2-3 Overview of R&D Activities of Security Fundamental Technologies

Shiho MORIAI

This paper introduces the overview of the R&D activities and achievements on security fundamental technologies during the 3rd Medium- to Long-Term Plan (from FY2011 to FY2015).

1 Introduction

A variety of security fundamental technologies have been applied for the purpose of preserving security in the use or construction of information-communication networks—the most well-known and frequently used technology is the cryptographic technologies. The modern cryptographic technologies, for which the base was established in 70s, were widely used in 90s; and since the 2000s, when its standardization was promoted, the cryptographic technology has been in the middle of its market-maturity stage. However, advanced cryptographic technologies and cryptanalysis techniques emerge everyday one after another. In addition, how to introduce cryptographic technologies into the field of automobile or IoT—where application of cryptographic technologies has been slow—has become the new challenge. Therefore, we at NICT, as the national research institute, regard it as one of our important missions to conduct the security evaluation of cryptographic technologies and promote the research and development of security fundamental technologies for the purpose of keeping information and communication networks in the state where people can use the networks without concern regarding their security.

Security Fundamentals Laboratory, aiming to attain the world-leading achievements and propose the cryptographic technologies guidelines that ensure the safe utilization of e-Government systems, has promoted its activities during the 3rd Medium- to Long-Term Plan (from 2011 to 2015).

In this article, we introduce the overviews of the following four targets of the research activities conducted in Security Fundamentals Laboratory which were accomplished in the 3rd term plan.

- **Quantum security (information-theoretic security) technologies**

  Research and development for constructing the networks where the security is information-theoretically ensured, through integrating quantum technologies and modern cryptographic technologies.
- **Long-term cryptography**

  Research and development of the long-term cryptography that ensure strong security for a long time even for the quantum computers that are expected to be realized in future.
- **Practical security technologies**

  Research and development of the technologies that provide the practical-use-level security that matches the individual security requirements in different environments.
- **Advanced security evaluation of cryptographic technologies**

  Research and development of the cryptography-security evaluation technologies that will contribute to the revision of the e-Government recommended ciphers list and to the future-migration of the cryptographic technologies that will occur in future. Also, the secretariat of the CRYPTREC Project, where the monitoring and evaluation of e-Government recommended ciphers takes place.

2 Overview of the research and development activities

2.1 Quantum-security (information-theoretic security) technologies

For the purpose of contributing to the construction of more flexible and versatile quantum-security networks, we conducted the research and development through integrating quantum technologies and modern cryptographic technologies—quantum technologies, while enabling the realization of information theoretically secure secret com-

munications, are unable, by themselves, to realize even the basic authentication functions with information theoretic security, such as user authentication. Therefore, by integrating quantum methods with the cryptographic technology called the secret sharing, we proposed an information theoretically secure user-authentication that uses a single password. In the scheme, data can be distributed and saved in a number of servers on clouds, and a user who is not issued a password, even if in collusion with multiple server managers, is not allowed to access the data because the scheme will prevent the user from stealing the secret data when the number of the server managers in such a collusion is below the predefined threshold value; and so the privacy is protected. The scheme is an information-theoretically secure password protected secret sharing protocol. We co-developed the protocol with Tokyo Institute of Technology (Fig. 1). Furthermore, we implemented the password protected secret sharing protocol on a quantum network. The system, developed in the "research and development of secure networks using quantum key distribution" project, a joint project with the Quantum ICT Laboratory in NICT and others, was the world first implementation of an information-theoretically secure system for both confidentiality and authentication. The achievement we made received such high evaluations that it was published in the Scientific Reports, an e-journal of the Nature Publishing Group in 2016. ISO/IEC JTC 1/SC 27 is currently working on the international standardization of technologies for secret sharing in which we are going to promote the international standardization of our password protected secret sharing protocol.

2.2 Long-term cryptography

Regarding the long-term cryptography that ensure strong and long-term security, we conducted our research efforts focusing on the lattice theory that has been regarded as promising; promoting research particularly focusing on how to design a new method based on the lattice theory and the security evaluation technologies of the new method we were developing. As for the design of the lattice-based cryptography, we developed: first in the world, the homomorphic encryption that enables updating the security level and also enables the operations of addition and multiplication while encrypted. The encryption method we developed ensures the statistical analysis over encrypted data—for example, gene information, for which a long range security of more than 100 years is required. It suggests that our method is applicable to data-mining while protecting the privacy information included in the encrypted data. We successfully conducted the simulations by applying linear-regression operations to encrypted big-data, to confirm that our method can perform calculations at a rate 100 times faster than the conventional methods. In addition, we created a logistic regression analysis method (Fig. 2) that can complete its processing within a practical time-period; we confirmed by simulations that the 100-million pieces of encrypted data were clustered within 30 minutes into two groups. At the same time, we have acquired a series of intellectual rights for the method.

Regarding the evaluation of lattice-based cryptography, we completed the speeding-up of our algorithm to evaluate the difficulty of the lattice shortest vector problem —such difficulty induces the security of lattice-based cryptography. Our algorithm was presented in the Eurocrypt 2016, one of the cryptography top conferences; and furthermore, we made, by applying the algorithm, several worlds records at the "Lattice Challenge" (Fig. 3), a security evaluation contest by Technical University Darmstadt. We conducted the research by joint works with the outside research-institutes including Kyushu University, INRIA France, Tokyo

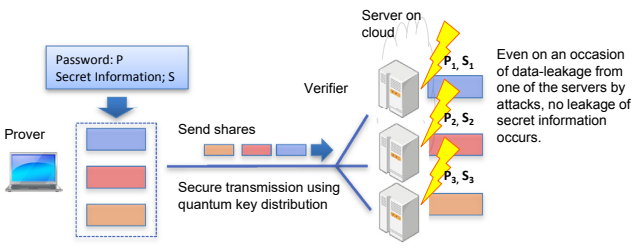

Fig. 1 Password protected secret sharing protocol

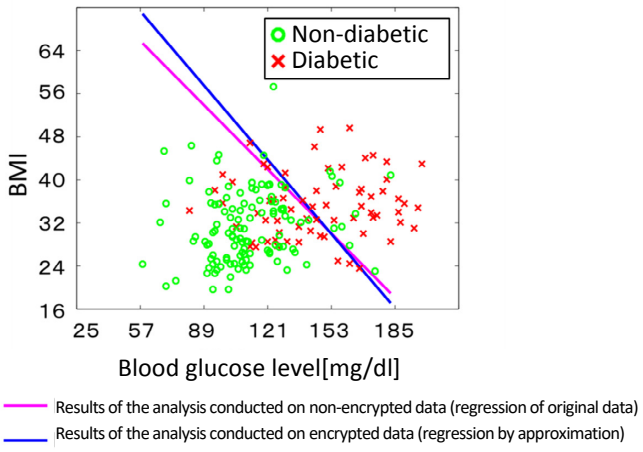

Fig. 2 Clustering encrypted big-data (by logistics regression analysis)

University, and the Bank of Japan.

2.3 Practical security technologies

For the subject, we developed a variety of research and developments as shown below aiming for providing practical security features matching the characteristics of the individual varied network-use environments.

- **Lightweight cryptography for CPS/IoT**

We, aiming for the preservation of the security of such systems that are used for the cloud-based analysis of the big-data that consists of data-pieces collected from a variety of sensors, conducted the performance evaluations of lightweight cryptography; testing their advantages over conventional cryptographic method. In addition, for the purpose of utilizing lightweight cryptographic technologies for the security-improvement of the systems that are continuously connected to the Internet such as "Connected Cars," Intelligent Transport Systems (ITS), or IoT systems, we created a prototype model of the lightweight security protocol for a tire-pressure-monitoring system. Furthermore, we made contributions, as an editor, to the development of the International Standard, ISO/IEC 29192-1, 29192-2, and 29192-4.

Fig. 3 Security-evaluation of lattice-based cryptography (TU darmstadt lattice challenge) https://www.latticechallenge.org/

- **PRINCESS (encrypted file sharing system) and its application to car-sharing systems**

We proposed "PRINCESS (Proxy Re-encryption with INd-Cca security in Encrypted file Storage System)," which is the encrypted-file sharing system that enables the designation of the file-sharing counter-partners at a confidentiality-level matching the file's confidentiality-

Fig. 4 Encrypted file sharing system: PRINCESS

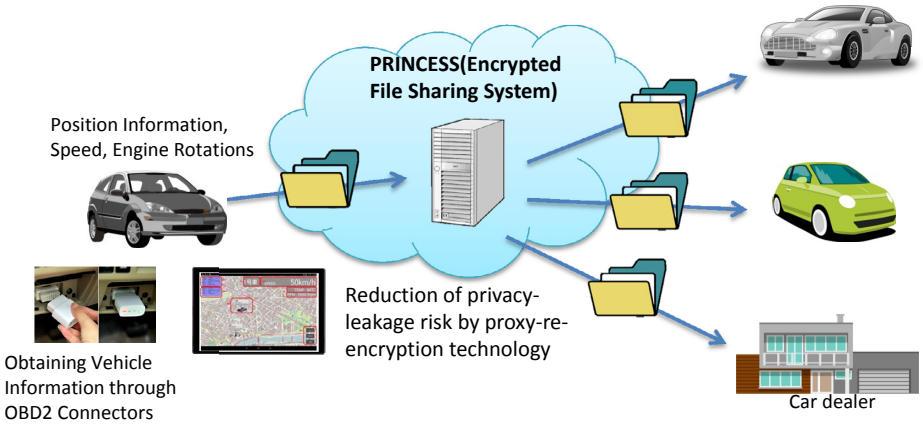

Fig. 5 Application of PRINCESS to vehicle-information sharing system

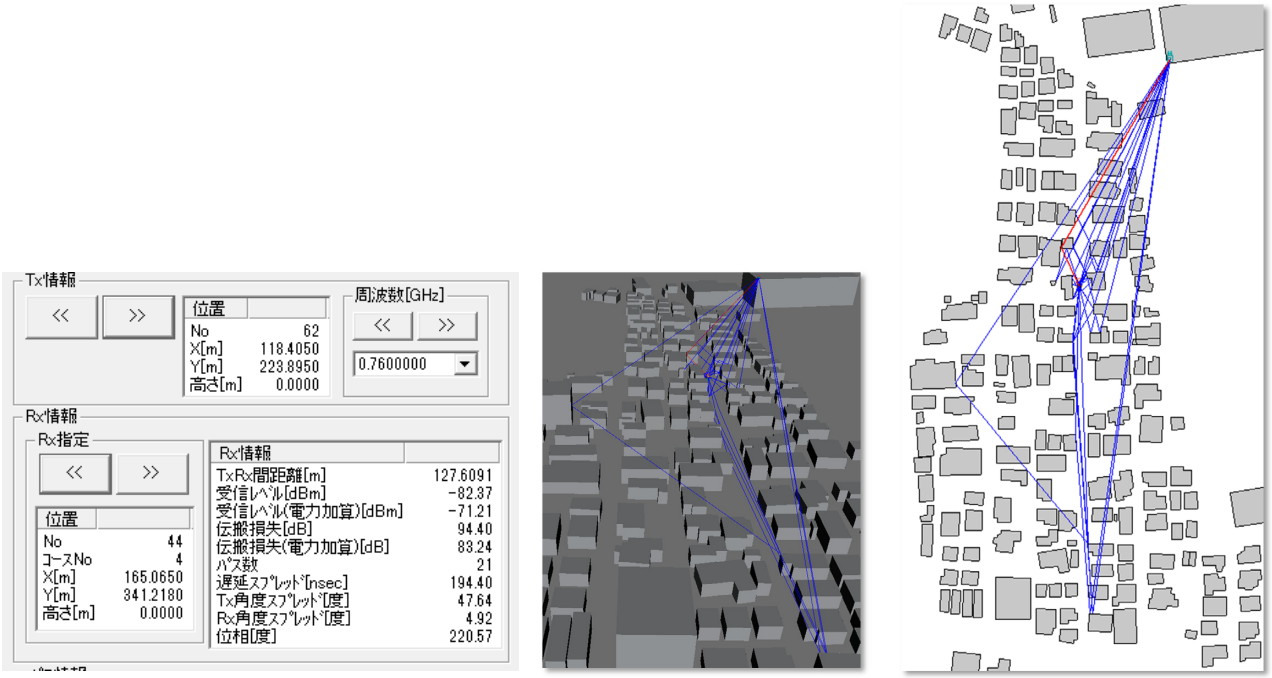

Fig. 6 Privacy-leakage analysis by using wave-propagation simulation

level by using ID-based cryptography achieving two functions (proxy-encryption and proxy-decryption); and we acquired the intellectual rights for the system: in addition, we developed a prototype of the system (Fig. 4).

Furthermore, we developed a prototype of the secured vehicle-information sharing system, by applying the above-mentioned technology, in order to cope with the situation where the security / privacy preservation of vehicle big-data becomes an urgent issue for the realization of the intelligent transportation system or the services through the system—there, its big-data consists of data including information coming from a variety of vehicle-mounted sensors, and vehicle position information (Fig. 6)

- **Analysis of privacy-leakage in vehicle to X (V2X) communications**

We conducted analyses using wave-propagation simulations, for the purpose of making assessments on the leakage-risks of privacy-information such as vehicle-identifiable information from the 700 MHz V2X communication system or the 315 MHz-band tire-pressure sensor systems—they are under proof-of-concept experiments by the MIC (Fig. 5).

- **Proposal of FACE (a practical key encapsulation mechanism, KEM), and its international-standardization**

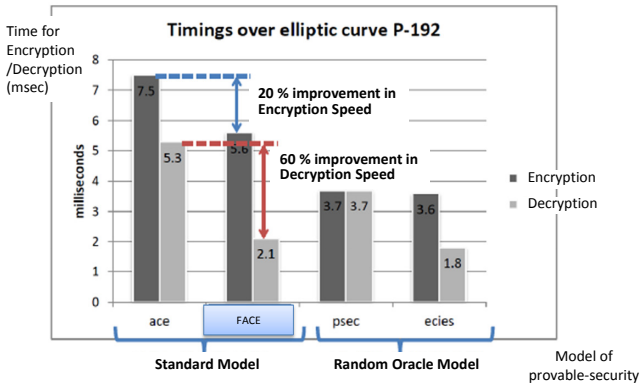

Fig. 7 Comparison of FACE to other ISO/IEC 18033-2 schemes

We developed a new key encapsulation mechanism, "FACE," (Fig. 7) that ensures more secure and more efficient processing than that by the schemes employed in ISO/IEC 18033-2; starting the activities for its international standardization at ISO/IEC JTC 1/SC 27. At the meeting in October 2015, the addition of our scheme to ISO/IEC 18033-2 was approved by its member countries, and at present, the standardization is on-going.

- **Starting-up of the Privacy-Study WG and participation to PWS CUP administration**

We started-up the research aiming for solving the privacy-issues expected to rise with the use of personal

data. We collected experiences and knowledge from the experts in a variety of fields through holding workshops, and, while at the same time placing efforts on collecting cases, we expanded the workshop to establish the Privacy-Study WG. In such a way, we made an arrangement of collaboration toward the 4th Medium- to Long-Term Plan. In addition, we started the construction of the poll-survey system for investigating what users think about their privacy-information and its protection. Also, we made contributions to PWS CUP (a contest of anonymization techniques or re-recognition techniques of anonymized data) sponsored by the Information Processing Society and held at the Privacy Workshop (PWS).

2.4 Advanced security evaluation of cryptographic technologies

- **Security evaluation of discrete logarithm problem based public-key cryptography scheme (pairing-based cryptography)**

Regarding the advanced security evaluation of cryptographic technologies, we evaluated the difficulty of the discrete logarithm problem—the security of cryptography comes from the difficulty in solving the problem—for the purpose of evaluating the security of the "pairing-based cryptography" that enables the realization of the privacy-protection functions in cloud computing. Jointly with Kyushu University and Fujitsu Laboratories Ltd., we successfully solved the 923-bit discrete logarithm problem for the first time in the world. We presented our success at the international conference ASIACRYPT 2012, also we made a press release in June, 2012 (Fig. 8). Our achievement was praised as a pioneering achievement that opens a door to the realization of next-generation cryptographic technologies that enable the use of secret data, and we received the following awards; Excellence Award 2013, Advanced Technology, Docomo Mobile Science Prizes; Achievement Award 2012, Kiyasu Memorial Prize, Information Processing Society; Achievement Award 2014, The Institute of Electronic, Information and Communications Engineering. In addition, we conducted a survey on the progress of discrete logarithm problem solutions—researches on the problem started and proceeded triggered by our achievement; enhancing the results by adding our comments on what impacts will be on the e-Government recommended ciphers and published it as the Cryptography Research and Evaluation Committee (CRYPTREC) Report. In such a way, we contributed to the security / reliability improvement of e-Government systems.

- **Construction of XPIA, and contribution to the society**

We, based on the database collected by the SSL Observatory on the public-key certificates used by SSL servers on the Internet, developed a security-test tool, XPIA—X.509 certificate Public-key Investigation and Analysis system (Fig. 9)—to investigate the insecure situation where a secret key of RSA is recycled and used in a number of servers; we made a press-release in October 2013. We transferred the techniques used in XPIA to the Japan Information Processing Development Corporation (JIPDEC), Also we confirmed that the "Self-Signed Certificates" have no risks of exposure of secret-keys induced by the above mentioned vulnerability—the

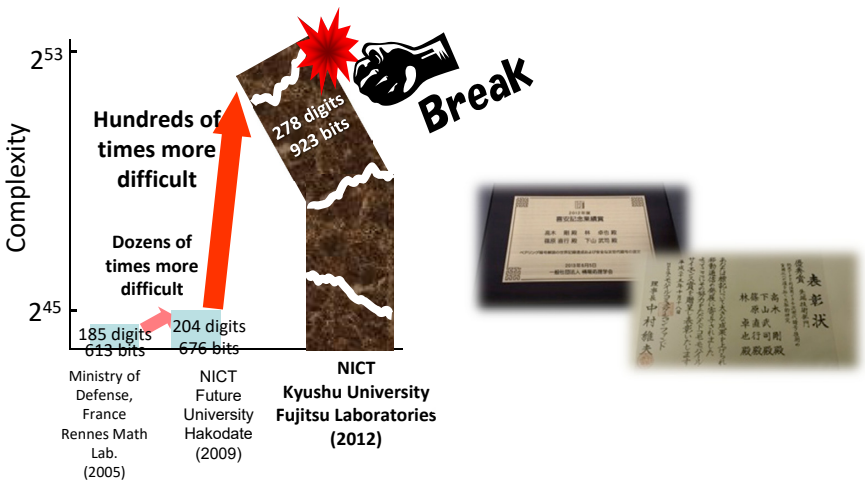

Fig. 8 Security evaluation of pairing-based cryptography

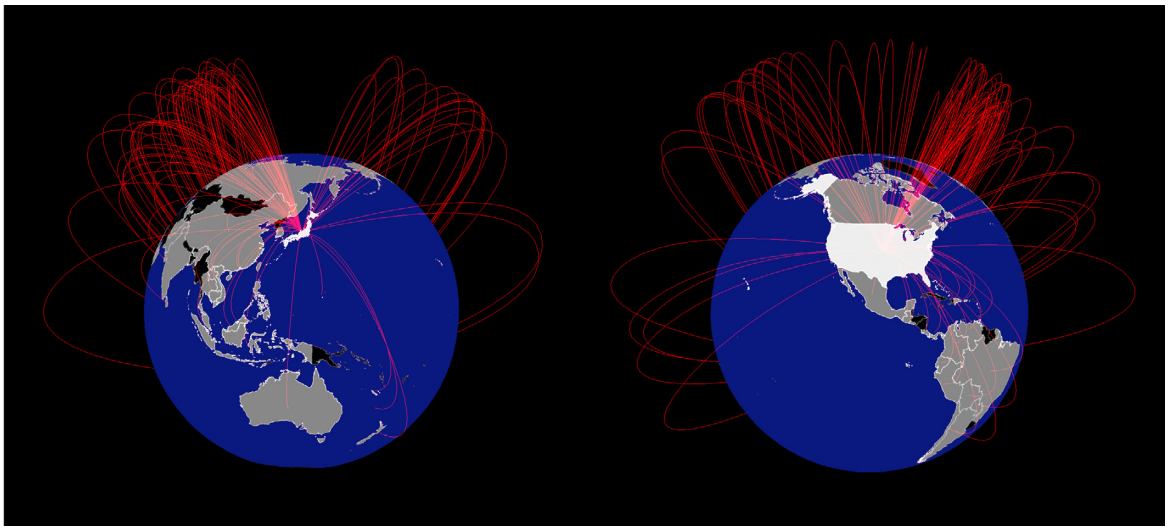

Fig. 9 An instance of vulnerability distribution display by "XPIA"
(The figures on the left and right hand sides show the views from Japan and the U.S., respectively.)
The red-line shows that the SSL-servers on both of its ends are sharing a prime number (used for a secret key) and they are in danger.

certificates have been used in the certification/authentication operations, of which the competent ministries for operation are the MIC, MOJ and METI, ministries that are supporting e-Bidding, e-Submission, and e-Contract which are run on the basis of e-signature/authentication. We made a press release on the above-mentioned confirmation in December, 2014.

- **Contributions in CRYPTREC to the revision of the e-Government recommended ciphers list**

  For over 15 years, NICT has been conducting, the activities to support the administration of CRYPTREC—it is a project established in 2001 to evaluate/monitor the security of the e-Government recommended ciphers list and conduct the survew2ys/studies on the proper implementation/operation methods of cryptographic technologies. In particular we conducted, for the first revision in 10 years of the e-Government recommended ciphers list, the security evaluations of the candidate cryptographic technologies—it was indispensable to the revision; and released the evaluation results for the purpose of providing the reference material for technical-evidence. In such a way, we made great technological/administrative contributions, in collaboration with the MIC, METI, and IPA, to the activities of CRYPTREC.

3 Conclusions

In this article, we introduced the overview of our major research subjects and their achievements that were conducted in Security fundamentals Laboratory during the years of the 3rd Medium- to Long-Term Plan. As for the details of those researches, we are going to introduce them in the sections of Chapter 7 "Security Fundamental Technologies." We have to express our appreciation to the research members engaged in so many researches which we were regretfully not allowed to have space to introduce in this article. For some of those research achievements, we fortunately had chances: not only to publish them in papers, but also to proceed to on-prototype test, technology-transfer, international standardization, or even to make social contributions. So, we are very happy to have completed our mission as a public research institute. We, presently, are formalizing our plan for the future where advanced social needs will emerge along with the expansion of IoT. We have a plan to research and develop the cryptographic technologies enabling new functions to satisfy such new needs for the purpose of making contributions to the promotion/standardization and also to the construction/management of the safe and secure ICT systems. In addition, through conducting research and development on privacy-enhancing technologies, we hope to provide technological supports for implementing proper privacy-measures.

Acknowledgment

We received great amount of support from many people since the second year of the 3rd Medium- to Long-Term Plan, when I took over the position of Director, Security Fundamentals Laboratory, from Dr. Hidema Tanaka (currently an associate professor at the National

Defense Academy). We express our appreciation particularly to Director General Dr. Kazumasa Taira and Vice President Dr. Makoto Imase for their helpful advice on laboratory management. Also, we appreciate the guidance for the smooth launch of our laboratory that former Director General Dr. Yukio Takahashi and the members of the Planning office gave me when I was appointed as a director. Regarding the administrative jobs of the laboratory, we thank the group assistants Shiori Takahashi and Tomoko Mineta for their great contributions; they supported the lab's activities and gave energy to all the laboratory members.

Shiho MORIAI, Ph.D.

Director of Security Fundamentals Laboratory, Cybersecurity Research Institute
Cryptography, Information Security