent laser sources at the measurement device in the middle, necessitating the observation of stable Hong-Ou-Mandel (HOM) interference. This section provides a detailed analysis of the effects of temporal distinguishability on MDI-QKD protocols during two-photon interference and derives the acceptable range of time delays under Gaussian photon conditions.

Chapter 5: We propose a novel synchronization scheme for MDI-QKD to address the temporal distinguishability effects described in the preceding sections. Our approach ingeniously leverages optical frequency comb (OFC) technology, installing each component of the synchronization system at the detection end, thereby mitigating errors introduced by long-distance optical fiber transmission. Experimental results indicate the high feasibility and exceptional cost-effectiveness of our proposed scheme.

Chapter 6: We summarize and discuss the research results of this study and describe the prospects of our research.