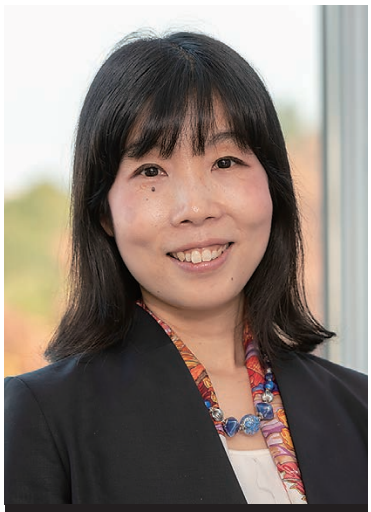
INTERVIEW

Toward Safe and Secure Data Utilization

The frontiers of cryptographic technologies



Shiho MORIAI
Director of Security Fundamentals Laboratory
Cybersecurity Research Institute

After graduating from Kyoto University, worked at NTT and Sony corporation. Entered NICT in 2012. Engaged in R&D in cryptography, information security, and privacy. Ph. D. (Engineering).

As the Internet has spread throughout modern society, cryptographic technologies have become indispensable. But now, in some sense, these technologies are facing a crisis. This is because research and development on quantum computers is advancing rapidly, and it may be easy for them to break public key cryptosystems that are currently used widely.

The National Institute of Standards and Technology (NIST) is now preparing for standardization of Post Quantum Cryptography (PQC) which will be resistant to attacks using quantum computers.

In this age of upheaval in information and communications technology, how will cryptographic technologies change, and how will they be implemented in society?

We spoke with Dr. Shiho MORIAI, Director of Security Fundamentals Laboratory of Cybersecurity Research Institute, which conducts fundamental research on ICT security based on cryptographic technologies.

The increasing importance of cryptographic technologies in the IoT era

—— Cryptography has a long history, but there's a feeling that in today's networked society it has become an indispensable technology. Can you tell us about any changes or other fundamental aspects of cryptographic technologies?

Moriai Cryptography has a long history, going back to the ancient Roman era in the first century B.C.E, when Julius Caesar used the well-known Caesar's cipher. It was quite simple, just shifting the letters of the alphabet by several places. Cryptography has gone through great changes since the development of networks such as the Internet.

As communication over networks has become common, there is an increasing amount of information being communicated that must not be disclosed to third parties, such as commercial transactions between enterprises, government procurement information, or diplomatic information. Cryptographic technology developed rapidly to ensure that information could be transmitted securely over networks.

Initially, the content of messages was kept secret by concealing the cryptographic algorithms used, but such systems could not be used among large numbers of unspecified people. Then, cryptosystems were developed that could maintain security even if the algorithm was made public, as long as a key used to decrypt the ciphertext was kept secret. In 1977, the National Bureau of Standards (NBS), which was the predecessor of NIST, established the Data Encryption Standard (DES) for the United States Government, and this became a global standard.

Since that time, networks began spreading rapidly, and research on cryptographic technologies has advanced. DES was replaced by the Advanced Encryption Standard (AES) later, both of which are symmetric-key cryptosystems. Around the time that DES was developed, public-key cryptosystems also made their appearance, and they have also revolutionized cryptography.

—— Could you tell us about public-key cryptography?

Moriai Cryptosystems use keys, which are strings of bits, to encrypt and decrypt messages. A symmetric-key cryptosystem uses the same key for both encryption and decryption. It is fast and convenient for communicating with a specific party, but the key to be used must be shared between both parties beforehand. Thus, the cost of sharing the key beforehand and the risk that the key could be leaked to a third party are issues with such systems.

In contrast, public-key cryptosystems generate a pair of keys, a public key and a private key. The public key can be made public. Messages to a particular party are encrypted using that party's public key and can then be decrypted using their private key. A public key cryptosystem can be used to share a key for a symmetric-key cryptosystem beforehand, which makes the symmetric-key cryptosystem much more secure (see Figure).

A typical public-key cryptosystem is RSA (Rivest-Shamir-Adleman), which is used in Transport Layer Security (TLS), the standard protocol for secure communication on the In-

INTERVIEW

Toward Safe and Secure Data Utilization

The frontiers of cryptographic technologies

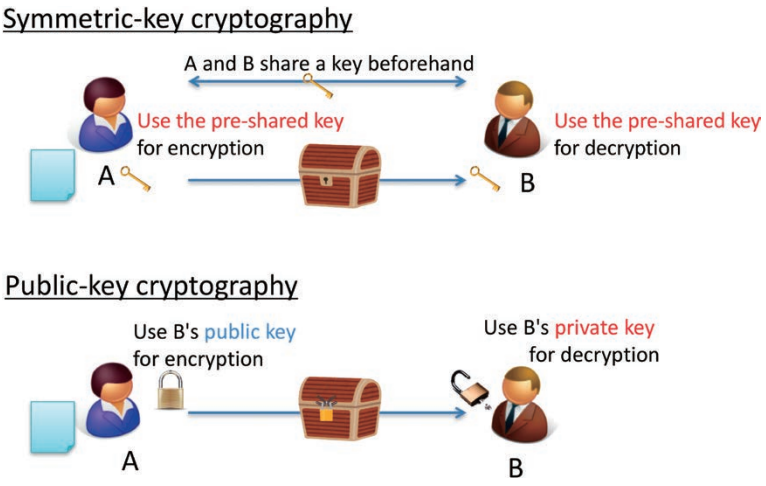


Figure Symmetric-key cryptography and public key cryptography

ternet.

—— How has cryptography changed with the Internet?

Moriai All kinds of information is exchanged over the Internet, so cryptographic technologies have advanced in order to protect this information: private information exchanged by e-mail, confidential financial information such as e-money and credit card data. Cryptographic technology is indispensable for protecting such information.

In the future, IoT will continue to spread, with all kinds of objects connecting to the Internet. This means that all of these items could also become the targets of cyberattacks, so cryptographic technology will become even more important.

Three R&D priorities

—— Can you tell us about NICT's initiatives in cryptographic technology?

Moriai NICT establishes a Medium- to Long-term Plan every five years, and this fiscal year is the third year of our Fourth Medium- to Long-term Plan (2016-2020). Our laboratory is working on three R&D initiatives in cryptographic technology from the Medium- to Long-term Plan, which are: Functional Cryptographic Technologies, Security Evaluation of Cryptographic Technologies, and Privacy Enhancing Technologies.

—— Could you tell us about "Functional Cryptographic Technologies" first?

Moriai There are new requirements emerging due to the spread of IoT. This R&D initiative is working to create cryptographic technologies with new functionality, able to meet these needs. For example, most IoT devices are small, low-power, and only have a small amount of memory, so they require cryptographic technology that is lightweight relative to conventional technologies.

We are also researching technologies that enable Big Data analysis on data while it is still encrypted. When users want to perform Big Data analysis, they often want to store data in the cloud, or contract the analysis to an external agency. This creates potential for personal information leaks.

Data can be encrypted in these cases, but analysis cannot usually be done on the data without decrypting. Homomorphic encryption schemes permit analysis of data in encrypted form, and research on them is currently advancing around the world. However, since the data is encrypted, there can be doubt whether the analysis was performed on the correct data. To deal with this concern, a technology called "mis-operation resistant searchable homomorphic encryption," has been proposed, which incorporates a feature for detecting when ciphertexts associated with different keywords have been introduced (See pp. 4-5). This technology enables secure Big Data analysis to be done while protecting privacy. Last year, in collaboration with Tsukuba University, we succeeded in analyzing encrypted data securely to find statistical relationships between genetic information and disease rates for individuals. This was announced in a press release.

—— Could you talk about the second initiative, "Security Evaluation of Cryptographic Technologies"?

Moriai The objectives of research on security evaluation of cryptographic technologies are to contribute to building and maintaining safe and secure ICT systems, and to standardizing and promoting new cryptographic technologies. These activities include evaluating the security of cryptographic techniques on the e-Government Recommended Ciphers List, and promoting the CRYPTREC* project, whose goal is to realize a secure ICT society. The project is operated in collaboration with the Ministry of Internal Affairs and Communications (MIC), the Ministry of Economy, Trade and Industry (METI), and the Information-technology Promotion Agency of Japan (IPA). As an example, major technological innovations such as quantum computers can have immeasurable impact on society. When quantum computers are realized, the public key cryptosystems currently supporting secure communication on the Internet will be breakable, so it is imperative that we prepare for this now.

—— So, when will quantum computers be realized?

Moriai That is difficult to predict, but it has been proven mathematically that public key cryptosystems currently in use can be broken using quantum computers, so something must be done. A quantum-gate quantum computer will have a direct impact on the security of public key cryptosystems, and such a computer at a scale large enough to solve the RSA currently in use is still some years in the future. On the other hand, quantum annealers are on the market, which are very efficient at solving optimization problems. We are working with Fujitsu Laboratories and Tokyo University, studying and evaluating methods using them to solve prime factorization problems, the mathematical basis of RSA, but we think it will still be difficult to solve such problems with large parameters.

—— And what about the third initiative, "Privacy Enhancing Technologies"?

Moriai R&D contributing to utilization of personal data is advancing from several perspectives, and we have initiatives on privacy-preserving data analysis as introduced on pp. 8-9, and also evaluation of data anonymization technologies. The revised Act on the Protection of Personal Information was instituted in May 2017, introducing the concept of Anonymized Information. Anonymized information is personal information that has been processed such that no particular individual can be identified, and the original personal information cannot be restored. If information has been anonymized, it can be provided to third parties without the consent of the data owner. Since 2019, so-called "information bank" companies, which gather and manage personal data, have taken hold and there are companies that want to use anonymized medical information. Is it possible to reduce the risk of re-identification somehow, while maintaining security and the utility of the data, so that it can be implemented in society? Our laboratory is evaluating the security and utility of such anonymized information.

Alongside NICT, the entire industry is working to promote development of secure, highly useful data anonymization technologies, with this and other initiatives, such as the PWS CUP anonymization and re-identification competition held at the Computer Security Symposium, Information Processing Society of Japan (IPSJ) since 2015.

—— What are your objectives for 2020, the final year of the current Medium- to Long-term Plan?

Moriai We must move forward with standardization of post quantum cryptography. In the past, it has taken nearly 20 years for new cryptographic technologies to take hold, so regardless of when large-scale quantum computers are realized, standardization and security evaluation of post quantum cyptography are urgent matters. There are currently various domestic and international activities in this area, and NIST in the USA is engaged in standardization that will be particularly influential. This is because, in its history, NIST has introduced many cryptographic technologies that have become de-facto international standards, so their standardization activities are watched closely by countries and related organizations around the world. NIST has announced that they aim to release a draft standard for post quantum cryptography in 2022 or 2023. NICT will contribute to security evaluation of post quantum cryptography and study on the cryptographic technologies referenced in information-system procurement documents for all government departments in the CRYPTREC project in Japan.

Objectives

—— What is your role as a national R&D agency?

As a national R&D agency, our intention is to continuously produce highly reliable information about security evaluation of cryptographic technologies from a neutral, impartial, and public standpoint.

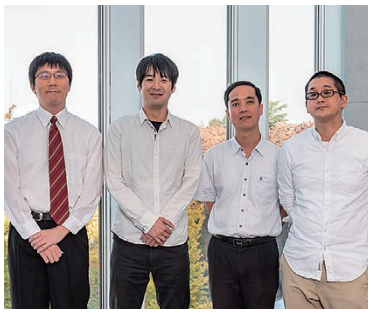
In addition to security, we are working to address protection of privacy, which has been of increasing concern recently. Both of these issues will continue to increase in importance and will be a basis for research in our effort to fulfill our role.

Our entire laboratory is working to produce research results with practical uses in society, and technologies that will be useful throughout the world.

* CRYPTREC: Cryptography Research and Evaluation Committees

Research and Standardization of Post-Quantum Cryptography

Measures against quantum computer threats on cryptosystems



From the left: Yoshinori AONO, Naoyuki SHINOHARA, Le Trieu PHONG, Takuya HAYASHI

Security Fundamentals Laboratory, Cybersecurity Research Institute

Naoyuki SHINOHARA
Senior Researcher
Joined NICT in 2009. He has been engaged in research on security evaluations of public key cryptosystems. Ph. D. (Mathematics).

Yoshinori AONO
Senior Researcher
Joined NICT in 2011. He is working on cryptanalysis algorithms and security evaluations. Ph. D. (Sciences).

Sachiko KANAMORI
Technical Researcher
Joined NICT in 2010. She is engaged in R&D about security and privacy.

Takashi KUROKAWA
Technical Researcher
Joined NICT in 2010. He is engaged in R&D about security evaluation of cryptographic technology.

Takuya HAYASHI
Senior Researcher
Joined NICT in 2018. He is working on cryptographic engineering, cryptanalysis, and privacy preserving data mining. Ph.D. (Functional Mathematics).

Le Trieu PHONG
Senior Researcher
Joined NICT in 2015. He is working on cryptographic algorithms, and privacy-preserving data mining. Ph.D. (Arts and Science).

Cryptosystems are essential technologies for secure communication and to protect information and are widely used in many familiar situations such as in mobile telephones, ePassports, wireless networks, Internet shopping, and Internet banking. Owing to recent developments in quantum computers, there is increasing concern that the security of cryptosystems currently being used will drop dramatically. To counter this, there is ongoing development and standardization of post-quantum cryptography (PQC) around the world. In this article, we introduce some results from the Security Fundamentals Laboratory.

Why Post-Quantum Cryptography (PQC) is needed

There is increasing concern regarding widely used public-key cryptosystems such as RSA and elliptic-curve cryptography (ECC) because they may be breakable using quantum computers. The reason for this concern is the relationship between the mathematical structures used in these cryptosystems and a quantum algorithm called Shor's algorithm.

RSA uses two prime numbers as the private keys which are the secret information. The public key used in RSA is the product of these prime numbers, as shown in Figure 1. Thus, the private keys can be obtained by factoring the composite number used as the public key. Currently, such products of 2048 bits (617 digits) are used as RSA public keys, and this is large enough to prevent them from being factored even when using the most efficient algorithm currently known, which is the general number field sieve (GNFS), on the fastest supercomputer in the world for a significant amount of time (e.g., a year). Even if an algorithm better than GNFS is discovered, or supercomputer performance increases, security can be preserved by increasing the size of the key. However, this would significantly increase the computational cost for cryptography processing and could make the cryptosystem impractical. Shor's algorithm factorizes integers using a quantum computer and is much more efficient than GNFS. Thus, if a high-performance quantum computer is developed and is able to apply Shor's algorithm to the products of sufficiently large prime numbers, the utility of RSA will drop greatly.

A similar result is known with respect to ECC. The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). Shor's algorithm can also be applied to solve the ECDLP and, as with integer factorization, it is known to also be efficient in this case.

Development of Post-Quantum Cryptography

Cryptography whose security is based on problems that cannot be solved efficiently using a quantum computer, in contrast with integer factorization and the ECDLP, is called post-quantum cryptography (PQC). Research, development, and standardization of PQC are currently advancing globally. A typical example of PQC is lattice-based cryptography, based on the lattice problem (Figure 2). The Security Fundamentals Laboratory has used lattice-based cryptography to develop a new cryptographic system called LOTUS.

With the recent developments in quantum computers, the National Institute of Standards and Technology (NIST) started the Post-Quantum Cryptography Standardization project in 2016, and it called for submissions of proposed standards in 2017. NICT developed the LOTUS lattice-based cryptography, and it was included in the 69 submissions that passed the document review (Figure 3). All submitted proposals have been posted on the NIST Web site,

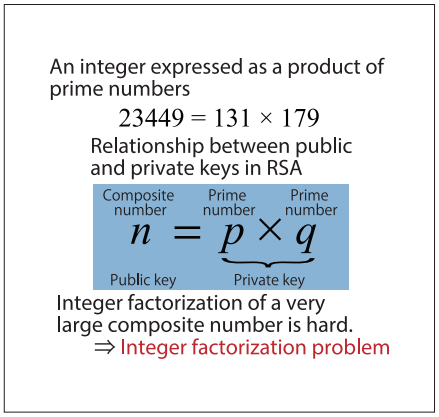


Figure 1 Security of RSA and integer factorization

and discussion of the proposals is published on dedicated mailing lists. As of December 2018, security defects have been identified in approximately 30 of the submissions, including some insignificant issues, and five of the proposals have already been withdrawn. NIST narrowed down these proposals and published the results on 30th January 2019. LOTUS did not remain on the ballot, however, at the time of writing, no significant defects have been discovered in LOTUS. Compared with the proposals based on LWE (Figure 2), LOTUS uses a large public key, but the size of the ciphertext is small. This implies LOTUS is suitable in situations requiring few renewals of the public keys.

Besides proposing cryptography systems, enterprises, universities, and public institutions are also publishing various mathematical problems related to the security of cryptographic systems, discussing issues such as the parameter settings needed when actually using a cryptography scheme, and evaluating the size of mathematical problems and how much time will be needed to solve them. The Lattice Challenge, organized by the Technical University of Darmstadt, is a well-known forum for the lattice problem, which is the basis of LOTUS security, where researchers from around the world report on their experiments. The Security Fundamentals Laboratory has contributed to the evaluation of lattice-based cryptography for many years, breaking records in this contest on several occasions.

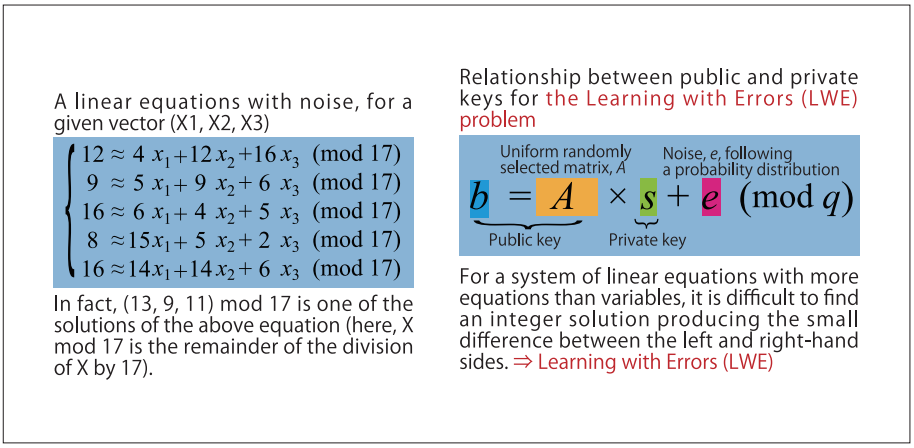


Figure 2 Example of a lattice problem (the LWE problem)

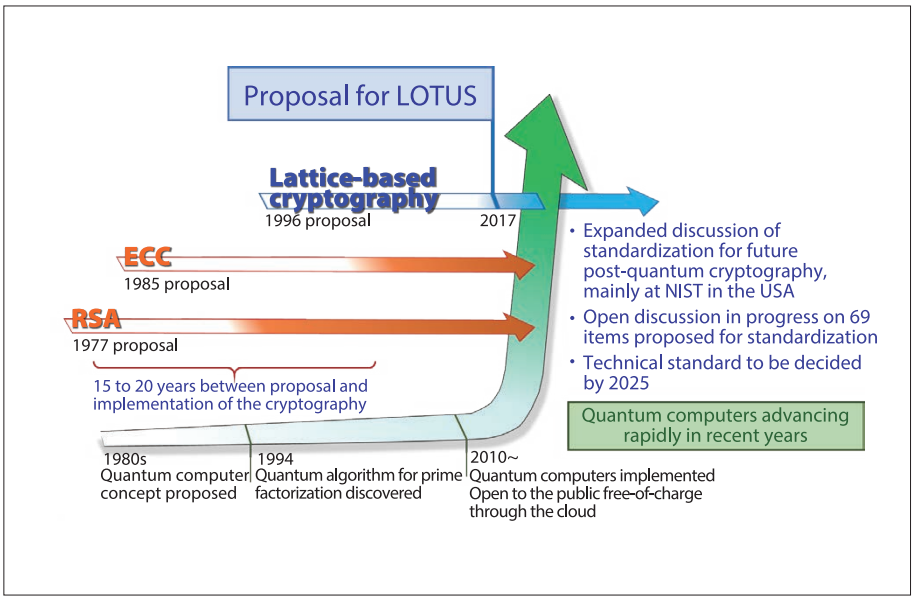


Figure 3 Development of LOTUS

Preparation for Standardization of Post-Quantum Cryptography in Japan

NICT collaborates with the Ministry of Internal Affairs and Communications (MIC), the Ministry of Economy, Trade and Industry (METI), and the Information-Technology Promotion Agency (IPA) in the administration of CRYPTREC, a project conducted to evaluate the security of cryptography used by e-Government in Japan. Within NICT, this is handled by the Security Fundamentals Laboratory. The project conducted a study of lattice-based cryptography as a promising candidate for PQC in 2014. It also began studying other promising candidates (code-based cryptography, multivariate cryptography, isogeny-based cryptography, etc.) in 2017, and technical reports on these studies are to be published in 2019.

Future Prospects

Recently, many PQC have been proposed, prompted by the call for proposals by NIST. We expect active research in the future to evaluate the security of these and other PQC proposals. Through its R&D efforts and activity with CRYPTREC, the Security Fundamentals Laboratory will contribute to the evaluation and development of lattice-based cryptography and other PQC systems.