Demonstration of quantum cryptography without error rate monitoring
-New scheme based on the "wave function collapse" verified experimentally-

Nippon Telegraph and Telephone Corp. (NTT; Head Office: Chiyoda-ku, Tokyo; President: Hiroo Unoura) and The University of Tokyo (Bunkyo-ku, Tokyo; President: Makoto Gonokami, Ph.D.) have realized a quantum cryptography scheme that can assure security without monitoring the error rate of photon transmission.

NTT and UTokyo researchers performed a quantum key distribution (QKD) experiment based on a novel QKD scheme called the round-robin differential phase shift (RRDPS) protocol. This result is the first demonstration of QKD based on “wave function collapse”, which is distinguished from previous QKD schemes whose security is based on Heisenberg’s uncertainty principle. This experiment enabled us to realize QKD that does not require error rate monitoring between the sender and receiver, which will lead to simple and efficient quantum cryptographic systems.

This result will be published in the UK science journal “Nature Photonics” on September 14, 2015.

This research was supported in part by the ImPACT Program of the Council for Science, Technology and Innovation (Cabinet Office, Government of Japan) under the program “Advanced Information Society Infrastructure Linking Quantum Artificial Brains in Quantum Network” led by Prof. Yoshihisa Yamamoto.

1. Background
Network security is becoming increasingly important in recent years. Quantum cryptography is a method to provide ultimately secure means of communication based on quantum physics. In quantum cryptography, the sender, Alice, and the receiver, Bob, share a secure key via quantum key distribution (QKD), and they encrypt their communication with it. Since the security of the key shared by QKD is guaranteed by the principle of quantum physics, we can achieve communication that is secure against
eavesdropping with any future technology.

The security of conventional QKD relies on the Heisenberg uncertainty principle, which states that observing a quantum state necessarily disturbs it. In QKD, Alice encodes the key information on a quantum state of a photon, the elementary particle of light, and sends it to Bob through a transmission channel. If an eavesdropper (Eve) performs a measurement on the photon during the transmission, the quantum state is altered, and as a result, Alice and Bob probabilistically observe an error in their photon transmission. Therefore in a QKD, Alice and Bob monitor the error rate of key distribution using test bits so that they can estimate the amount of information that can be leaked to an eavesdropper. By compressing the key using the estimated amount of information leakage, they can obtain a quantum-secure key. Thus, in conventional QKD schemes, periodical monitoring of the error rate has been necessary. In 2014, a research team from the University of Tokyo (one of the authors of the release) together with a team from the National Institute of Informatics proposed the RRDPS protocol, whose security is based on wave function collapse, unlike previous QKD schemes. However, the experimental verification of the RRDPS protocol remained to be realized.

2. Achievements
By implementing the RRDPS protocol, NTT Basic Research Laboratories and the University of Tokyo jointly realized, for the first time, a QKD without the need for monitoring the error rate.

In the RRDPS protocol, the amount of information that can be leaked to Eve is bounded by a certain value (Figure 1). The protocol uses a quantum state that consists of multiple pulses as a carriers of the key, and the amount of the leaked information is determined solely by the number of pulses and is independent of the error rate. Therefore, by compressing the key using the estimated amount of the leaked information, we can distribute a secure key without monitoring the error rate.

With the present result, we can omit the periodical monitoring of the error rate between Alice and Bob using test bits in a QKD system and thus significantly simplify the control sequence between the sender and receiver. Furthermore, we can improve the efficiency of key generation since an RRDPS system does not consume keys as test bits. Note too that this is the first experiment where we can achieve unconditionally secure key distribution without relying on the Heisenberg uncertainty principle.
[Experiments]

1. The setup is shown in Figure 2. Alice prepares an optical packet that consists of five weak coherent pulses whose temporal interval is denoted by $T$, and modulates the phase of each pulse randomly by 0 or $\pi$. The modulated packet is then sent to Bob through an optical fiber. Bob is equipped with a round-robin phase difference measurement setup, which is composed of a $1 \times 4$ optical splitter, four delay Mach-Zehnder interferometers (MZI) with delay times of $T$, $2T$, $3T$ and $4T$, and single photon detectors that are connected to the output ports of MZIs. Since the average number of photons per packet is much smaller than 1, the phase difference measurement is performed at one of the four MZIs to which a photon happens to arrive.

2. We experimentally confirmed that secure key distribution is possible with the RRDPZS protocol (Figure 3). The maximum tolerable transmission loss between Alice and Bob is 8.7 dB. We also demonstrated secure key distribution over 30 km of fiber.

3. With our experimental data, we confirmed that we could distribute a secure key with its finite-size effect taken into account (Figure 4). Accordingly, we showed that we can achieve secure key distribution in a realistic situation where the finite-size effect of the key should be considered.

3. Technical Features

1. RRDPZS protocol

As shown in Fig. 1, Alice prepares an optical packet that consists of $L$ weak coherent pulses whose temporal interval is $T$, modulates the phase of each pulse randomly by 0 or $\pi$, and sends the packet to Bob through a transmission line. Bob is equipped with a variable-delay MZI that can take delay times of $T$, $2T$, $3T$, $4T$, ..., $(L-1)T$, and the two output ports of the MZI are connected to photon detectors. When the MZI delay is set at $NT$, Bob can measure the phase difference between two pulses separated by $NT$. If the phase difference between the two pulses is 0 ($\pi$), a photon is observed at detector 0 (1). Since the optical intensity of each packet is very low, Bob detects only one photon per packet in most cases. For every packet Bob receives, he records (a) the temporal position (or pulse number) where he received the photon, (b) the detector which detected the photon, and (c) the delay time chosen for the measurement. He then sends the recorded (a) and (c) to Alice via a conventional communication line. From this information, Alice can know (b), and so Alice and Bob can share an identical bit string by allocating the detection event at detector 0 and detector 1 as bit 0 and 1, respectively.
The RRDPS protocol has already been proven to be safe against an eavesdropper with an unlimited power from the principle of quantum mechanics. Here we explain the rough idea of the security of the RRDPS protocol using the concept of “wave function collapse”. In quantum mechanics, a wave function of a quantum state, which is initially in a superposition of several states, is reduced to a single state by a measurement. Since we can observe only the result after the state reduction, we can obtain only a portion of the information contained in an initial quantum state. An important characteristic of wave function collapse is that we can change the kind of information that can be extracted from the measurement by changing the way the wave function is measured. In the RRDPS protocol, the choice of the delay time corresponds to the choice of measurement, and the fact that a photon is detected only at a single pulse in the packet means that only a fraction of the wave function information is obtained in a measurement. The fact that Bob choose one from as many as L-1 measurements strengthens the security of the RRDPS protocol. Eve succeeds in eavesdropping only when she happens to choose the same delay as Bob’s, which means that the success probability depends only on the pulse number L and is independent of the error rate. In addition, the success probability decreases as L increases, and thus the amount of the leaked information is severely limited at a large L. In the above manner, the characteristics of the wave function collapse enable us to perform secure QKD with the RRDPS protocol.

(2) Implementation of round-robin phase difference measurement with optical splitter and delay interferometers
It is not very easy to realize a delay MZI that can actively vary the delay time with a low loss and high phase stability. To overcome this difficulty, we realized a round-robin phase difference measurement with only passive components as shown in Fig. 2, which consisted of an optical splitter, four delay MZIs, and photon detectors. Since the light intensity in a packet is very weak, a packet contains only one photon or less in most cases. Therefore, a photon launched into an optical splitter is randomly routed to one of the four MZIs that are connected to the output ports, and thus Bob can achieve random selection of delay time with good phase stability and relatively small loss.

4. Future Plans
In the present experiment, the number of pulses in a packet L was limited to five. However, it is predicted that the performance of an RRDPS system, such as the secure key rate and maximum reachable distance, will be greatly enhanced by increasing L.
NTT Laboratories will implement a round-robin phase difference measurement with ~100 delays using NTT's optical waveguide fabrication technologies so that we can enhance the performance. The University of Tokyo will investigate some expected features of the RRDPS protocol, such as the possibilities of highly efficient secure key generation with a shorter key length and high tolerance against noise as a research program supported by ImPACT.

[Publication]

<Contact information>
Nippon Telegraph and Telephone Corporation
Science and Core Technology Laboratory Group, Public Relations
a info@lab.ntt.co.jp
Figure 2: Experimental setup: implementation of round-robin phase difference measurement

Clock frequency: 2 GHz
Pulse number \( L = 5 \)
Average photon number per pulse: \( \ll 1 \)

Figure 3: Secure key distribution result

Secure key rate as a function of transmission loss (asymptotic key length assumed)

Error rate as a function of transmission loss
Figure 4: Results of finite-key analysis

Secure key length as a function of transmission loss for an effective measurement time of 260 s.

Fraction of the secure key length obtained with finite-key analysis relative to the asymptotic secure key length as a function of sifted key length.

20-km fiber

Without fiber

20-km fiber