4-5 Research Activity of Quantum Security

WASEDA Atsushi

Since only the quantum security can realize the unconditional security, the importance of the quantum security technologies is increasing. Therefore, it is researched by laboratories in each country. The quantum security technology is researched also by Security Fundamental Group aiming at the achievement of the society where the quantum cryptography is widely used in general. In this paper, we report the outline of researches of the quantum security in this group of five years recently, the cooperation with other groups and the relating events such as UQCC.

Keywords
Quantum cryptography, Quantum security, Updating Quantum Cryptography and Communications (UQCC)

1 Introduction

Because of the development of technologies in recent years, very extensive networks have been built up, and a huge number of computers have been connected with the networks. In this situation, the roles played by security technologies to protect the networks are truly important. The typical examples of attacks to the networks include those which crash communications systems themselves such as a DoS (Denial of Service) attack, computer hacking with computer viruses or the like, and attacks aiming at data disclosure and falsification by masquerading as the other party and retrieving data or by picking up data which flows on networks. General measures which deal with these attacks include establishment of a network monitoring mechanism such as nicter[1] and introduction of antivirus software and modern cryptography technologies.

Among the measures aforementioned, many of the modern cryptography technologies have been based on an idea, with respect to safety, that the technologies cannot be beaten even with use of computers. However, the safety of the technologies has been placed under threat because of significant improvements in recent computer performance. Typical measures to deal with this problem and ensure safety are to change hash functions from SHA-1 (160 bits) to SHA-2 (256 bits) and to extend the key length of RSA public-key cryptography from 1024 bits to 2048 bits. However, system upgrading due to replacement of cryptographic technologies not only adversely affects service continuity (BCP) but also decreases operational safety due to, for example, parallel operations of old and new systems and the necessity of maintaining compatibility with old data. In addition, new types of computers such as quantum computers have been introduced to the market. Therefore, cryptography technologies whose safety is not affected by the improvement of computer technologies have been demanded. With respect to modern cryptography, methods such as one time pad[2] have been suggested to meet this demand. However, those methods are very inefficient and have not been regarded as practical. On the other hand, attempts have also been made to solve the problems by introducing quantum technologies. In particular, quantum key distribution has drawn attention because it can solve the biggest problem regarding one time pads, namely safe key sharing. As a result, demonstration experiments of quantum networks such as SECOQC[3] and Tokyo QKD network[4] have been conducted. In this way, using quantum technologies can improve safety regarding communications and data protection, and quantum security is an attempt to actively utilize quantum technologies.

To deal with the aforementioned problems, the Security Fundamentals Group has conducted joint research with the Quantum ICT Group and Space Communication Group. With the Quantum ICT Group, the Security Fundamentals Group has performed safety evaluation in terms of quantum cryptography and other quantum security protocols. With the Space Communications Group, the Group has conducted research on issues such as evaluation of communication channel capacity regarding quantum communications when using quantum measurement devices. The Quantum ICT Group, when the joint research was started, did not have a framework for following the latest movements in modern cryptography. On the other hand, the Security Fundamentals Group had a limited understanding of experimental apparatus and safety theories in terms of quantum cryptography. Therefore, the two groups have attempted to optimally combine their respective knowledge and experience, resulting in the achievement of certain research accomplishments.

This article outlines the accomplishments of quantity security research conducted by the Security Fundamentals Group. In **1.1**, research accomplishments and events in the second medium-term plan are briefly described in chronological order. In **1.2**, as a representative major event in this medium-term plan, a description of Updating Quantum Cryptography and Communications (UQCC)[5] is provided. In **1.3**, the Tokyo QKD network is described. In **1.4**, the Quantum ICT Committee is outlined at which the policies of Japanese quantum cryptographic research are determined. Then, research conducted by the staff members of the Security Fundamentals Group in the second medium-term plan are outlined, followed by a conclusion.

1.1 Flow of quantum security research by the Security Fundamentals Group in the second medium-term plan

Full-fledged quantum security research activities by the Security Fundamentals Group were started when the author was employed as an expert researcher in 2007, the second year of the medium-term plan. In this fiscal year, the Group had not yet started practical joint research with other groups and conducted research mostly on its own. The accomplishments in this fiscal year include a paper accepted for the IPSJ Journal, in terms of suggestion of quantum multi-secret sharing[6] as one variation of quantum secret sharing; this accomplishment resulted from improvement of the author's research conducted in his postgraduate program. As for presentations at domestic conferences, the author made suggestions about quantum secret sharing between multiparty and multiparty[7] at the 2008 Symposium on Cryptography and Information Security (SCIS). In October that year, UQC (Updating Quantum Cryptography) 2007 was held in Tokyo for the first time.

In FY 2008, the Security Fundamentals Group started practical discussions and joint research with the Quantum ICT Group, evaluated the channel capacity regarding quantum communication channels, and presented the results at SCIS 2009[8]. In addition, the author made a presentation about the quantum secret sharing at International Symposium on Information Theory and its Applications (ISITA 2008)[9]. The UQC conference was also held in Tokyo in 2008.

In also FY 2009, an article about channel capacity regarding fiber band quantum channels was accepted for the Journal of the Optical Society of America[10]. To extend the accomplishments to deep space, the author's group worked with the Space Communication Group, followed by presentation of the accomplishments at 2010 International Conference on Availability and Security[11]. In this fiscal year, the group started exchanging ideas with Dr. Antonio Assalini from University of Padua, to further develop the research. In addition, Group Leader Tanaka made a presentation at SCIS 2010, about examination of the quantum secret modulation method using modes of operation[12].

In FY 2010, the final year of the medium-term plan, such major events as the start of the operation of the Tokyo QKD network and UQCC 2010 took place. In addition, two projects with respect to research & development promotion fund pre-projects were adopted: “research and development about ultra-high-speed mobile communication and high-security global quantum key distribution technologies” and “basic development of quantum authentication and cryptography technologies for materialization of high security”. As for presentations, the author made a presentation at SCIS 2011 about multiparty simultaneous quantum identity authentication[13].

1.2 Updating Quantum Cryptography[5]

UQC and UQCC (Fig. 1) are international conferences organized by NICT, Information-technology Promotion Agency (IPA), and National Institute of Advanced Industrial Science and Technology (AIST), and were held three times in total so far.

The first conference was held for three days from October 1 to 3, 2007, at the convention hall in Akihabara Daibiru, and a lot of people attended also from overseas organizations and institutions including the NIST (National Institute of Standards and Technology). On the third day, closed sessions by experts only were held, and reports were made about various countries’ latest movements in quantum cryptography and research/development of key technologies. At the discussions, participants from the NIST actively expressed their opinions about unconditional safety and side channel attacks. On the following days, on October 4 and 5, the second Quantum ICT Committee was held in the SCAT, and reports were made by research institutions, about, for example, openly-selected research granted by the Ministry of Internal Affairs and Communications(SCOPE) and research delegated by NICT, and discussions were held about future activity schemes.

The second UQC was held for two days from December 1 and 2, 2008, once again at the convention hall in Akihabara Daibiru. At the conference, presentations were made about, for example, the SECOQC (Secure Communication based on Quantum Cryptography) held in the EU and standardization activities at the ETSI (European Telecommunications Standards Institute). In addition, ICT-related Japanese national strategies including quantum cryptographic technologies were explained by the participants from the Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry.

The third UQCC was held for three days

Fig.1 UQCC

from October 18 to 20, 2010, at ANA Inter-Continental Hotel in Tokyo. On October 14, just several days before the conference, the Tokyo QKD Network, which is the latest quantum cryptography network composed of optical fiber networks, started to operate in the Tokyo metropolitan area, and thus the outline and expectation regarding the Tokyo QKD network were explained, in addition to the latest domestic and overseas research accomplishments and movements toward actual utilization.

1.3 Tokyo QKD network[4]

The Tokyo QKD network (Fig. 2) is the testbed of the quantum cryptography network whose operation was started in October 14, 2010. NICT's Quantum ICT Group has played central roles in its construction and operation, together with NEC Corporation, Mitsubishi Electric Corporation, and Nippon Telegraph and Telephone Public Corporation. The creation rate of secret keys is 100,000 bits per second with 45 km optical fiber lines, the world's highest speed in actual environments. In the future the network is likely to be used for mutual connectivity experiments with other systems and for research and development of integrative operation technologies with modern cryptography.

1.4 Quantum ICT Committee

The Quantum ICT Committee has been held once a year. At the committee, reports were made by research teams adopted by SCOPE about the latest research accomplishments, and discussions were performed about, for example, the next research implementation strategies such as important issues including the extension methods of quantum cryptography related accomplishments, linkage with other fields, next-generation quantum cryptography, quantum relay, quantum device, and basic theories regarding quantum information.

2 Research overview

This chapter outlines the research accomplishments made by the Security Fundamentals Group's staff members in the second medium-term plan.

2.1 Quantum multi-secret sharing scheme[6]

A quantum secret sharing scheme converts secrets handled by a secret sharing scheme that performs distributed encoding of secrets to quantum states, and converts the communication channels used into quantum communication channels. This article defines a quantum multi-secret sharing scheme for the first time, in which secret information is turned into quantum states and multiple secret states

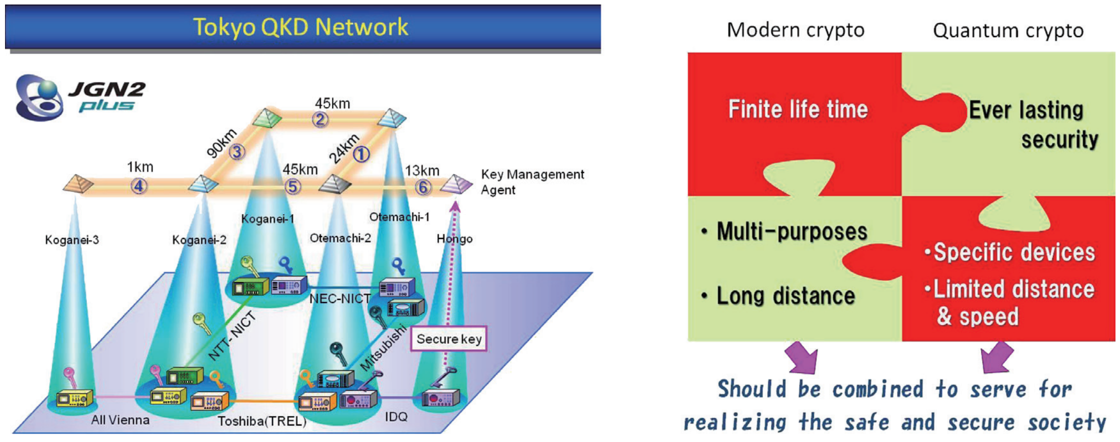


Fig.2 Tokyo QKD Network

are handled, and suggests its configuration method. Furthermore, the article clarifies various characteristics to be satisfied by a quantum multi-secret sharing scheme.

Definition: A set of participants is P, and a set of quantum states of secrets is $\{S_1, \cdots S_n\}$. With respect to individual secrets S_i, the auxiliary system used for purification is R_i, and the access structure is Γ_i. For each Γ_i, $T_i = \{R_1, \cdots, R_n\} \setminus \{R_i\}$ is defined. Then, a quantum multi-secret sharing scheme satisfies the following two conditions.

(1) Recoverability

For all $A \in \Gamma_i$, $I(R_i : T_i A_i) = I(R_i : S_i)$

(2) Secrecy

For all $B \notin \Gamma_i$, $I(R_i : T_i B_i) = 0$

Where $I(A : B)$ represents mutual information quantity of system A and system B.

This result is an extension of the definition of the quantum secret sharing scheme having a single secret, and (1) indicates that an inverse transform is present in terms of quantum operation through which secret S_i was distributed. (2) indicates that an inverse transform is absent in terms of quantum operation through which system B_i and auxiliary system T_i were distributed.

The suggested method (Fig. 3) is extension of the quantum secret sharing scheme which uses a Monotone Span Program (MSP). An MSP on set P is composed of (F_q, M, g, t) such as the following (1) to (4). (1) F_q: finite field with order q; (2) M: matrix of $d \times e$ on F_q; (3) g: function $(\{1, \cdots d\} \rightarrow P)$ which assigns the line of M to participant P; (4) target vector t. The MSP is accepted when t is included in subspace generated by submatrix M_A of M where $g(\cdot) \in A$ is resulted in terms of set A.

Such a quantum multi-secret sharing scheme is called an (m, t, d) quantum threshold multi-secret sharing scheme such that the number of secret states is m, the number of shares is t and all secret states can be reconstructed by collecting d or more number of shares. Regarding this quantum threshold secret sharing scheme, the following theorem has been obtained.

Theorem: An (m, t, d) quantum threshold multi-secret sharing scheme composed with an MSP has secrecy if and only if the following two conditions are satisfied: (1) $d \geq t + m + 1$; (2) $e \geq t + m + 1$.

2.2 Quantum secret sharing scheme between multiparty and multiparty[7] [9]

This is one variation of a quantum secret sharing scheme like the one in the previous section. This method distributes secrets in the classical state, using quantum states (Fig. 4). In the method, participants are divided into two groups; both groups cooperate to generate distribution information, but the members of the individual groups reconstruct distributed information separately. The method does not allow secret information to be selected beforehand, so that secret information cannot be known until the secret is reconstructed; it performs bit sharing and secret distribution at the same time. This method can be used, for example, to update distribution information without changing secret information when part of the distri-

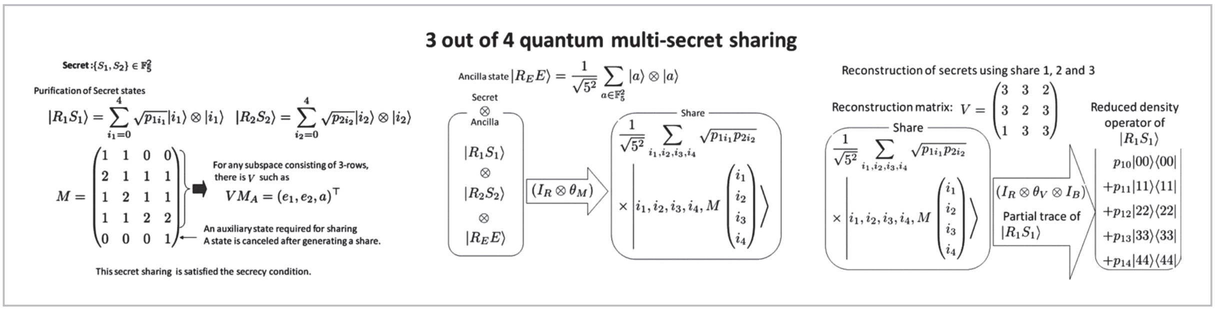

3 out of 4 quantum multi-secret sharing
Secret :$\{S_1, S_2\} \in \mathbb{F}_5^2$
Purification of Secret states
$|R_1S_1\rangle = \sum_{i_1=0}^{4} \sqrt{p_{1i_1}}|i_1\rangle \otimes |i_1\rangle$
$|R_2S_2\rangle = \sum_{i_2=0}^{4} \sqrt{p_{2i_2}}|i_2\rangle \otimes |i_2\rangle$
$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
For any subspace consisting of 3-rows, there is V such as
$VM_A = (e_1, e_2, a)^\top$
An auxiliary state required for sharing
A state is canceled after generating a share.
This secret sharing is satisfied the secrecy condition.
Ancilla state $|R_E E\rangle = \frac{1}{\sqrt{5^2}} \sum_{a \in \mathbb{F}_5^2} |a\rangle \otimes |a\rangle$
Secret
$\otimes$
Ancilla
$|R_1S_1\rangle$
$\otimes$
$|R_2S_2\rangle$
$\otimes$
$|R_E E\rangle$
$(I_R \otimes \theta_M)$
Share
$\frac{1}{\sqrt{5^2}} \sum_{i_1,i_2,i_3,i_4} \sqrt{p_{1i_1}p_{2i_2}}$
$\times \left| i_1, i_2, i_3, i_4, M \begin{pmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \end{pmatrix} \right\rangle$
Reconstruction of secrets using share 1, 2 and 3
Reconstruction matrix: $V = \begin{pmatrix} 3 & 3 & 2 \\ 3 & 2 & 3 \\ 1 & 3 & 3 \end{pmatrix}$
Share
$\frac{1}{\sqrt{5^2}} \sum_{i_1,i_2,i_3,i_4} \sqrt{p_{1i_1}p_{2i_2}}$
$\times \left| i_1, i_2, i_3, i_4, M \begin{pmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \end{pmatrix} \right\rangle$
$(I_R \otimes \theta_V \otimes I_B)$
Partial trace of $|R_1S_1\rangle$
Reduced density operator of $|R_1S_1\rangle$
$p_{10}|00\rangle\langle 00|$
$+p_{11}|11\rangle\langle 11|$
$+p_{12}|22\rangle\langle 22|$
$+p_{13}|33\rangle\langle 33|$
$+p_{14}|44\rangle\langle 44|$

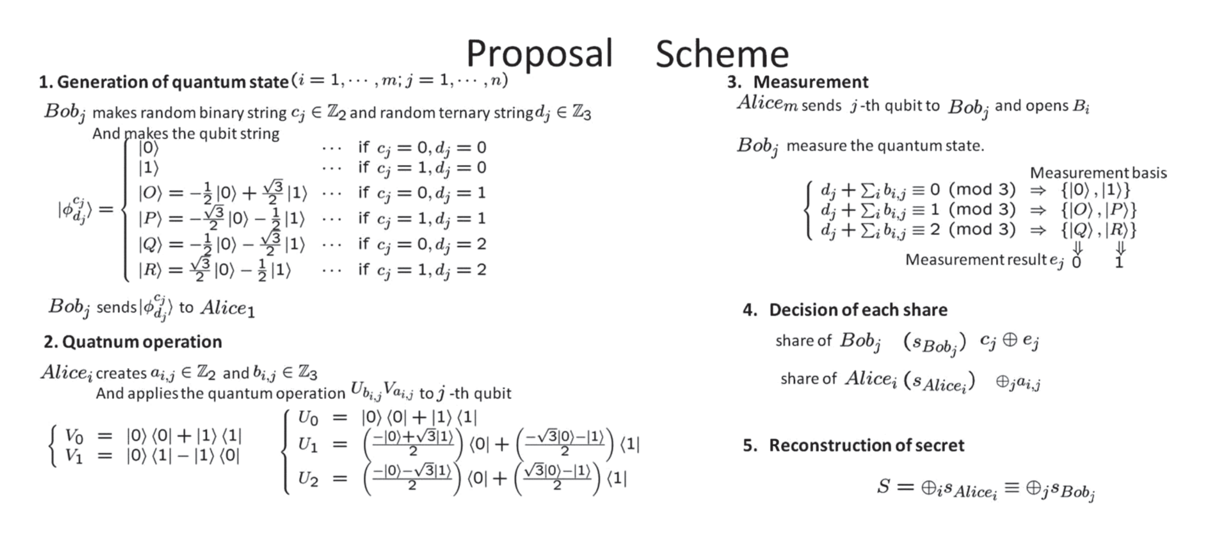
Fig.3 Quantum multi-secret sharing scheme

bution information is leaked.

2.3 Evaluation of channel capacity regarding fiber band quantum channel [8][10][11]

In the joint research with the Quantum ICT Group, communication channel capacity of quantum communication channels was calculated for each of the following cases and compared with the theoretical upper limit given by Giovannetti et al.; with two modulation methods, phase shift keying (PSK) and quadrature amplitude modulation (QAM), in fiber band 50 THz (1.2 – 1.6 µm); Holevo information was used that gives the maximum quantity of information obtained through homodyne detection, heterodyne detection, square root detection (SRD), and quantum measurement. The result has allowed the author's group to confirm superiority over the existing optical communications which do not consider quantum effect in terms of 1 mW or less input power (Fig. 5).

The result has also allowed the author's group to confirm that the maximum communication channel capacity results when the BPSK modulation method is used for 1 µW or less input power and homodyne detection is performed, and when modulation with more values is performed for 1 µW to 1 mW input power and heterodyne detection is performed.



Proposal Scheme

1. Generation of quantum state $(i = 1, \cdots, m; j = 1, \cdots, n)$

Bob_j makes random binary string $c_j \in \mathbb{Z}_2$ and random ternary string $d_j \in \mathbb{Z}_3$

And makes the qubit string

$$|\phi_{d_j}^{c_j}\rangle = \begin{cases} |0\rangle & \cdots \text{ if } c_j = 0, d_j = 0 \\ |1\rangle & \cdots \text{ if } c_j = 1, d_j = 0 \\ |O\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle & \cdots \text{ if } c_j = 0, d_j = 1 \\ |P\rangle = -\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle & \cdots \text{ if } c_j = 1, d_j = 1 \\ |Q\rangle = -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle & \cdots \text{ if } c_j = 0, d_j = 2 \\ |R\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle & \cdots \text{ if } c_j = 1, d_j = 2 \end{cases}$$

Bob_j sends $|\phi_{d_j}^{c_j}\rangle$ to $Alice_1$

2. Quatnum operation

$Alice_i$ creates $a_{i,j} \in \mathbb{Z}_2$ and $b_{i,j} \in \mathbb{Z}_3$

And applies the quantum operation $U_{b_{i,j}} V_{a_{i,j}}$ to j -th qubit

$$\begin{cases} V_0 = |0\rangle\langle 0| + |1\rangle\langle 1| \\ V_1 = |0\rangle\langle 1| - |1\rangle\langle 0| \end{cases} \quad \begin{cases} U_0 = |0\rangle\langle 0| + |1\rangle\langle 1| \\ U_1 = \left(\frac{-|0\rangle + \sqrt{3}|1\rangle}{2}\right)\langle 0| + \left(\frac{-\sqrt{3}|0\rangle - |1\rangle}{2}\right)\langle 1| \\ U_2 = \left(\frac{-|0\rangle - \sqrt{3}|1\rangle}{2}\right)\langle 0| + \left(\frac{\sqrt{3}|0\rangle - |1\rangle}{2}\right)\langle 1| \end{cases}$$

3. Measurement

$Alice_m$ sends j -th qubit to Bob_j and opens B_i

Bob_j measure the quantum state.

Measurement basis

$$\begin{cases} d_j + \sum_i b_{i,j} \equiv 0 \pmod 3 \Rightarrow \{|0\rangle, |1\rangle\} \\ d_j + \sum_i b_{i,j} \equiv 1 \pmod 3 \Rightarrow \{|O\rangle, |P\rangle\} \\ d_j + \sum_i b_{i,j} \equiv 2 \pmod 3 \Rightarrow \{|Q\rangle, |R\rangle\} \end{cases}$$

Measurement result e_j $\Downarrow$ 0 $\Downarrow$ 1

4. Decision of each share

share of Bob_j (s_{Bob_j}) $c_j \oplus e_j$

share of $Alice_i$ (s_{Alice_i}) $\oplus_j a_{i,j}$

5. Reconstruction of secret

$$S = \oplus_i s_{Alice_i} \equiv \oplus_j s_{Bob_j}$$

Fig.4 Quantum secret sharing between multiparty and multiparty

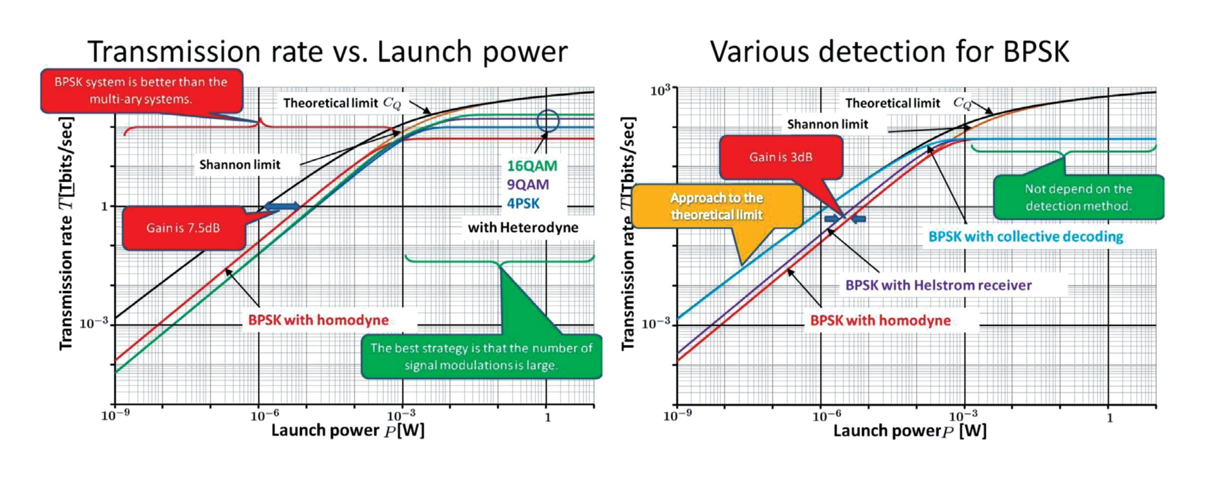


Fig.5 Transmission rate of quantum channels using an optical fiber

2.4 Evaluation of channel capacity regarding quantum communication channels in terms of space communications[11]

The conditions in the previous section were applied to space communications and calculations were performed. The diameters of the transmitting antenna and receiving antenna were set as 305 mm and 10,000 mm respectively, and the same items as those in the previous section were compared. That is, comparison with the theoretical upper limit given by Giovannetti et al. was performed for each of the following cases; with two modulation methods phase shift keying (PSK) and quadrature amplitude modulation (QAM), Holevo information was used that gives the maximum quantity of information obtained through homodyne detection, heterodyne detection, square root detection (SRD), and quantum measurement (Fig. 6). The result shows that, with respect to communications to Mars, theoretically 10 Gbits/sec can be achieved when 1 W is used for signal generation, with these antennas. The result has also allowed the author's group to confirm that the maximum communication channel capacity results when the BPSK modulation method is used for long distances or small input power and homodyne detection is performed, and when modulation with more values is performed for short distances or large input power and heterodyne detection is performed.

2.5 Security evaluation of the quantum secret modulation method[12]

The author's group examined the safety of the quantum secret modulation method represented by Y-00. This method has been treated as one type of stream cipher, and its safety has been evaluated from that viewpoint. The results of the evaluations have lead to the conclusion that the safety is equivalent to that of stream ciphers of modern cryptography. For

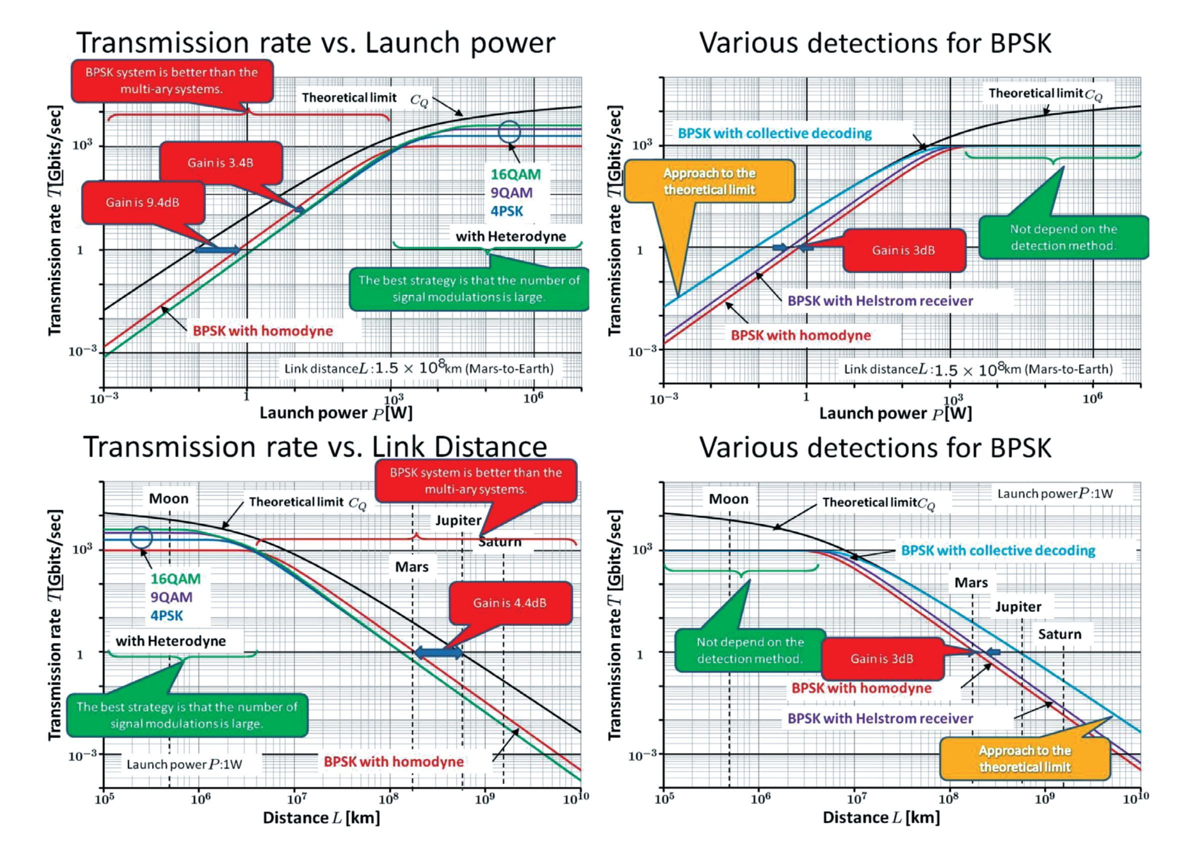


Fig.6 *Transmission rate for deep-space links*

this article, the quantum secret modulation method is treated as a type of cryptography use mode assuming quantum communications, not a type of stream cipher. The use of an ideally safe pseudo-random generator is assumed, and the structural safety was evaluated under the condition that attacks other than exhaustive search are not possible.

2.6 Multiparty simultaneous quantum authentication method[13]

While quantum cryptography has been suggested as a method which satisfies unconditional safety, it has a disadvantage that communication distances are largely restricted. Therefore, communications over long distances need key sharing via several nodes. At present, nodes which are used for this communication are considered as reliable, but in principle, such reliability is not ideal. To deal with the problem, the multiuser quantum authentication method authenticates multiple nodes at a time using quantum states, in terms of communication channels which pass through multiple nodes (Fig. 7). As for this research, the author's group has improved quantum states and quantum conversion which are not safe in terms of the conventional methods and has suggested a method superior to the conventional methods.

3 Conclusion

This article outlines the Security Fundamentals Group's research accomplishments and events regarding quantum cryptography, in terms of the second medium-term plan. As aforementioned, the Group's research about quantum security has been conducted with the Quantum ICT Group and the Space Communications Group. In the third medium-term plan, it is expected that close relationships with other many research institutions are established through joint projects and others, and more research accomplishments are achieved through further synergistic effects.

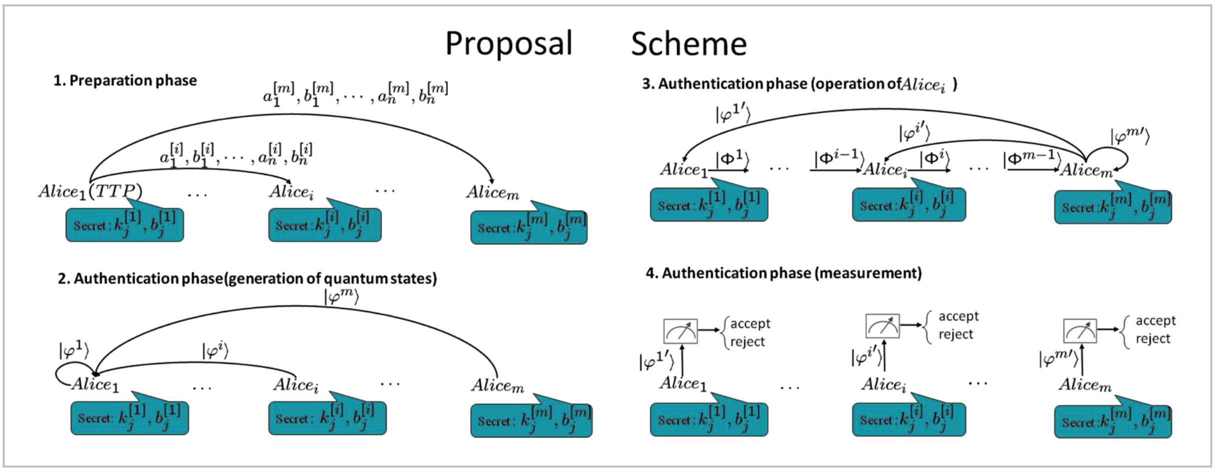

Proposal Scheme
1. Preparation phase
$a_1^{[m]}, b_1^{[m]}, \cdots, a_n^{[m]}, b_n^{[m]}$
$a_1^{[i]}, b_1^{[i]}, \cdots, a_n^{[i]}, b_n^{[i]}$
$Alice_1(TTP)$ … $Alice_i$ … $Alice_m$
Secret : $k_j^{[1]}, b_j^{[1]}$
Secret : $k_j^{[i]}, b_j^{[i]}$
Secret : $k_j^{[m]}, b_j^{[m]}$
2. Authentication phase(generation of quantum states)
$|\varphi^m\rangle$
$|\varphi^1\rangle$
$|\varphi^i\rangle$
$Alice_1$ … $Alice_i$ … $Alice_m$
3. Authentication phase (operation of $Alice_i$)
$|\varphi^{1'}\rangle$
$|\varphi^{i'}\rangle$
$|\varphi^{m'}\rangle$
$|\Phi^1\rangle$ $|\Phi^{i-1}\rangle$ $|\Phi^i\rangle$ $|\Phi^{m-1}\rangle$
4. Authentication phase (measurement)
accept
reject

Fig.7 *Multiparty simultaneous quantum identity authentication*

References

1 http://www.nict.go.jp/publication/NICT-News/0607/research/index.html

2 Douglas R. Stinson, "Cryptography: Theory and Practice, Third Edition," Chapman and Hall/CRC, 2005.

3 http://www.secoqc.net/

4 http://www2.nict.go.jp/pub/whatsnew/press/h22/101014/101014.html

5 http://www.uqcc2010.org/about/index.html

6 Atsushi Waseda, Masakazu Soshi, and Atsuko Miyaji, “Consideration for Quantum Multi-secret Sharing,” IPSJ Journal, Vol. 48, No. 7, pp. 2447–2464, 2007.

7 Atsushi Waseda, Takayuki Takagi, Masakazu Soshi, and Atsuko Miyaji, “Consideration for Quantum Secret Sharing between Multiparty and Multiparty,” The 2008 Symposium on Cryptography and Information Security, 2008.

8 Atsushi Waseda, Masahiro Takeoka, Masahide Sasaki, Mikio Fujiwara, and Hidema Tanaka, “Consideration of channel capacity of coherent light communication in optical fiber band,” The 2009 Symposium on Cryptography and Information Security, 2009.

9 Atsushi Waseda, Takayuki Takagi, Masakazu Soshi, and Atsuko Miyaji, “Quantum Secret Sharing between Multiparty and Multiparty against the Attack with Single Photons or EPR-pair,” The 2008 International Symposium on Information Theory and its Applications, Proceedings of ISITA 2008, 2008.

10 Atsushi Waseda, Masahiro Takeoka, Masahide Sasaki, Mikio Fujiwara, and Hidema Tanaka, “Quantum detection of wavelength division multiplexing optical coherent signals,” Journal of the Optical Society of America B-OPTICAL PHYSICS, Vol. 27, No. 2, pp. 259–265, 2010.

11 Atsushi Waseda, Masahide Sasaki, Masahiro Takeoka, Mikio Fujiwara, Morio Toyoshima, and Hidema Tanaka, “Quantum detection of wavelength division multiplexing optical coherent signals in lossy channels,” 2010 International Conference on Availability and Security, Proceedings of ARES 2010, 2010.

12 Hidema Tanaka, Masahide Sasaki, Masahiro Takeoka, Mikio Fujiwara, and Atsushi Waseda, “A study on a security evaluation of quantum secret modulation,” The 2010 Symposium on Cryptography and Information Security, 2010.

13 Atsushi Waseda, “Consideration for multiparty simultaneous quantum identity authentication,” The 2011 Symposium on Cryptography and Information Security, 2011.

(Accepted June 15, 2011)

WASEDA Atsushi, *Ph.D.*

Expert Researcher, Security Fundamentals Laboratory, Network Security Research Institute

Quantum Security