7-8 Information Theoretic Secure Cryptosystems

Atsushi WASEDA and Ryo NOJIMA

Information theoretically secure schemes are remarkable techniques because its security level doesn’t decrease even if the computational power increases. This paper describes our research, especially “multiparty simultaneous quantum identity authentication schemes” and “password protected secret sharing schemes”, which were studied in the Security Fundamentals Laboratory during the last 5 years.

1. Introduction

Many modern cryptographic technologies have computational security as the basis for security, which means it is difficult to attack even with the use of computers. However, although a cryptographic system is based on problems that were once considered secure, its security can be threatened by advancements in computer performance, evolution of parallel processing, and more advanced solution methods. These problems are being dealt with by building new cryptographic systems, and by increasing the scale of problems that form the basis of security. However, it is impossible to ignore the fact that with the giant growth in the scale of problems, there is also a rise in the computational cost and the memory cost for ensuring security. Also, system updates due to replacement of cryptographic technologies not only adversely affects service continuity or business continuity planning (BCP), but there are also large concerns about decrease in security due to parallel operation of new and old systems, the necessity of maintaining compatibility with old data, etc. One way to deal with this problem is the existence of methods that ensure security in information theory. The method to ensure security by information theory not only has efficient computer performance and parallelism, but it also has an advantage that it is possible to build a security protocol not threatened by the introduction of new types of computers such as quantum computers. Typical examples of security protocols which are secure because of such information theory include the quantum security protocol[2][3], which uses the quantum state as represented by the quantum key distribution[1], and secret sharing[4] wherein the secret information can be distributed into multiple distributed information, stored and then the secret information can be reconstructed only by combining the specific distributed information together, thus preventing the secret information leaking under any other conditions.

The Security Fundamentals Laboratory has conducted research and development on security technologies based on such information theory. Specifically, we have proposed simultaneous quantum identity authentication[5] which is an authentication system of using quantum states, and password protected secret sharing[6] that is secret sharing with special functions, which authenticates whether the user has the right to reconstruct the secret information based on his/her possession of the password. Moreover, in order to carry out this research, we have asked for cooperation from researchers within and outside Japan, resulting in some achievements. Within NICT, we have collaborated with the Quantum ICT Laboratory, the Nano ICT Laboratory, and the Space Communication Systems Laboratory (names of each laboratory are as of the date of research) under a project led by Mikio Fujiwara, senior researcher of the Quantum ICT Laboratory. In the field of

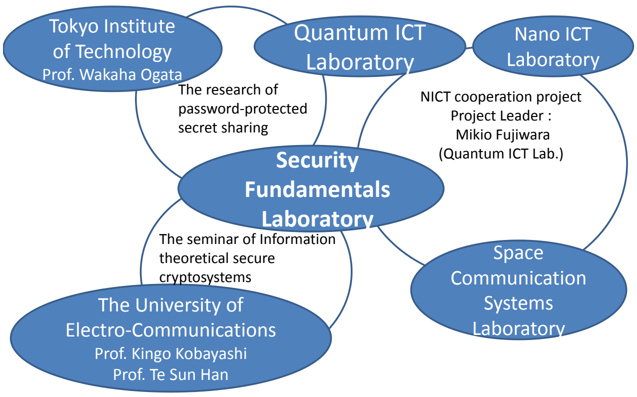
Tokyo Institute of Technology
Prof. Wakaha Ogata
Quantum ICT Laboratory
Nano ICT Laboratory
The research of password-protected secret sharing
NICT cooperation project
Project Leader :
Mikio Fujiwara
(Quantum ICT Lab.)
Security Fundamentals Laboratory
The seminar of Information theoretical secure cryptosystems
Space Communication Systems Laboratory
The University of Electro-Communications
Prof. Kingo Kobayashi
Prof. Te Sun Han

Fig. 1 Partnership with researchers within and outside the Security Fundamentals Laboratory for this research (Names are as of the date of research)

password protected secret sharing, with Professor Wakaha Ogata of the Tokyo Institute of Technology, in the field of theoretical aspect; and with the Quantum ICT Laboratory for implementation. We also received guidance on theoretical aspects of information theory and suggestions for application of information theory techniques to security protocols, from Kingo Kobayashi and Te Sun Han, Professors Emeritus of the University of Electro-Communications (Fig. 1).

This research paper outlines the accomplishments for the security technique which is also based on the information theory security, at the Security Fundamentals Laboratory, followed by a conclusion.

2 Research overview

2.1 Simultaneous quantum identity authentication

2.1.1 Overview

This system is an authentication protocol that uses quantum states. A usual authentication protocol is executed between two users, wherein either one user authenticates the other, or both users authenticate each other, regarding whether the other party is a legitimate user or equipment. However, considering usual communications, in reality many equipment (nodes) intervene between the sender and recipient. In such a communication route that passes through several nodes, it is this simultaneous quantum identity authentication that attempts to authenticate each node at a time by using quantum state. In this research, we show that the existing system proposed by Yang et al.[3] discloses the user's authentication key by an attack using the quantum entangled state, and we propose a scheme for security against this attack. This result was presented in IEICE Transactions[5].

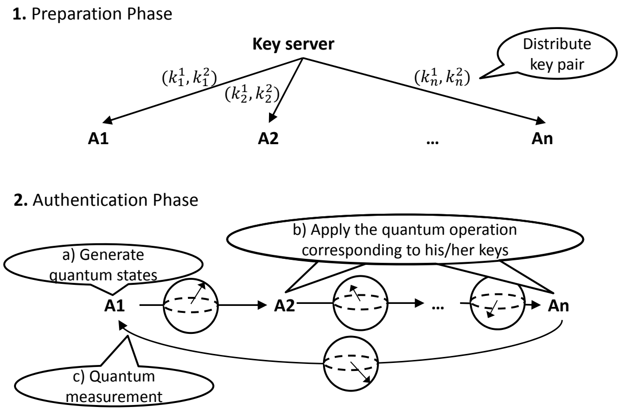

Fig. 2 Schematic view of simultaneous quantum identity authentication

2.1.2 Overview and evaluation of proposed protocol

The proposed protocol is a system that is executed for n users A_1, A_2, … A_n, wherein user A_1 authenticates the other users (Fig. 2). This protocol is comprised of a preparation phase and authentication phase. In the preparation phase, a trusted key distribution center generates keys for all the users and distributes them. In the authentication phase, first, user A_1 creates the quantum state, next each user A_i applies a quantum operation according to the key to the quantum state sent from A_{i-1} , and in the end, user A_1 performs measurement and accepts another user's authentication when the correct quantum state could be measured. By devising the quantum state and the quantum operation to be used, we have proved that the proposed protocol has high resistance to both (a) the intercept-resend attack, wherein information is obtained by intercepting the state during the communication and measuring it, and then resending the state, and (b) the fake signal attack with entangled state, wherein information is obtained by sending the quantum entangled state for attack, and measuring it after performing the quantum operation. Especially, the fake signal attack with entangled state can expose the user key with great reliability, when it is applied to the system proposed by Yang et al. The pair of the quantum state and the quantum operation, which is being used in the system proposed by Yang et al., used a basis transformation using the Hadamard gate, therefore the problems raised for security protocols using this and the proposed protocol that carried out its countermeasure can be said to be especially significant.

2.2 Password protected secret sharing

2.2.1 Overview

This system is a protocol that combines a password authentication scheme with secret sharing (Fig. 3). In the secret sharing scheme, the secret information is encoded into the distributed information, which is stored in multiple servers. The distributed encoded information is called shares. if specified multiple shares are collected, the original secret can be reconstructed. Otherwise, the secret related information does not get leaked at all with information theory. The most famous secret sharing scheme is the scheme proposed by Shamir[4]. In Shamir's scheme, the secret information is split into *n* shares, and the secret information can be reconstructed by collecting any *t* shares, which is also called (*t, n*) threshold secret sharing. But the secret sharing schemes have several problems, such as, how to distribute the shares to each server without leaking them

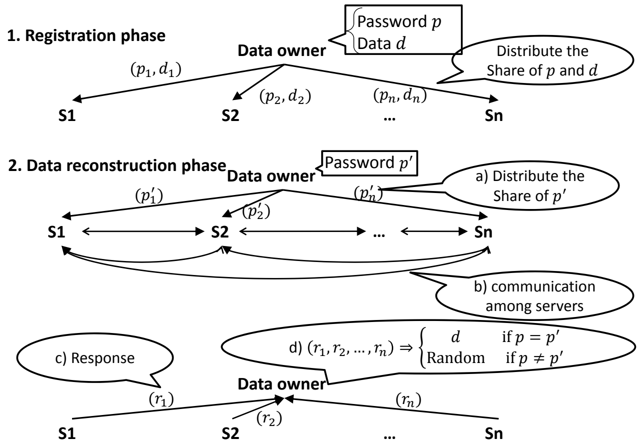
1. Registration phase
Password p
Data d
Data owner
Distribute the Share of p and d
(p_1, d_1)
(p_2, d_2)
(p_n, d_n)
S1
S2
…
Sn
2. Data reconstruction phase
Data owner
Password p'
a) Distribute the Share of p'
(p'_1)
(p'_2)
(p'_n)
S1
S2
…
Sn
b) communication among servers
c) Response
d) $(r_1, r_2, \dots, r_n) \Rightarrow \begin{cases} d & \text{if } p = p' \\ \text{Random} & \text{if } p \neq p' \end{cases}$
Data owner
(r_1)
(r_2)
(r_n)
S1
S2
…
Sn

Fig. 3 Schematic view of password protected secret sharing

to the attacker, and how each server will give permission to reconstruct the secret. In this research, we have focused on the second problem, which is how each server will give permission to reconstruct the secret, and we have proposed password protected secret sharing, a scheme in which only those who know the correct password can reconstruct the correct secret. A similar technique has been proposed by Bagherzandi et al.[7] and Camenish et al.[8]. These schemes use homomorphic encryption. Then, the overall security level of these schemes drops from information theoretic security to computational security.

The password protected secret sharing proposed in this research is the first that maintains information theoretic security. For conducting this research, we collaborated with Professor Wakaha Ogata of the Tokyo Institute of Technology, and gave a presentation at the 31st Symposium on Cryptography and Information Security (SCIS 2014)[6]. Moreover, the first problem of secret sharing was how the shares can be stored in each server in a secure manner. We are working towards implementation by collaborating with the Quantum ICT Laboratory in order to achieve it using quantum cryptography, which also achieves unconditional security.

2.2.2 Overview and evaluation of proposed protocol

The user holds secret information $d \in \mathrm{D}$ and password $p \in \mathrm{P}$, and these are stored in n servers as shares. The user restores the secret information by using shares that are stored in any k servers, with password $p' \in \mathrm{P}$ as the input. The proposed protocol is comprised of *registration phase* and *data reconstruction phase*. In the registration phase, the secret information d and password p are saved by using Shamir's secret sharing, and in the data reconstruction phase, the user sends the shares of password p' to the server, each server combines the shares of stored secret information and the shares of password, and creates information for reconstructing, and sends it back to the user. The user restores the secret information by using the information that is sent back. If $p' = p$, the correct secret can be restored, but if $p' \neq p$, a random number is restored, and it is thus not possible to obtain the secret information. This system helps prevent restoring the secret information by a user who is not originally authorized to do so. This result is a beginning toward achieving creation of a secure storage system, which can be said to be of great significance.

3 Conclusion

As research done on security techniques based on the information theoretic security that has been carried out by the Security Fundamentals Laboratory, we have introduced a simultaneous quantum identity authentication as well as password protected secret sharing, which is a combination of a password authentication system and secret sharing. The information theory is an important concept which is not just limited to security. We at the Security Fundamentals Laboratory will continue conducting research in the future not just on developing security protocols, but also on analysis based on information theory for privacy protection protocols.

References

1 C.H.Bennett and G. Brassard, "Quantum cryptography: Publickey distribution and coin tossing," Proc.IEEE International Conference on Computer, Systems and Signal Processingp. 175, IEEE Press, Bangalore, lndia, New York, 1984.

2 M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A, vol.159, no.3, pp.1829–1834, 1999.

3 Y. Yang, Q. Wen and X. Zhang, "Multi-party simultaneous quantum identity authentication with secret sharing," Science in China Series G: Physics Mechanics and Astronomy, 51, pp.321–327. 2008.

4 A. Shamir, "How to Share a Secret," Communications of the ACM, vol.22, no.11, pp.612–613, 1979.

5 A. Waseda, "Multiparty simultaneous quantum identity authentication secure against fake signal attacks," IEICE TRANS. on Fundamentals of Electronics, Communications and Computer Sciences, vol.E96-A, no.1, pp.166–170, 2013.

6 A. Waseda, W. Ogata, R. Nojima, S.Moriai, "Password-protected secret sharingwith IT condentiality against active adversaryActive," The 31st Symposium on Cryptography and Information Security, 2014 (in Japanese).

7 A. Bagherzandi, S. Jarecki, N. Saxena, Y. Lu, "Password-protected secret sharing," In Proceedings of the 18th ACM conference on Computer and communications security, pp.433–444, 2011.

8 J. Camenisch, A. Lysyanskaya, and G. Neven, "Practical yet universally composable two-server password-authenticated secret sharing," In Proceedings of the 19th ACM conference on Computer and communications security, pp.525–536, 2012.

Atsushi WASEDA, Ph.D.

Senior Researcher, Security Fundamentals
Laboratory, Cybersecurity Research Institute
Information Security

Ryo NOJIMA, Ph.D.

Senior Researcher, Security Fundamentals
Laboratory, Cybersecurity Research Institute
Cryptography, Cryptographic Protocol