

Research Activities in Quantum Cryptography and Security Analysis

Authors: *Toshio Hasegawa** and *Toyohiro Tsurumaru**

1. Introduction

Quantum cryptography is a technology that ensures ultimate security¹⁾. Compared to current cryptography that could be defeated by the development of an ultra high-speed computer, quantum cryptography ensures secure communication because it is based on the fundamental physical laws. Among the various quantum information technologies, the most extensive research is being conducted on quantum cryptography, including the development of experimental equipment, field tests, and discussions on proposals of new theoretical schemes. This paper outlines the domestic and overseas trends in research and development on quantum cryptography and presents our achievements and current efforts toward its practical application. The security analysis of quantum cryptography, which is attracting an increasing amount of attention, is also discussed.

2. Research and Development Trends

In experiments with quantum cryptography, phase modulation is often used as the coding method. In this case, an interferometer is configured (for example, a Mach-Zehnder type) and the interference effects are detected by a photon detector. In actual communication experiments, careful and improved preparation such as higher interferometer stability is required. Typical optical schemes include a one-way setup where the light source is placed on the sending side and the detector on the receiving side, and a two-way setup ("plug & play" system) where the light source and detector are both placed on the same side and the photons traverse the same path twice to compensate for fluctuation. In the "plug & play" system, when transmitting from Bob (the recipient) to Alice (the sender), fluctuating path lengths and polarization shifts in the optical fiber is

compensated by that of the returning signal reflected by the Faraday mirror, resulting in a stable system. This high stability has made the plug & play system the mainstream until now. However, since the light source and the detector are both placed on the receiving side in this system, scattered light from the light source becomes a high-intensity input, which may increase the error rate and can be an obstacle for long-distance transmission. In addition, this system is vulnerable to one type of implementation attack (so-called "Trojan horse attack"), which creates a security issue. For these reasons, the one-way setup is more advantageous for longer-distance experiment and has been widely used in recent experiments. In this case, however, active compensation such as an optical path adjustment is required to maintain the stability of the interferometer.

Quantum cryptography experiments using optical fiber have been actively conducted, with several reports being published including one on a long-distance experiment over 100 km conducted at Toshiba Research Europe Ltd.²⁾ Field experiments between two remote points have also been conducted using existing optical fiber cables, including a 67-km experiment by the University of Geneva³⁾, a 96-km experiment by Mitsubishi Electric⁴⁾, and a 125-km experiment by the University of Science and Technology of China (USTC)⁵⁾. Table 1 shows representative field experiments between two remote points using the Bennett-Brassard 1984 protocol (BB84 protocol, the de facto standard).

In the field test, it is important to establish synchronization between the transmitting and receiving equipment and achieve stability. The timing of photon detection must be adjusted to within an accuracy of several hundred picoseconds, which requires optical and timing synchronization as essential functions. For effective use of the transmission line, it is desirable to achieve syn-

Table 1 Representative quantum cryptographic system experiments using optical fiber
(Field test between two remote points)

Research institute (year)	Optical scheme	Wavelength (μm)	Transmission distance (km)	Error rate QBER (%)	Raw key transmission rate (bps)
Geneva (2002)	P&P	1.55	67 (Field)	6*	150*
Mitsubishi (2004)	P&P	1.55	96 (Field)	9.9	8.2
USTC (2004)	One-way	1.55	125 (Field)	6	–
Toshiba R.E. (2005)*	One-way	1.3/1.55	20.3 (Field)	0.87*	430*

* Experiment with average photon number of 0.2, double the ordinary case.

chronization by sending a clock synchronization signal of high intensity, together with a quantum signal at the single-photon level. When this high-intensity clock synchronization signal is transmitted through an optical fiber along with the very weak quantum signal using a wavelength division multiplexing (WDM) technique, the technical challenge is to achieve high-isolation wavelength separation.

Progress in security analysis also continues, accompanied by proposals for new quantum cryptographic schemes. Formerly, the BB84 protocol and weak laser beam were used for most quantum cryptographic experiments at research institutes. However, this system is vulnerable to certain attacks called PNS (photon number splitting) attacks, which limits the transmission distance to less than 25 km if strict security standards are applied. To mitigate this drawback, it was, until recently, acceptable in the worldwide academic community to apply imperfect standards to practical quantum cryptography, which is that "a weak laser beam having an average photon number of 0.1 or less is assumed to be a single photon." Underlying such an assumption was an implicit common understanding: to achieve unconditional security for long-distance transmission, it is essential to have a strict single photon source, but this is difficult to realize. As a result, giving priority to the completion of a quantum cryptographic system, a weak laser has meanwhile been used for the light source to accelerate research on the detector, optical system and other elements. Once a low-cost single photon source eventually becomes available, it can be integrated into the system at any time.

This situation has changed greatly over the last several years since the "decoy method," an improved BB84 protocol, was proposed. With this method, unconditional security is achieved for long-distance transmission using a weak laser beam without a single photon source. With these developments, mainstream research is shifting its focus toward efficiently implementing an unconditionally secure quantum cryptographic system.

The basic setup for the decoy method is the same as that for the BB84 protocol except that Alice, the sender, changes the intensity of each light pulse intentionally and randomly. In addition, the distribution of light intensity will not be disclosed until Bob, the recipient, receives the light. Under this condition, Eve, the eavesdropper, is forced to attack without any knowledge about the intensity distribution. Therefore, if an attack is made, Bob finds statistical inconsistency in the signal detection rate. This enables accurate detection of the abovementioned PNS attacks and thus achieves more secure quantum cryptography. The unconditional security of the decoy method has been theoretically proved, and the achievable long distance is estimated

to be approx. 140 km. In fact, an approx. 100-km optical fiber experiment and 144-km free space experiment have already been reported.

To achieve secure and long-distance implementation with equipment simpler than the decoy method, a "differential phase shift scheme" (DPSQKD protocol) has been proposed. The equipment setup for this protocol is the same as that for a conventional optical communication scheme (DPSK scheme), resulting in a relatively low-cost system configuration. The basic idea is that quantum mechanical effects clearly appear because of the extremely low light intensity, and thus the system can be used for quantum cryptography. The greatest difference from the BB84 protocol in terms of security is that the bit information of the private key is coded into multiple light pulses, and thus the effect from eavesdropping appears in multiple light pulses and is easy to detect. The proposers initially claimed that this system can provide communication distance and speed exceeding that of the decoy method. However, they did not rigorously prove system security and discussed it only within the limited conditions of "individual attacks." Based on such evaluation, they reported their experimental results and claimed the world's longest distance of 100 to 200 km. After that, as a result of rigorous security analysis conducted by Mitsubishi Electric, it was found that the quantum cryptography in these experiments was not secure and that the communication distance using the DPSQKD protocol only reached 95 km⁶⁾ in practical experimental setups which are commonly used today. Since this scheme was found to be unsuitable for long-distance communication, discussion is now focused on the security of high-speed communication over short distances.

3. Research and Development at Mitsubishi Electric

3.1 Activities up to 2005

In 1999, Mitsubishi Electric started R&D activities of quantum cryptography, and in 2000, in collaboration with Hokkaido University, successfully conducted experiments on short-wavelength (830 nm) quantum cryptographic communication⁷⁾. In 2001, Mitsubishi was awarded a 5-year commission under the NICT (National Institute of Information and Communications Technology) Project I entitled "Research and Development on Quantum Cryptography," together with NEC and the University of Tokyo. In this project, Mitsubishi was responsible for "single photon generation," "single photon detection," "random number generation" and "technology for the quantum cryptographic key distribution system." Since then, our achievements include 1,550-nm high-performance single-photon detectors (dark count probability of approx. 10^{-6} , detection efficiency of approx. 20%) and experiments using these

detectors on an 87-km long-distance quantum cryptographic communication system⁸⁾ in 2002, and practical field experiments using the existing 96 km of optical fiber between Osaka and Kyoto in 2004⁴⁾. In the final year of the project, we also developed and functionally tested WDM quantum cryptographic equipment using 4 wavelengths to achieve higher speed. In addition to these achievements, Mitsubishi Electric also proposed a "circular-type quantum key distribution scheme" in the area of new optical scheme protocol studies, and conducted experiments on the proposed system to demonstrate transmission speed faster than that in conventional methods as well as multi-user communication capability⁹⁾. Mitsubishi Electric has actively participated in international exhibitions (ITU Telecom World 2003, 2006; RSA Conference 2005 Japan, etc.), presenting our quantum cryptographic system and quantum encrypted secure voice telephone / videophones as practical application examples.

3.2 Research and development for practical application

In 2006, we were awarded a 5-year commission under the NICT Project II entitled "Research and Development for Practical Applications of Quantum Cryptography." In this project, we have been working on the development of high-speed and high-stability quantum transmission technology, and key management and security evaluation technology, which will be required to realize a quantum cryptographic network. The quantum cryptographic equipment under development has a practical performance target: communication distance of 50 km and speed of 1 Mbps, and the following features: (1) Time-division transmission of the classical signal and the quantum signal (the classical signals are high intensity pulses, that is, they have a light strength similar to those used in conventional optical communications, and they carry the system clock information and the information to compensate for fluctuation in the polarization. On the other hand, the quantum signals are extremely weak laser pulses at the single-photon level which carry secret key bits.) (2) High-speed equipment with light source repetition rate at the GHz level, and transmission distance of several dozen km using BB84, decoy, or DPSQK quantum cryptographic protocol.

3.3 Development of multiplex transmission of quantum and classic signals

The key technology is the separation of multiplexed quantum and classical signals using time-division multiplexing. Specifically, we have developed and implemented a method to compensate for environmental temperature change and polarized state fluctuation, which is achieved through synchronized

gate control and feedback control by monitoring the clock and polarized state information contained in the classical signal. A very weak light at the single photon level is used for the quantum cryptographic communication, whereas a high-intensity signal at the classical optical level is used for the control of the communication equipment. The conventional way to provide a transmission line for this classical signal is to use a physically separated line or to separate the classic and quantum signals using WDM on a physically common line. However, the former poses a problem with facility cost, and the latter involves the difficult issue of separating the quantum and classical signals. Therefore, we are striving to develop such equipment that transmits and separates quantum and classical signals by WDM and time-division multiplexing (TDM) on a physically common transmission line. The equipment using TDM utilizes the classical control signals to compensate for the optical fiber propagation characteristics (polarized state fluctuation, etc.) and to transmit the clock signal. We also plan to transmit path control information with a view to networking applications.

3.4 Development of high-speed optical system equipment

Combining the multiplex transmission of quantum and classical signals and the high-speed single-photon detection technologies, we studied an experimental optical system required to achieve one of the final objectives of 1 Mbps at 50 km (see Fig. 1). This equipment features high-speed quantum cryptography using applicable protocol based on the BB84, decoy or DPSQKD protocol, light source repetition rate at the GHz level, and transmission distance of several dozen km. We also studied circuit-board partitioning by system functions that provides efficient configuration of the optical and electronic control system. Specifically, we further divided the transmitting and receiving functions and adopted AdvancedTCA to configure the circuit-board modules. The quantum and classical light sources are designed using DWDM CW DFB laser modules with wavelength of 1550.918 nm (classical signal) and 1549.315 nm (quantum signal), and driving frequency up to $\nu = 1$ GHz. To separate wavelength-multiplexed signals, DWDM DEMUX is designed for channel isolation between two signals of 80 dB or greater, which will be tested in the experimental system to determine if the weak quantum signal is accurately separated from the strong classical signal.

3.5 Security analysis technology

In parallel with the experiments, Mitsubishi Electric has also been conducting theoretical studies on system security. Recent achievements, as described at the end of Section 2, include a proposal related to a new attack

method against DPSQKD protocol and security analysis results based on the proposal⁶⁾. Theoretical study is also being conducted in collaboration with Hokkaido University on the decoy method, and, in 2007, we developed a new mathematical analysis method that precisely estimates the upper and lower bounds of the "yield" parameter¹⁰⁾. This achievement is expected to further enhance the communication distance and speed of the decoy method.

Theoretical studies have also been conducted on general quantum cryptographic protocols including authentication and signature not limited to quantum key distribution. Achievements in this area include quantum bit-string commitment¹¹⁾.

4. Summary and Future Prospects

In this paper, we presented research and development trends and Mitsubishi Electric's achievements and current R&D status on quantum cryptography. We also described the security analysis technology. Such theoretical analysis is important because quantum cryptography carries meaning only when its security is theoretically proven, and also for promoting steady and efficient development of actual quantum cryptographic equipment. Even today, the search for a new method continues and in addition to the decoy method and DPSQKD protocol as presented in this paper, new protocols such as the six-state protocol and continuous-variable protocol are being proposed. However, proof of security has not kept pace with new proposals,

and protocols that are proven to have unconditional security are in the minority. It is important to understand the trend in security analysis and we will continue to strive toward our own research goals.

Part of this work was supported by the project "Research and Development on Quantum Cryptography" of National Institute of Information and Communications Technology as part of Ministry of Internal Affairs and Communications of Japan's program.

References

- (1) Edited by Sasaki et al., Quantum Information Communication, Optronics Co., Ltd. (2006)
- (2) C. Gobby et al., Appl. Phys. Lett. 84, 19, 10 (2004)
- (3) D. Stucki et al., New J. Phys. 4, 41 (2002)
- (4) T. Hasegawa et al., CLEO/Europe-EQEC2005, EH3-4, Munich (2005)
- (5) X. Mo et al., Opt. Lett. 30, 2632 (2005)
- (6) T. Tsurumaru, Phys. Rev. A 75, 062319 (2007)
- (7) T. Hasegawa et al., IEICE E85-A No. 1, 149 (2002)
- (8) T. Hasegawa et al., CLEO/QELS2003, OTuB1, Baltimore (2003)
- (9) T. Nishioka et al., IEEE PTL 14, 4 (2002)
- (10) T. Tsurumaru et al., Phys. Rev. A 77, 022319 (2008)
- (11) T. Tsurumaru, Phys. Rev. A 71, 012313 (2005) and 74, 042307 (2006)

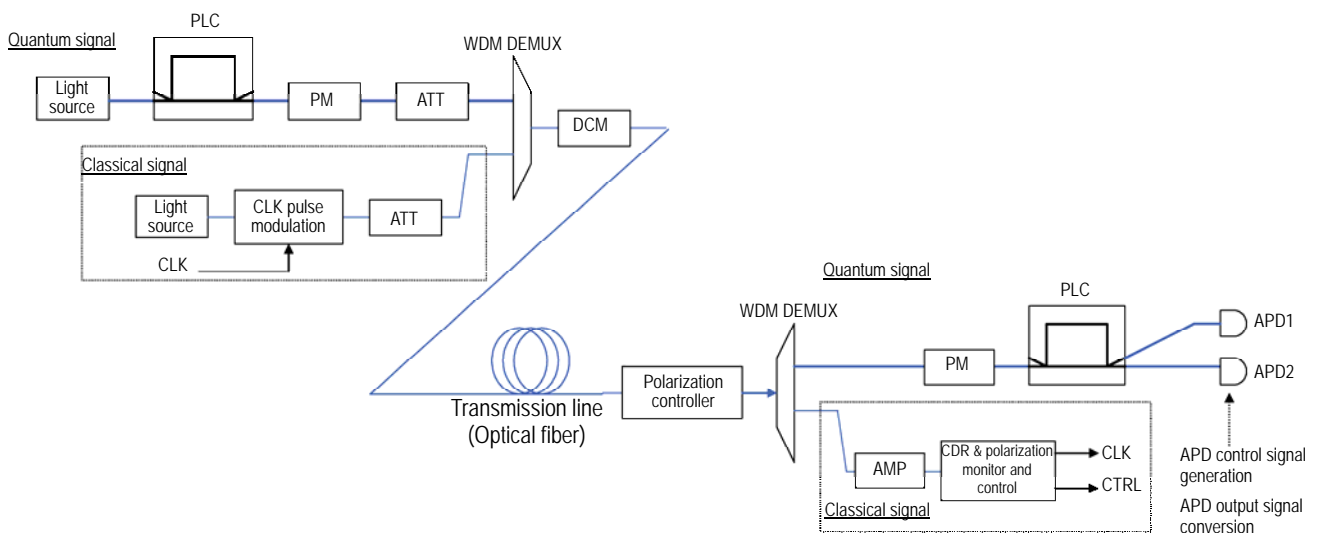


Fig. 1 Basic configuration of the quantum cryptographic system under development

PLC: planar light circuit, PM: phase modulator, ATT: optical attenuator, CLK: clock, WDM MUX: wavelength division multiplexing, DCM: dispersion compensation module, AMP: optical amplifier, CDR: clock data recovery, APD: avalanche photodiode