Quantum Cryptography—Quantum Mechanics Opens up a New Trend in Communication Security

Kyo Inoue and Kaoru Shimizu[†]

Abstract

Quantum cryptography is a promising candidate for future technology that can provide photonic communication with unconditional security on the basis of the physical principles of quantum mechanics. This paper outlines why we will require quantum cryptography in the near future and reports recent efforts at NTT Basic Research Laboratories.

1. Introduction and background

The recent rapid growth in computer communication networks enables us to perform such tasks as conducting commercial transactions and voting in elections electronically, where the data is distributed among the people involved over a network. Information security technology plays an essential role in guaranteeing the secrecy and authenticity of such data. Modern cryptography involving public key cryptography and digital signatures has been believed to be able to cope with these requirements and is employed worldwide.

The security of modern cryptography is based on the computational complexity assumption, *i.e.*, the difficulty of solving certain mathematical problems using available computational power within a practical computational time. However, available computational power is increasing rapidly, and a group of many networked computers can provide tremendous computational power. Therefore, the security of the modern cryptography is continually being threatened or can be guaranteed only by ceaselessly increasing the key length. Moreover, an important new development—quantum computational power—has been theoretically proved to offer exponentially faster decryption. For these reasons, it is necessary to provide an alternative form of communication security that is secure against any amount of computational power.

Quantum cryptography is a promising candidate for such alternative security technology [1]. Unlike modern cryptography, the security is guaranteed by the laws of quantum physics—the quantum uncertainty principle, as we will explain later—and by information theory. We can reduce the probability of undesirable decryption to arbitrarily close to zero in an exponential way by increasing the key length, *i.e.*, the number of particles carrying quantum information. In the last decade, many theoretical and experimental studies have clarified that quantum cryptography can offer unconditional security for secret key distribution (quantum key distribution) between two parties. Quantum effects let users detect if a key has been leaked to an eavesdropper before they use it for encryption.

We can illustrate the physical aspect of quantum cryptography as follows. If we continue to divide the size of any material to a microscopic size, mysterious effects of quantum physics appear. One of these effects is the quantum uncertainty principle. Here we suppose that a microscopic particle can have two different features such as color and shape. Quantum uncertainty states that the color is inevitably erased whenever the shape is measured, and vice versa. Because a macroscopic material contains a tremendous number of microscopic particles, we can measure both the color and shape at the same time. This is why we usually do not experience the effects of quantum uncertainty. Quantum cryptography employs microscopic particles (photons), so we can detect any eavesdropping on the basis of quantum uncertainty. If the eavesdropper measures the shape

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan
E-mail: shimizu@will.brl.ntt.co.jp

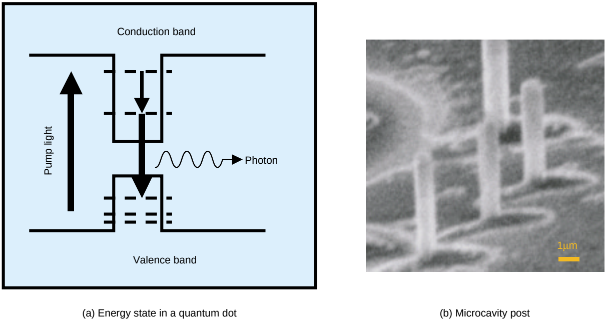
(color), he cannot resend the particle with the correct color (shape). Therefore, the sender and receiver can detect the eavesdropper by finding disagreements in shape or color. In typical quantum cryptography, the different sets of polarization states of photons correspond to the shape and color in the above illustration.

In the rest of this paper, we report both experimental and theoretical efforts at NTT Basic Research Laboratories.

2. Experimental efforts at NTT Laboratories

The security of quantum key distribution is based on the fact that an eavesdropper cannot perfectly identify a transmitted photon state without disturbing the state. This is true of situations in which one bit of information is carried by exactly one photon. However, if a signal pulse contains two or more photons, it is possible for an eavesdropper to acquire the information without being traced, by picking one photon out of the multitude and letting the remainder go to the receiver (which is called a ‘beam splitting attack’). To prevent this kind of eavesdropping, one can use a very weak laser light, which is attenuated so that one time-slot of pulse contains 0.1 photons on average, for example. However, the photon number of laser light fluctuates due to quantum uncertainty, and some pulses contain multiple photons even in such a weak laser light, enabling an eavesdropper to obtain partial information. It is known in principle that long-distance systems are especially vulnerable to information leakage caused by a beam splitting attack. To completely prevent such an attack, it is essential to use a single-photon source, which emits exactly one photon per pulse. For several years, a research group at Stanford University, USA, has been developing single-photon sources, with the support of NTT. In collaboration with the Stanford group, NTT Basic Research Laboratories recently carried out a quantum key distribution experiment using a single-photon source.

The single-photon source developed at Stanford University is an InAs semiconductor quantum dot cooled to about -270°C. When a semiconductor material is formed into a very small size (the height is 4 nm and the diameter is 20 nm in our case) and cooled to a low temperature, the medium has discrete energy levels like an isolated atom. (Note that conventional semiconductors have a continuous energy-level spectrum with a band structure.) Under illumination by a pump-light pulse, electrons in the semiconductor medium are excited from lower to upper energy levels by the pump light energy, and then spontaneously return to the original lower level (Fig. 1(a)). In the downward transition, the electrons lose energy, in the form of photons. Because the energy and the wavelength of a photon have a one-to-one correspondence in general, the photon emitted from the transition has



(a) Energy state in a quantum dot

(b) Microcavity post

Fig. 1. Semiconductor quantum dot single-photon source.

a wavelength corresponding to the energy level difference. In the above process, one energy level can accept just one electron (Pauli's exclusion principle), so one transition from one upper level to one lower level emits one photon. In other words, only one photon is emitted at a particular wavelength corresponding to the energy difference. By utilizing this photon emission phenomenon, we can obtain a single-photon source by optically filtering the photon emission from the dot at a particular wavelength. However, there is a problem with using a quantum dot: the spontaneously emitted photons can travel in any direction and it is difficult to collect them efficiently for use in transmission systems. To overcome this problem, a quantum dot is embedded in a post-shaped microcavity (Fig. 1(b)). In the upper and lower sides of the post, two different refractive index layers are formed alternately. Each of these acts as a mirror for a particular wavelength band (this is called a distributed Bragg reflector: DBR). The distance between these two DBRs determines the reflected wavelength. This microcavity allows a particular resonance mode to exist. A quantum dot embedded in such a structure emits photons in a particular direction, and we can efficiently collect them from the microcavity.

Using this directional single-photon source, we carried out a quantum key distribution experiment called BB84 protocol [2]. The experimental setup is shown in Fig. 2. Every 13 ns, the transmitter's single-photon source emitted single photons, whose polarization state was randomly set to one of four polarization states {vertical/horizontal linear} and {right/left circular} by a polarization modulator driven by a data generator working at 76 Mbit/s. The data pattern was recorded on a computer. In the receiver, the incoming photon train passed through a beam splitter with two outputs, equipped with different polarization state measuring devices. Because one photon cannot be split, each photon went to one or the other of the two outputs at random. Thus, a photon was randomly measured by either the apparatus for vertical/horizontal or right/left circular state measurement. The measured state was recorded on a computer. Then, after the photon transmission, the polarization state sent from the transmitter and that measured at the receiver were compared.

The results are shown in Fig. 3. When the transmitter sent photons with the vertical polarization state, for example, the receiver measured the photons as vertical linear, horizontal linear, right circular, and left circular states, with a ratio of 1:0:1/2:1/2, roughly speaking. This result shows that the apparatus for

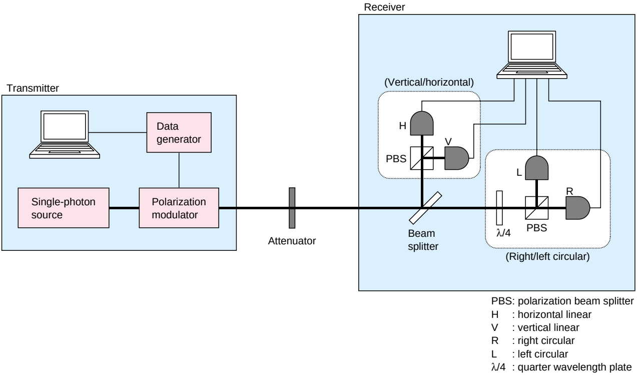


Fig. 2. Experimental setup for BB84 quantum key distribution scheme.

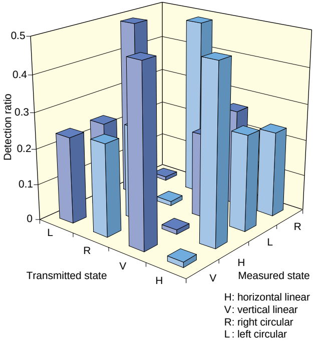


Fig. 3. Correlation between transmitted and measured states.

vertical/horizontal measurement correctly identified the transmitted state, whereas that for right/left circular measurement did not. The same is true for the other polarization states, such that when the transmitter sent vertical/horizontal states (or right/left circular states), the apparatus for vertical/horizontal (or right/left circular states) measurement gave correct answers while that for right/left circular (or vertical/horizontal) measurement did not.

This result indicates that this system can function as a quantum key distribution system as follows. After photon transmission, the receiver tells the transmitter which apparatus measured the photons, and the transmitter tells the receiver which polarization mode was sent, {vertical/horizontal} or {right/left circular}, but not the polarization state itself. Photons whose polarization modes match between transmitter and receiver have matching transmitted and measured states. Thus, the transmitter can obtain exactly the same bit information as the receiver, provided that both agree that the vertical (or right circular) state denotes bit “0” and horizontal (or left circular) state denotes bit “1”, for example. On the other hand, photons whose polarization modes do not match between transmitter and receiver are discarded because it is not possible to obtain identical bit information. The bit string obtained in this way is used as a secret key for encryption by the transmitter and decryption by the receiver when they perform one-time pad secret communication by classical means. Although the polarization state is utilized for encoding bit information in the above illustration, the same operation is possible by encoding bit information onto the phase of a photon split into two time-slots, which is more robust in fiber optic transmission.

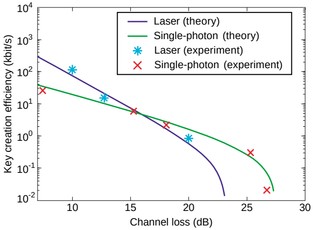


Fig. 4. Efficiency of creating a secret key as function of channel loss between the transmitter and receiver.

Because single photons are used, we do not have to worry about information leakage in a beam splitting attack. Moreover, we do not have to worry about an eavesdropper pretending to be the receiver and acquiring information by measuring the signal during transmission and resending a fake signal (an ‘intercept and resend attack’), because the mode-mismatched photons give incorrect answers. If an eavesdropper tried this attack, she would resend an incorrect signal when she measured the mode-mismatched photons, which would result in a discrepancy in the secret key bits between the transmitter and receiver. Thus, it is guaranteed that the key is free from eavesdropping if a sufficiently large number of test bits match between the transmitter and receiver.

The point of the above experiment is that a single-photon train is used as a signal carrier. To demonstrate the advantage of a single-photon source, we performed the same experiment using weak laser light for various channel loss rates between the transmitter and receiver. Figure 4 shows the results, where the secret key creation efficiency is plotted as a function of the channel loss. For small channel loss, weak laser light shows better performance because the photon emission efficiency of our single-photon source is still low, even with the microcavity structure. For large channel loss, on the other hand, the advantage of single photons overcomes the disadvantage of the lower efficiency, and better performance is obtained by the single-photon source. This clearly demonstrates that a single-photon source can be used to make long-distance quantum cryptography systems. This is the first experiment on quantum cryptography using a single-photon source, and also the first to demonstrate the superiority of a single-photon source.

3. Theoretical efforts at NTT Laboratories

This section describes our theoretical studies of the feasibility of general quantum cryptography for application to signature, authentication, and commitment tasks. In modern cryptography, these kinds of tasks are generally called "magic protocols." Our purpose is to guarantee their security on the basis of quantum physics, instead of by the computational complexity assumption.

Here, let us introduce the bit commitment task as the simplest example of the magic protocols. (i) Alice and Bob, who are located far apart, choose bit values "0" or "1" independently and memorize them. (ii) Commitment phase: Alice writes her bit value on a piece of paper and seals it in an envelope. She then sends the envelope to Bob. (iii) After receiving the envelope, Bob announces his selected bit to Alice. (iv) Opening phase: Alice gives the key to Bob so that he can open the envelope and read her commitment bit. If the sum of the bits is even (odd), Alice (Bob) wins the game. The bit commitment task is defined as the combination of the commitment phase and the opening phase, as illustrated in Fig. 5. For the game to be fair, (i) Alice's bit value must be kept secret from Bob in the commitment phase (concealing) and (ii) Alice must not be able to change her commitment bit in the opening phase (binding). In daily-use communication networks, similar requirements may arise frequently in electronic commerce, trade, and so on. For example, it is required in electronic auctions where bids must be concealed and bound. In modern cryptography, we can implement bit-commitment protocols by using as yet unproved computational complexity assumptions. However, the security of such mathematical protocols has always been threatened by the rapid progress being made in computational power with current computer technology. In early studies, therefore, it was widely expected that quantum cryptography would also be able to perform the task of bit commitment.

In recent years, however, it has become widely accepted that any type of quantum bit-commitment is impossible in principle. This is because the no-go theorem of quantum bit-commitment has been proved mathematically, provided that we require perfect concealment for the envelope transmitted in the commitment phase. In other words, if Alice can seal the envelope perfectly, she can always change her commitment bit by sending a faked key in the opening phase to invert Bob's decryption result and Bob cannot detect that the key was faked. Does this really mean that all quantum bit-commitment protocols are insecure in principle? Our answer to this question is "No!" In the last year, we have succeeded in finding an ingenious framework for accomplishing the bit-commitment task on the basis of quantum mechanics [3].

In our framework, as illustrated in Fig. 6, we redefined the task of quantum bit-commitment as a two-step procedure. (i) First step: Alice prepares a key and

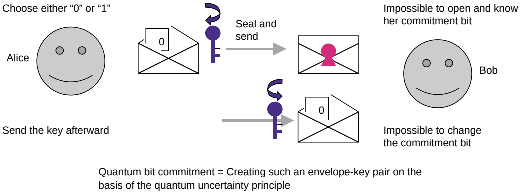

Choose either "0" or "1"
Alice
0
Seal and send
Impossible to open and know her commitment bit
Bob
0
Send the key afterward
Impossible to change the commitment bit
Quantum bit commitment = Creating such an envelope-key pair on the basis of the quantum uncertainty principle

Fig. 5. What is bit commitment?

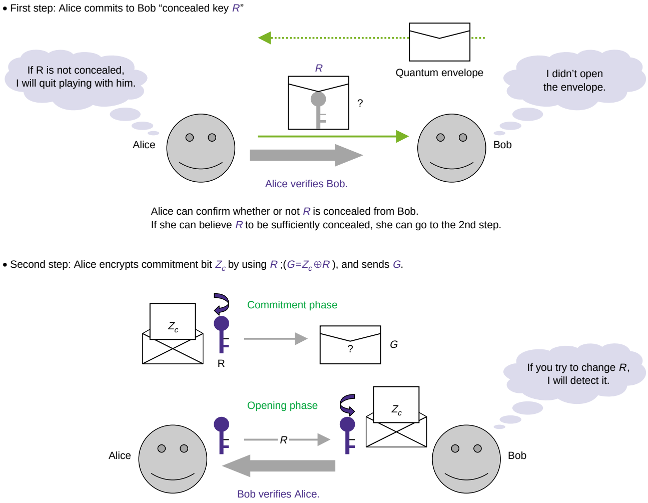

• First step: Alice commits to Bob "concealed key R"
If R is not concealed,
I will quit playing with him.
Quantum envelope
R
?
I didn't open
the envelope.
Alice
Bob
Alice verifies Bob.
Alice can confirm whether or not R is concealed from Bob.
If she can believe R to be sufficiently concealed, she can go to the 2nd step.
• Second step: Alice encrypts commitment bit Z_c by using R ;($G=Z_c \oplus R$), and sends G.
Z_c
R
Commitment phase
?
G
If you try to change R,
I will detect it.
Opening phase
Z_c
R
Alice
Bob
Bob verifies Alice.

Fig. 6. Our approach to quantum bit commitment: mutual verification frameworks.

puts it in a "quantum" envelope that was provided by Bob, and then sends the envelope to him. Although Alice cannot prevent Bob from opening the envelope, she can confirm whether or not he did, by asking him certain questions. If she finds no evidence of his dishonesty, she can be convinced the key is concealed. If she detects any inconsistency, she should quit playing with him. Because the key contains no information about her commitment bit, violation of the concealment is not a problem as long as it can be detected. This is the trick that makes it possible for us to avoid the no-go theorem. (ii) Second step: Alice encrypts her choice of commitment bit by using the key and then tells Bob the cipher information. This is exactly the same as the commitment phase because he cannot decrypt the cipher information without knowing the key. In the opening phase, Alice opens her key and Bob can decrypt. Here, he can determine whether or not she tried to fake the key by opening the quantum envelope correctly and asking her certain questions. Aside from the details, the quantum uncertainty principle and the probabilistic feature of quantum measurement processes make it possible for us to construct a secure bit-commitment protocol. In addition, we can prepare the quantum envelope by using many photons, which is more convenient.

4. Conclusion

After a short review of the basic principles and background, this paper reported the experimental and theoretical efforts at NTT Laboratories on quantum cryptography, which is expected to be the ultimate security technology. Although recent progress in basic research is significant, there still remain many technical hurdles that are obstructing practical and commercial implementation. In particular, it is important to develop photonic devices specialized for quantum cryptography use. Moreover, it is also necessary to design architectures for future secure communication network that are supported by a complementary combination of both modern cryptography and quantum cryptography. These fall within the scope of NTT Laboratories.

Our research was done in collaboration with Professor Yoshihisa Yamamoto at Stanford University and Professor Nobuyuki Imoto at The Graduate University for Advanced Studies in Japan.

References

[1] C.H. Bennett, G. Brassard, and A.K. Ekert, "Quantum cryptography," Scientific American, Vol. 267, No. 4, pp. 50-57, 1992.

[2] E. Wak, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, "Secure communication: Quantum cryptography with a photon turnstile," Nature Vol. 420, pp. 762-763, 2002.

[3] K. Shimizu and N. Imoto, "Communication channels analogous to one out of two oblivious transfers based on quantum uncertainty," Physical Review A 66, article number 052316, 2002.

Kyo Inoue
Senior Research Engineer, Physical Science Laboratory, NTT Basic Research Laboratories.

He received the B.S., M.S., and Ph.D. degrees from the University of Tokyo, Japan, in 1982, 1984, and 1997, respectively. He entered NTT Laboratories in 1984, and had been involved in research on optical communications. From 2001 to 2003, he stayed at Stanford University, USA, as a visiting scholar, working on quantum optics.

Kaoru Shimizu
Senior Research Engineer, Physical Science Laboratory, NTT Basic Research Laboratories.

He joined the Basic Research Laboratories, NTT in 1996. He is currently engaged in research on quantum information and quantum optics.