National Institute of
Information and Communications Technology

NICT NEWS

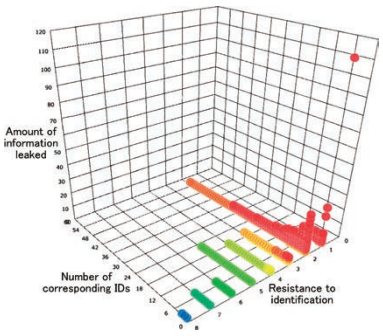
2019
No. 2
Vol. 474

FEATURE

New Frontiers in Cryptography

NICT NEWS 2019 No.2 Vol.474
National Institute of Information and Communications Technology

CONTENTS



FEATURE

New Frontiers in Cryptography

1 INTERVIEW
Toward Safe and Secure Data Utilization
The frontiers of cryptographic technologies
Shiho MORIAI

4 Research on Security Improvement for Homomorphic Encryption
Towards privacy-preserving data mining for personal data
Keita EMURA / Miyako OHKUBO / Takuya HAYASHI

6 Research and Standardization of Post-Quantum Cryptography
Measures against quantum computer threats on cryptosystems
Naoyuki SHINOHARA / Yoshinori AONO / Sachiko KANAMORI / Takashi KUROKAWA / Takuya HAYASHI / Le Trieu PHONG

8 Privacy-Preserving Data Analytics
Le Trieu PHONG / Takuya HAYASHI / Yoshinori AONO / Takuma ITO

10 Information-Theoretically Secure Communication Technologies for Small Satellites
Maki YOSHIDA

TOPICS

12 Development of Vertical Gallium Oxide (Ga_2O_3) Transistors Using Highly Versatile Process
—Opening the way to mass production of low-cost Ga_2O_3 power devices—

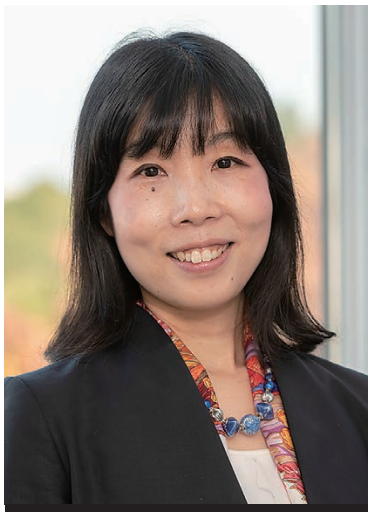
13 NICT's Challengers File 3
Cryptographic Implementations
–Achieving both efficiency and security–
Takuya HAYASHI

Cover photo:
Members of the Security Fundamentals Laboratory in discussion. Each member is involved in several research projects being promoted by the laboratory, with many friendly discussions and cooperating organically in their activities.
Upper-left photo: The URANUS privacy risk evaluation system, which provides support for privacy enhancing data processing. It is a tool that evaluates the risk of identifying individuals from data that has been processed to remove names and other personal identifiers. Cases where individuals could be identified with a small amount of information (resistance to identification is small) or where the amount of information leaked will be large if their identities are revealed are circled in red, warning that the risk is large before such data is released.

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

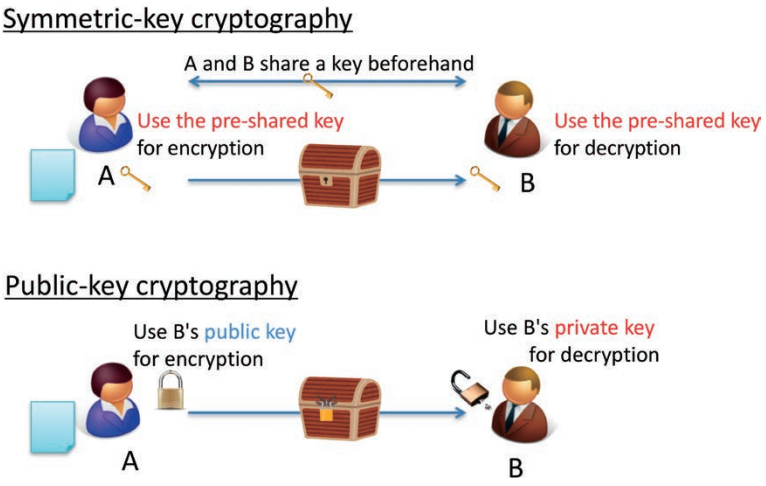


Figure Symmetric-key cryptography and public key cryptography

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.

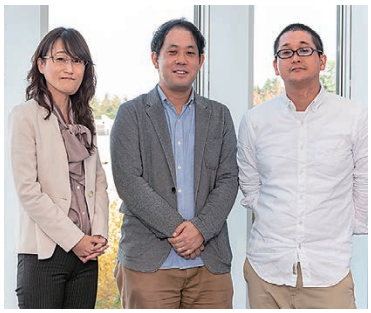
In addition to security, we are working to address protection of privacy, which has been of increasing concern recently. Both of these issues will continue to increase in importance and will be a basis for research in our effort to fulfill our role.

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 on Security Improvement for Homomorphic Encryption

Towards privacy-preserving data mining for personal data



From the left: Miyako OHKUBO, Keita EMURA, Takuya HAYASHI

Security Fundamentals Laboratory
Cybersecurity Research Institute

Keita EMURA
Senior Researcher

He joined NICT in 2012 and has been a Senior Researcher since 2014. His research interests include public-key cryptography and information security. Ph.D. (Information Science).

Miyako OHKUBO
Senior Researcher

She joined NICT in 2010. Her research interest is to establish theory and practice on cryptographic primitives and protocols. Ph.D. (Engineering).

Takuya HAYASHI
Senior Researcher

He joined NICT in 2018. He is working on cryptographic engineering, cryptanalysis, and privacy preserving data mining. Ph.D. (Functional Mathematics).

Since many security incidents have been frequently reported on TV, the importance of security is now widely recognized. Cryptography, our area of research, is part of the field of security. What do you think about when you hear this? You may think of passwords or techniques employed in online shopping if you are aware of security techniques. Confidentiality, integrity, and availability are fundamental functionalities of security in cryptography. In addition, several cryptosystems with high functionalities have been proposed so far, and here we introduce homomorphic encryption and its security improvement as one topic related to these cryptosystems.

Structure of Homomorphic Encryption

It may be difficult to imagine what homomorphic encryption can do. In simple terms, it can perform computations on encrypted data. For example, if one votes 1 for YES and 0 for NO, then the sum of the voting results represents the number of YES votes. If one does not want to reveal who voted for what, then the votes can be protected from a third person by encrypting them. However, how should the votes be aggregated? If the aggregator decrypts ciphertexts, then they can compute the aggregated sum. However, the aggregator knows which ciphertexts are encryptions of YES and NO. By using a homomorphic encryption scheme, a ciphertext of the aggregated sum can be computed from the ciphertexts of YES and NO without decrypting them. As an application of this functionality, we can delegate some computations of data that must be kept secret, for example, personal data, medical data, and bank transfers. We aim to apply our research results to real problems in the financial industry such as detecting illegal money transfers and making credit limit decisions based on big data across industries (See JST CREST "Privacy-preserving Data Analytics to Promote Cross-industry Data Sharing"). See Figure 1.

Security Improvement for Homomorphic Encryption

Here, we introduce the security of homomorphic encryption (please see p8-9 in this issue. "L. T. Phong et al., Privacy Preserving Data Analytics" for a discussion of what can be computed by homomorphic encryption). The property that anyone can "freely" perform the operation inevitably means that ciphertexts are malleable. Thus, it is well known that security against adaptive chosen ciphertext attack (CCA) and the homomorphic property can never be achieved simultaneously. Although we do

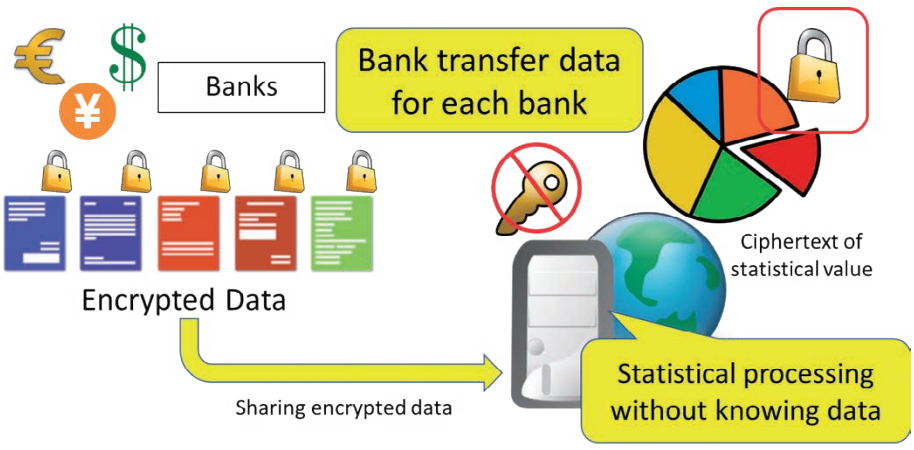


Figure 1 Privacy-preserving data analytics to promote cross-industry data sharing

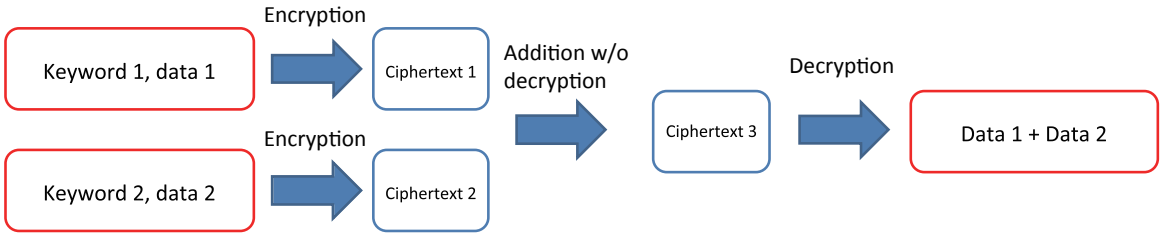


Figure 2 Homomorphic operation for the same keyword (keyword 1 = keyword 2)

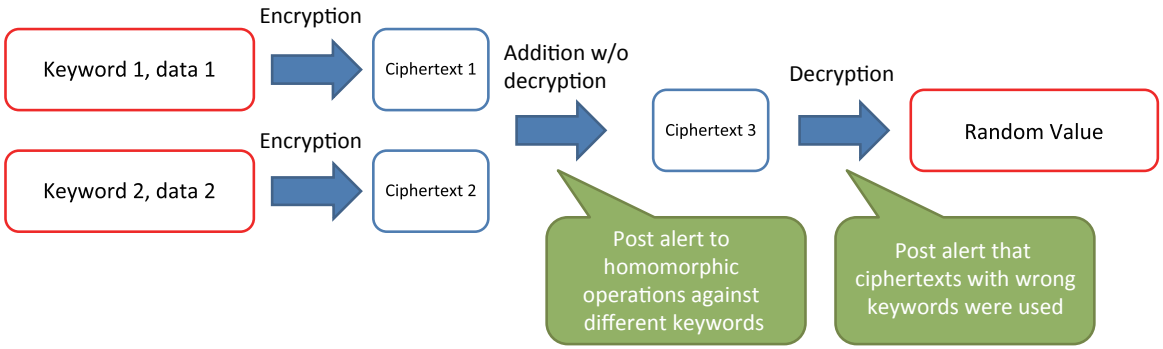


Figure 3 Homomorphic operation for different keywords (keyword 1 ≠ keyword 2)

not explain CCA security in more detail here, it has been widely recognized as a standard security. For example, CCA-secure encryption schemes are contained in the CRYPTREC Ciphers List (https://www.cryptrec.go.jp/en/list.html). We have shown that CCA security and the homomorphic property can be simultaneously handled in situations that the user(s) who can perform homomorphic operations on encrypted data should be controlled/limited, and we proposed a new concept of homomorphic public-key encryption, which we call keyed-homomorphic public-key encryption. This result was awarded the Symposium on Cryptography and Information Security (SCIS) Innovation Paper Award from IEICE in 2012.

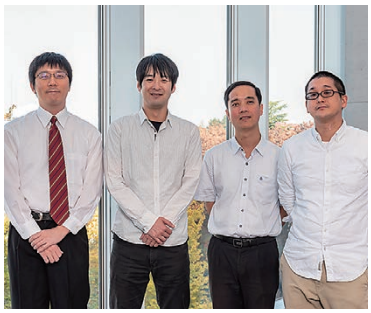
Since data are encrypted, it is difficult to check whether the correct data are used for statistical processing. For example, when medical data are treated, then the homomorphic operation against ciphertexts related to different diseases should NOT be allowed to be performed. If such a mis-operation happens, then medical records of different diseases are unexpectedly mixed. In conventional homomorphic encryption, there is no way to prevent such an unexpected homomorphic operation. This fact may become visible after decrypting a ciphertext, or in the worst case it might be never detected. We proposed mis-operation resistant homomorphic encryption, which allows homomorphic operations to be performed against ciphertexts associated with the same disease without revealing the disease name (See Figures 2 and 3). This result was awarded the Computer Security Symposium (CSS) Best Paper Award from IPSJ in 2016. We further improved its efficiency by employing our technique that changes the underlying elliptic curve for fast computation.

Future Prospects

Homomorphic encryption has a unique property that it can be performed on encrypted data. At the cost of this property, the standard security level is reduced. We hope to encourage privacy-preserving data mining for personal data by further improving the security of homomorphic encryption.

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,

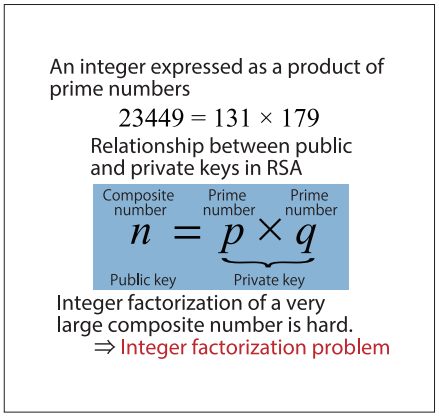


Figure 1 Security of RSA and integer factorization

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.

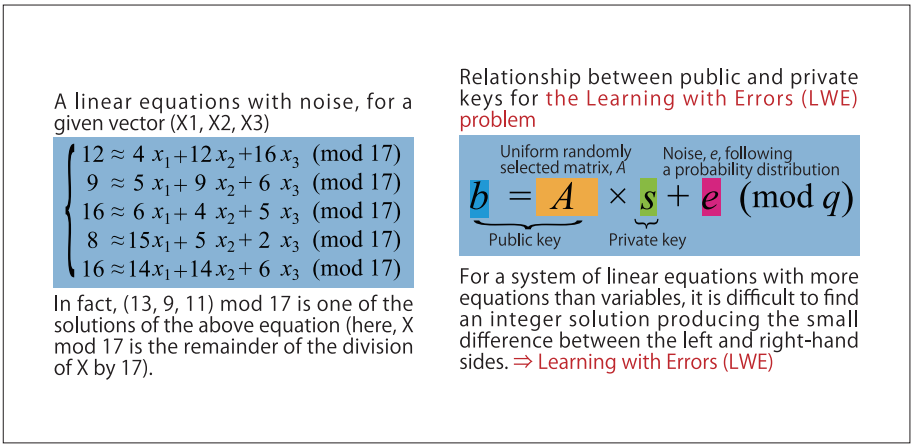


Figure 2 Example of a lattice problem (the LWE problem)

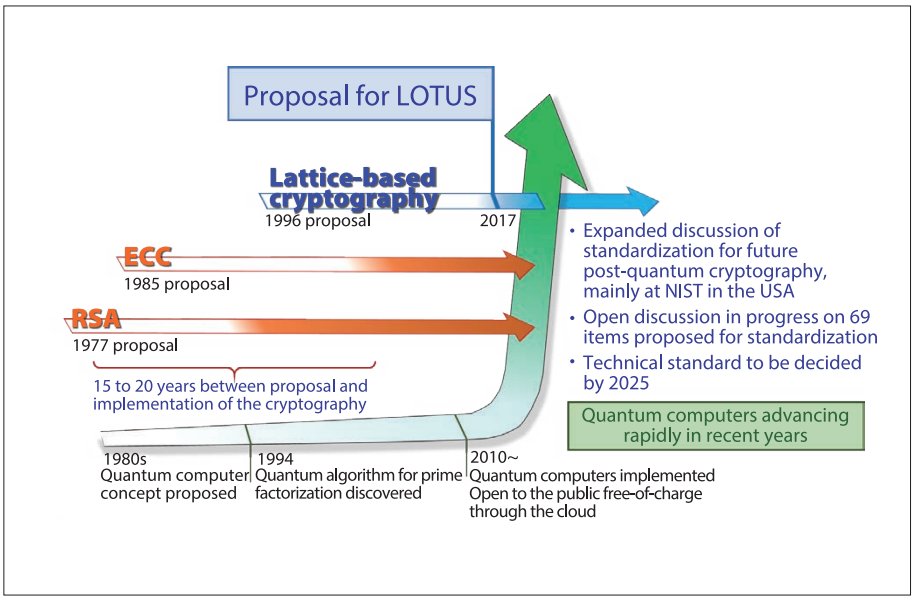


Figure 3 Development of LOTUS

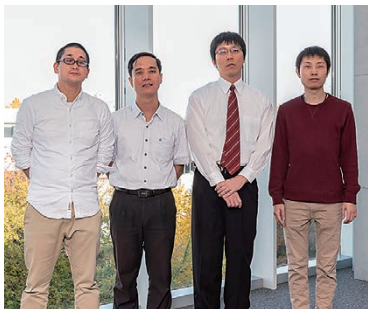
Preparation for Standardization of Post-Quantum Cryptography in Japan

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.

Privacy-Preserving Data Analytics



From the left: Takuya HAYASHI, Le Trieu PHONG, Yoshinori AONO, Takuma ITO

Security Fundamentals Laboratory
Cybersecurity Research Institute

Le Trieu PHONG
Senior Researcher

Joined NICT in 2015. He is working on cryptographic algorithms and privacy-preserving data mining. Ph.D. (Arts and Sciences).

Takuya HAYASHI
Senior Researcher

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

Yoshinori AONO
Senior Researcher

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

Takuma ITO
Researcher

Joined NICT in 2018. He is working on security evaluations and implementations in cryptographic technology.

Recent advances in data mining technology have enabled information of high value to be extracted from big data, to be used in implementing various services. For example, systems that are able to recommend products of interest to customers have been implemented by analyzing their age, sex, and purchase history data from retail services. On the other hand, this high-value information can also contain a significant amount of private information, so users have an increasingly uneasy feeling regarding the possibility that this information could leak or be used without appropriate restrictions. One way to resolve this type of problem is to use privacy-preserving data analytics technologies.

The Security Fundamentals Laboratory is conducting R&D on high-speed, big-data analytics technologies that use encryption technology to keep data in a state that preserves privacy. This technology is able to prevent organizations*1 unrelated to the data provider from seeing the data while they perform data analysis with machine learning or artificial intelligence. This should reduce feelings of insecurity for the providers of data.

This article introduces DeepProtect, which uses deep learning together with a new homomorphic encryption technology called SPHERE, developed at the laboratory.

SPHERE (Security-updatable Public key Homomorphic Encryption with Rich Encodings)

Homomorphic encryption technology is able to process data in encrypted form, and when used in privacy-preserving data analytics, the server processing the data knows what computations are being done, but it cannot know what data has been included in the computation.

The security of a cryptosystem is its ability to preserve confidentiality, but as encryption breaking technologies advance, there is always a danger that this security will break down. Opinions on whether data that is encrypted today will remain secure decades into the future are divided, even among experts, so to be on the safe side, we must continue to work on technology that will be effective in the long term.

The Security Fundamentals Laboratory developed the SPHERE homomorphic encryption technology in 2015, to find solutions to this sort of basic problem. SPHERE incorporates a technology to increase the security level of encrypted data, making it possible to strengthen the encryption as encryption breaking technologies advance. It is promising for data mining applications with genetic and other data in fields such as insurance and medicine.

SPHERE uses lattice-based homomorphic encryption, which is recognized as a promising candidate for post-quantum cryptography. We have focused on a feature that partitions the ciphertext into a data region and additional data, and the strength of the encryption is determined by this additional data. We are able to increase the level of security, while keeping the data in an encrypted state, by extending the additional data (Figure 1). When doing so, the data region is not altered, so homomorphism is maintained and data analytics can continue to be performed on the data in encrypted form.

Data analytics experiments using SPHERE

To verify the utility of SPHERE, we conducted encrypted data analytics experiments on a server using simulated data. We performed a

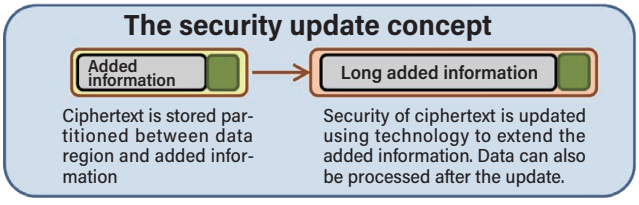


Figure 1 The security update concept

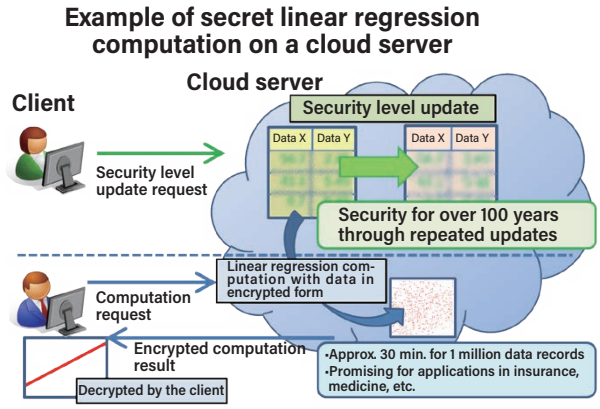


Figure 2 Secret linear regression computation using SPHERE

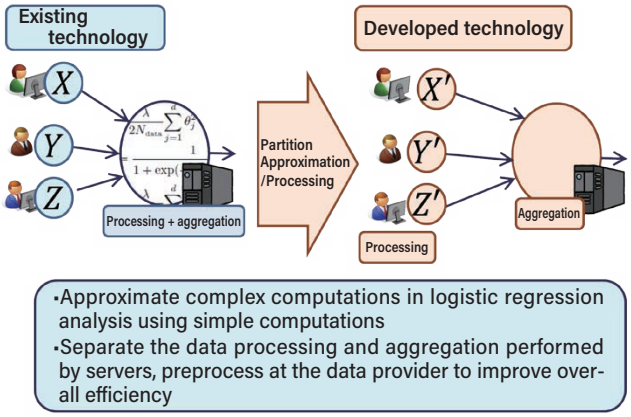


Figure 3 Logistic regression analysis

linear regression computation on one million encrypted data items and confirmed that the analysis could be completed on a standard server in approximately 30 minutes (Figure 2).

Then, over a period of one year, we worked on ways to perform a logistic regression analysis on encrypted data. The following two techniques were found to be factors that determined computation speed in tests including use of real data (Figure 3).

[Approximating calculation] When using machine learning, meticulous computation is not mandatory, and adequate classification on a practical level can be obtained using an approximating calculation.

[Data pre-processing] The provider performs appropriate pre-processing before uploading data to the cloud.

Logistic functions are difficult to perform using homomorphic encryption, but these techniques can be used to approximate the computation with simple 2D functions. Speed can also be increased significantly by having data providers perform multiplication operations before submitting data.

In 2016, we performed a simulation of these techniques using simulated data and showed that analysis of one hundred million data items was possible on a server in less than 30 minutes.

DeepProtect

The laboratory is currently developing technology able to apply deep learning with data from multiple organizations, without disclosing individual data items (Figure 4). Generally with deep learning, increasing the amount of data used improves the results obtained, so combining data from different organizations in the same field can be expected to improve results further. However, considering the need to maintain confidentiality, it has been almost impossible to take data out of an organization for such purposes.

As such, we have developed a deep learning technology called DeepProtect, which combines encryption technology with cooperative computation.

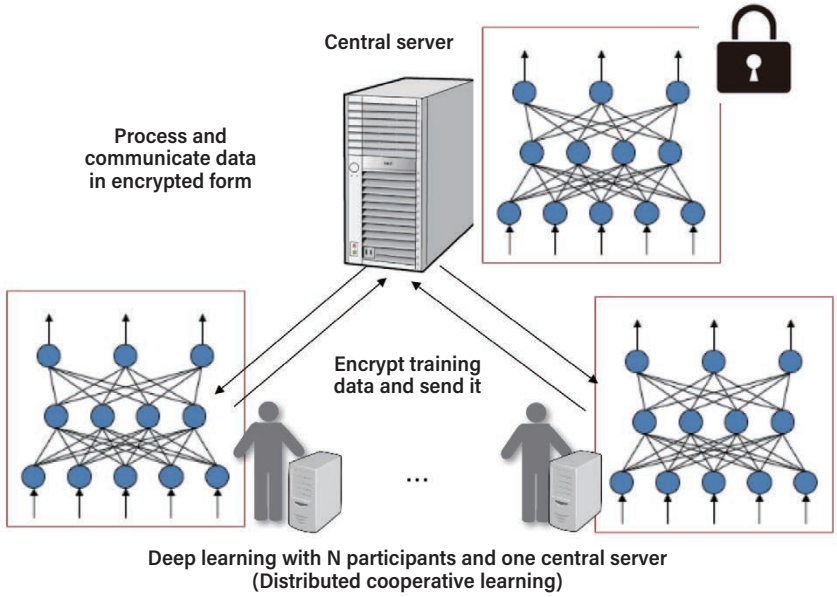


Figure 4 Technology enabling deep learning without disclosure of data

For deep learning, we perform training using an optimization algorithm called "stochastic gradient descent." A feature of this algorithm is that it performs training computations successively for each data item. Thus, training can be done using the data at one organization, and only the training results are passed to the next organization. In this way, training can be done at all participating organizations, yielding the same result as if data from all organizations was combined.

This enables training using all data to be done without disclosing any individual data items.

DeepProtect is also very practical. We conducted a practical test using DeepProtect, training with 280,000 unauthorized credit-card transaction records. Training completed in a few minutes, and the results were able to identify unauthorized transactions in approximately one millisecond, demonstrating performance adequate for real-time operation.

Conclusion

With the development of data mining technologies, they are attracting attention as a way for enterprises to exploit big data in their possession, but protection of privacy is becoming more important globally, with developments like the enactment of the EU General Data Protection Regulation.*2 As such, there is increasing demand for data analytics that can be done at high speed, while also maintaining security that protects privacy. The Security Fundamentals Laboratory is advancing R&D on privacy-protecting data analytics that achieves both high speed and security.

*1 E.g.: The administrators of cloud servers that perform data storage or computation.

*2 Regulations protecting data regarding all individuals in the EU region. It is also being applied to businesses outside the EU region. Enacted on May 25, 2018.

Information-Theoretically Secure Communication Technologies for Small Satellites

Maki YOSHIDA
Senior Researcher
Security Fundamentals Laboratory
Cybersecurity Research Institute

After completing the doctoral course at a graduate school, worked as an Assistant Professor at Osaka University. Entered NICT in 2013. Engaged in R&D in information security. Ph. D. (Engineering).

On November 15, 2018, the Act on Launching of Spacecraft, etc. and Control of Spacecraft was enacted. Guidelines related to this act state that security measures, including encryption, must be taken for the transmission of signals related to safety-critical systems. In this new age, with private enterprise engaging in space business, we present a feasibility study for achieving the highest level of security, called information-theoretic security, in the context of spacecraft communication using currently available, low-cost electronic devices. In this article, we introduce a secure communication technology that we have proposed.

Towards NewSpace

Many small satellites are being launched for scientific and commercial purposes. Low-cost small launch vehicles for launching small satellites are also being developed by private enterprise. We are entering the so-called "NewSpace" era, with private enterprise engaging in space business, and accordingly, the Act on Launching of Spacecraft, etc. and Control of Spacecraft (the so-called "Space Activity Act") was enacted on November 15, 2018.

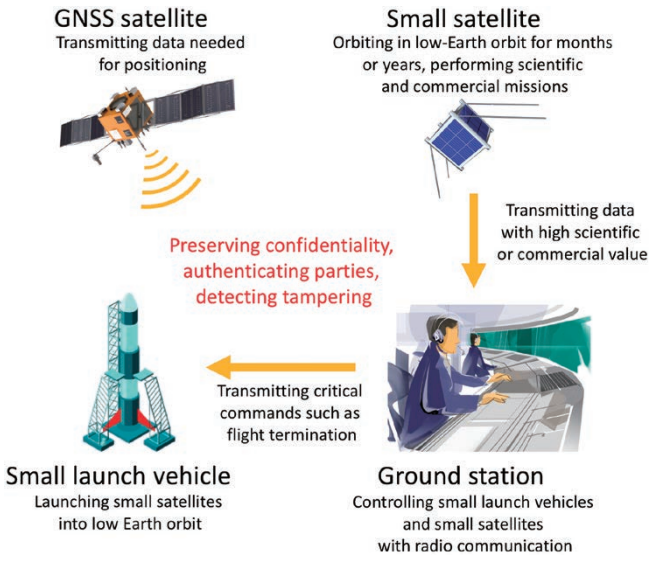


Figure 1 Secure communication between ground stations, small satellites, and small launch vehicles

In guidelines related to the Space Activity Act, the transmission of signals related to safety-critical systems is required to take security measures, including appropriate encryption, to prevent interference or takeover. Because signals related to safety-critical systems include commands for flight termination (Figure 1, bottom), threats to public safety, such as the fall, collision, or explosion of spacecraft in an unintended location, could result if a third party could freely impersonate the ground station and tamper with signals. Even noncritical signals, such as data transmitted from the satellite to the ground station (Figure 1, right), could have scientific or commercial value. Thus, eavesdropping or tampering would be very undesirable.

The objective of this research is to develop secure communication technologies using cryptosystems, designed mainly for transmitting signals between ground stations, small satellites, and small launch vehicles.

The highest level of security: "Information-theoretic security"

There are several security levels of cryptosystems. However, the guidelines for the Space Activity Act do not specify an adequate level of security. Considering public safety and protecting the scientific and commercial value of the transmitted data, achieving the highest level of security possible would be ideal.

In the theory of cryptography, the highest level of security is referred to as information-theoretic security. In an information-theoretically secure system, large keys are used to protect the communication so that the system cannot be broken even by adversaries with unlimited computing resources.[*1] Here, "unlimited computing resources" include all current technologies such as supercomputers as well as future technologies such as quantum computers, in continuous operation until the end of the universe, and all resources in the universe.

Achieving information-theoretic security with low-cost electronic devices

In this work, we have presented the first feasibility study on achieving information-the-

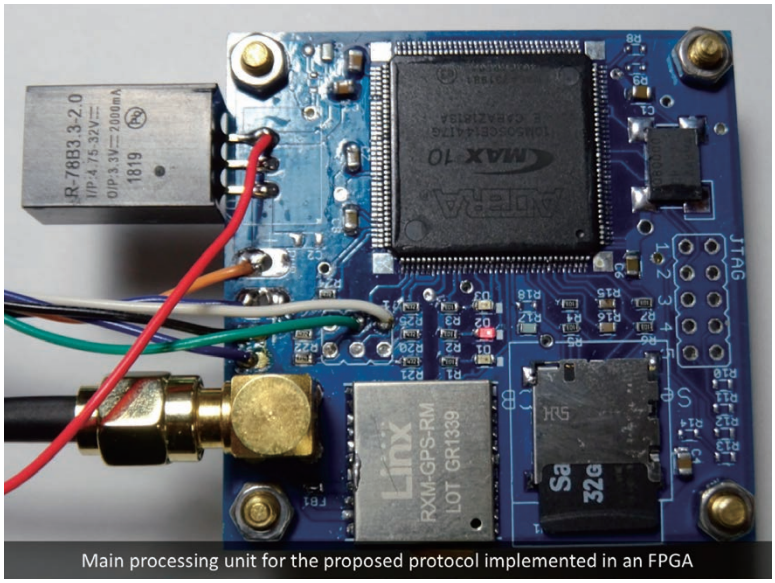


Figure 2 Prototype board

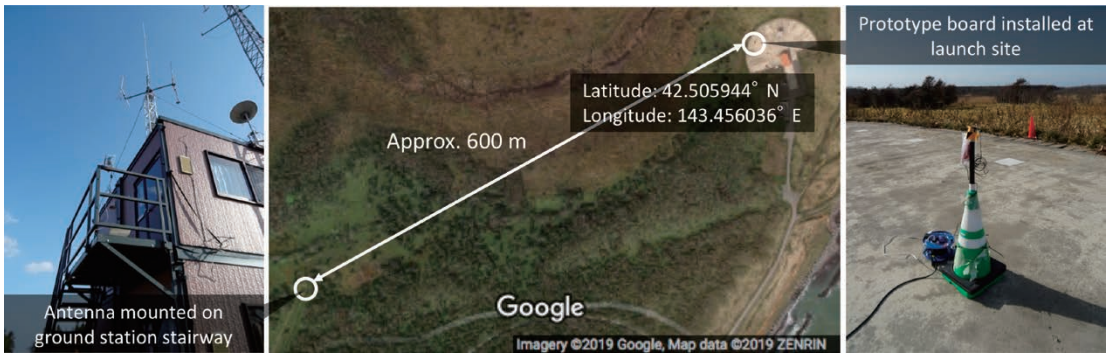


Figure 3 Radio transmission test site

oretic security in communication systems for satellite launches by private enterprise using currently available, low-cost electronic devices. Specifically, we have collaborated with Dr. Sumio Morioka of Interstellar Technologies Inc. and Prof. Satoshi Obana of Hosei University to analyze such communication systems, define the security requirements, formulate a security model, propose cryptographic protocols, and evaluate these protocols.

To achieve information-theoretic security, we need to combine various cryptographic technologies and design how these technologies are used for processing and transmitting data using keys. Even if the cryptographic technologies used are secure and the keys are sufficiently large, the strength of the security is also affected by how they are used. Any design flaw can make a key useless or make the system easy to break. Conversely, by using a suitable design, the effectiveness of the keys can be maximized, reducing the cost without reducing the strength of the security.

The proposed protocols consist of a process to establish secure communication between the ground station and the small launch vehicle or small satellite (referred to as entities below), and a process to maintain synchronization between the entities. First, to prevent loss of control due to inconsistencies between entities, we exclude interaction. Second, we also use the same mechanisms for the authentication of data and entities in both processes, establishing secure communication and synchronization, so that they can be performed simultaneously without weakening the security. Then, because entities in the communication systems being considered are physically close before the launch, it is easy to physically share a key. The communication lifetime is also relatively short, so the total amount of communication can be controlled. These factors enable information-theoretic security to be achieved at a low cost.

We implemented the main processes of the proposed protocols using devices currently available for small satellites and small launch vehicles, including a low-end FPGA (Figure 2). We then tested radio transmission between a ground station and a launch pad location (Figure 3). Note that for the transmission of commands and a small amount of mission data, memory cards and SSDs of several hundred megabytes to several terabytes are sufficient for key storage. We confirmed that our hardware implementation achieved speeds of up to 16 Gbps,*2 and that in our radio transmission tests, the processes to establish secure communication and maintain synchronization functioned simultaneously.

Future prospects

This work is a pioneering study toward the introduction of information-theoretically secure communication systems for spacecraft. It has also provided the valuable result of showing that information-theoretic security is now reaching the stage of practical use owing to recent progress on highly integrated, low-cost semiconductor devices and communication equipment.

A possible future work is to apply the results to high-capacity data transmission such as optical satellite constellation networks. This will contribute to safety and security in space, an emerging new venue for human activity.

*1 Widely used cryptographic technologies such as public key cryptosystems are computationally secure even when the amount of key information is significantly reduced, but the systems can be broken by those who have very large computing resources.

*2 The proposed protocols could use computationally secure cryptographic technologies commonly employed in various systems. However, the information-theoretically secure version is much more efficient in terms of computational cost.

Development of Vertical Gallium Oxide (Ga_2O_3) Transistors Using Highly Versatile Process

—Opening the way to mass production of low-cost Ga_2O_3 power devices—

Currently, innovative energy-saving technologies are being pursued with high priority on a global scale. The power switching devices used for power conversion have many applications in these technologies, so any reduction of losses in individual devices accumulates to large-scale energy saving in the society. Use of gallium oxide (Ga_2O_3) as a material for power switching devices promises to yield higher voltage, higher power, and lower loss than existing semiconductor devices. Furthermore, high-quality, large-diameter, single-crystal Ga_2O_3 wafers can be fabricated relatively easily and at low cost. For these reasons, Ga_2O_3 power transistors and diodes are being actively developed globally.

Dr. Masataka HIGASHIWAKI, Director of the Green ICT Device Advanced Development Center in the NICT Advanced ICT Research Institute, in collaboration with Prof. Yoshinao KUMAGAI and Associate Prof. Hisashi MURAKAMI of the Department of Applied Chemistry, Tokyo University of Agriculture and Technology, have successfully developed a vertical Ga_2O_3 transistor* using ion-implantation doping technology. Ion-implantation doping technology is a fabrication process in which impurity atoms are ionized, accelerated to high speed, and directly implanted into a solid substrate. The technique allows us to simultaneously fabricate many types of device structures on the same substrate easily and is often used for production of practical semiconductor devices. The transistor developed in this work demonstrated a drain-current on/off ratio of more than eight orders of magnitude by gate voltage modulation and better device characteristics than any other similar vertical Ga_2O_3 transistors reported thus far.

This collaborative research team will continue development to solve some remaining issues, such as increasing device breakdown voltage, as needed for power switching devices. If vertical Ga_2O_3 transistors can be commercialized in the near future, they promise to significantly reduce losses in switching operations, compared to existing semiconductor transistors.

The device fabrication technology based on the ion-implantation doping used in this research is suitable for mass production, is highly versatile, and enables low-cost production, so it is expected to contribute in the future to the full-scale development of Ga_2O_3 power devices at private enterprises such as electronics and automobile companies. High-performance Ga_2O_3 power devices will contribute directly to global energy conservation and also, in economic terms, to the creation of a new semiconductor industry in Japan.

This work was partially supported by Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Next-generation power electronics" (funding agency: New Energy and Industrial Technology Development Organization).

Reference

Man Hoi Wong, Ken Goto, Hisashi Murakami, Yoshinao Kumagai, and Masataka Higashiwaki, "Current Aperture Vertical β-Ga_2O_3 MOSFETs Fabricated by N- and Si-Ion Implantation Doping," in IEEE Electron Device Letters.
https://ieeexplore.ieee.org/document/8556005
DOI: 10.1109/LED.2018.2884542

*Vertical transistor
Compared with transistors having a horizontal structure, wherein the drain current flows horizontally, the current flows vertically in transistors with a vertical structure. The larger cross-sectional area of the current path in vertical transistors allows operation with larger currents. Also, vertical transistors can be used for high voltage operation since the applied voltage when the transistor is off can be absorbed by a drift layer.

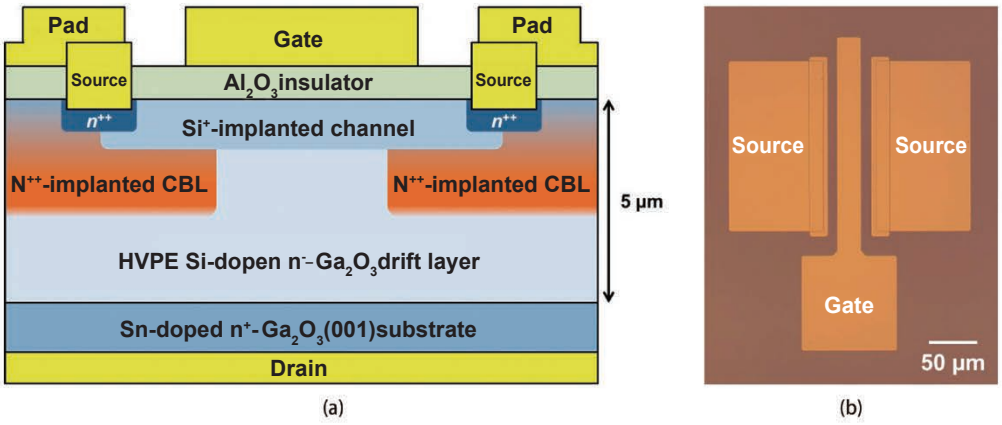


Figure (a) Cross-sectional schematic and (b) plan-view optical micrograph of the vertical Ga_2O_3 MOSFET.

Related press release

- **Successful Development of World's First Vertical Ga_2O_3 Transistor through Low-Cost, Highly-Manufacturable Ion Implantation Doping Process** (released on December 12, 2018 https://www.nict.go.jp/en/press/2018/12/12-1.html)

Cryptographic Implementations
–Achieving both efficiency and security–

Takuya HAYASHI

Ph.D. (Functional Mathematics)
Senior Researcher, Security Fundamentals Laboratory,
Cybersecurity Research Institute

Cryptosystems such as key exchange and digital signatures produce value by providing confidentiality and integrity to services such as secure mutual authentication in e-commerce. Cryptographic processing can be slow, and creating a bottleneck for services is clearly undesirable; therefore, improving the efficiency of cryptographic primitives is a critical issue. There are various ways to improve efficiency, such as selecting arithmetic algorithms and optimizing cryptographic parameters depending on cryptographic primitives, and making architecture-dependent optimizations by coding with low-level languages such as assembly, so it is necessary to combine these approaches appropriately to maximize the efficiency.

Taking the perspective of an attacker is also important to implement cryptographic primitives securely. Recently, it has been necessary to implement cryptographic processing such that there is no correlation between computing time and secret information, such as the secret keys, to thwart side-channel attacks that exploit such correlation to reveal secrets. A naive implementation of a countermeasure can also result in slower processing, so countermeasures must be implemented by designing new arithmetic algorithms and implementation techniques which affect the efficiency as little as possible.

In research leading to my degree, I focused on breaking cryptosystems, looking at cryptographic primitives from an attacker's perspective. When breaking cryptosystems, it is necessary to understand the cryptographic primitives and algorithms for breaking cryptosystems theoretically, and also needed to implement these algorithms efficiently. As I mentioned earlier, this knowledge is also important for cryptographic implementations. Recently, in addition to research on breaking cryptosystems, I have been using this knowledge for research on cryptographic implementations.

One thing that I have been focusing on recently is efficient implementations of homomorphic encryption, which is a fundamental technology used in privacy-preserving data mining (See pp. 4-5 and 8-9 in this issue). Homomorphic encryption requires more computation than conventional cryptosystems, so improving efficiency is particularly important. Although there are other researchers in the world working on this topic, it is still necessary to improve efficiency further to apply it in various services.

An interesting aspect of cryptographic implementations is that implementations should not make trade-offs between efficiency and security but must achieve both of them simultaneously. To accomplish both goals, it is important to use knowledge of efficient implementations and also take the perspective of an attacker. Going back and forth between mathematics and implementation, I am always thinking about how to implement the cryptographic primitives and whether there are flaws in the implementation.

Q&As

Q: What do you like the most about being a researcher?

A: I think being a researcher is one of the few professions that you can enjoy with the most advanced technology in the world and also (a little bit) advance the leading edge of technology in some sense. Though, of course, there will be some hardship in developing/advancing the technologies…

Q: What are you currently interested in outside of your research?

A: The weather is getting cold these days, so I'm enjoying nabe (Japanese hot-pot) for dinner. I'm not good at cooking, but nabe will yield an excellent dish by just adding vegetables, meat and/or fish to the pot.

Q: What advice would you like to pass on to people aspiring to be researchers?

A: I recommend creating a network with as many different people as you can, through opportunities such as conferences. Besides increasing your friends, they may help you in various ways later on.

Biography

1985 Born in Sapporo
2008 Graduated in Media Architecture at Future University Hakodate
2010 Completed master's degree in Systems Information Science at Graduate School of Systems Information and Science, Future University Hakodate
2013 Completed doctoral degree in Functional Mathematics at Graduate School of Mathematics, Kyushu University. Then, a postdoctoral researcher at this university.
2014 Joined the NICT Security Fundamentals Laboratory
2017 Specially appointed assistant professor for Faculty of Engineering, Kobe University
2018 Current position (2019 Senior Researcher)

Awards, etc.

2012 IPSJ Kiyasu Special Industrial Achievement Award
12th DOCOMO Mobile Science Award, Advanced Technology Division, Excellence Award

In this column "NICT's Challengers" you will find a profile of NICT staff tackling a variety of things.

NICT NEWS 2019 No.2 Vol. 474
Published by **Public Relations Department, National Institute of Information and Communications Technology**
Issue date: Mar. 2019 (bimonthly)

4-2-1 Nukui-Kitamachi, Koganei, Tokyo
184-8795, Japan
TEL: +81-42-327-5392 FAX: +81-42-327-7587

URL: https://www.nict.go.jp/
@NICT_Publicity
#NICT

Subscription applications accepted by
E-mail or on the Web site.

ISSN 2187-4050 (Online)