Cutting-edge Research on Cryptography Theory in Response to Changes in Computing Environments

Masayuki Abe, Yuuki Tokunaga, Mehdi Tibouchi, Ryo Nishimaki, and Keita Xagawa

Abstract

Triggered by the case that a government employee successfully forged a bank card in 1982, NTT established the first research group on cryptography around the same time. NTT Secure Platform Laboratories has contributed to building a firm theoretical ground for cryptography while developing cryptographic technologies that can respond to the changes in evolving communication and computing environments. In this article, research activities of NTT Secure Platform Laboratories on cryptography and information security technologies—in preparation for the emergence of rapidly developing quantum computers—are discussed.

Keywords: quantum computer, post-quantum cryptography, attribute-based encryption

1. Background

The notion of security in cryptography is defined on the basis of the amount of computational resources (i.e., memory and computational speed) that an attacker can have. In the 1990s, when the Internet began to spread, a public key of Rivest–Shamir–Adleman (RSA) encryption, having about 512 bits, was considered secure. In 2001, when the Electronic Signature Law was enacted in Japan, public keys are required to be 1024 bits, and in the revision to that law, which has been being considered since 2008, they will soon be required to be at least 2048 bits.

Many cryptosystems are moving toward the more efficient *elliptic curve* approach. More advanced public key cryptography (such as identity-based cryptography based on pairing groups over elliptic curves), efficient digital signature schemes protecting privacy of the signer, and highly efficient non-interactive zero-knowledge proof systems have been developed. Cryptography naturally has the ability to control access to information through key-management methods. Regarding conventional cryptographic communication, the sender and receiver of information have a one-to-one relation. In the more complex scenario of encrypted communication, however, encrypted data are stored in the cloud and the embedded information is accessible by multiple recipients satisfying the condition specified by the sender. Some advanced cryptosystems, such as attribute-based encryption (ABE), have been developed for such purposes.

It has been shown that if a general-purpose quantum computer is developed that can handle a large number of qubits with sufficient precision so that Shor's algorithm can be executed, it will be able to break efficient public-key cryptographic schemes, such as RSA encryption and Diffie–Hellman key exchange, currently in wide use [1]. Even if such advanced quantum computers do not become viable for several decades, it is necessary to develop cryptographic techniques that are secure against the threat such computers pose—so-called *post-quantum cryptography*—without waiting for quantum computers to become a reality. In fact, much research and development (R&D) and standardization of post-quantum cryptography is already underway. As well as the motive of the providers of cryptographic systems, there are two practical reasons for such effort. The first is that a new encryption method takes a very long time from development to deployment in the real world. That is, updating a system that appears to be working to a new system that is not compatible is not something that every user can do in a short time. The other reason is the concern that current privacy will be compromised by future advances in attack techniques in a manner called *long-term security compromise*. It is a concern that even encrypted communications may be intercepted and stored for long periods, and their content may be exposed by quantum computers created in the future. In other words, for content that would be difficult to leak after several decades, a quantum-computer attack is a threat that must be addressed in the present. Post-quantum cryptography is not executed on a quantum computer; instead, it is executed on current computers. It is therefore necessary to consider security in terms of post-quantum cryptography in the current computer environment.

The activities of NTT Secure Platform Laboratories (SC Labs) regarding quantum information processing technology are first described. The latest topics concerning post-quantum cryptography are then discussed. Finally, SC Labs' latest research results on ABE, which is one of the functions of conventional public-key cryptography, are presented.

2. Quantum information processing

2.1 Quantum information processing technology at SC Labs

In October 2019, news circulated that quantum computers had finally achieved "quantum supremacy," namely, capabilities beyond those of conventional computers [2]. SC Labs has been researching and developing quantum computers that process information on the basis of the principles of quantum mechanics.

Quantum computers implemented to date can still only process data on the order of tens of qubits, and many issues on how to achieve scalability remain unresolved. In other words, R&D on how to construct quantum computers and achieve scalability is the litmus test for verifying the current security level of cryptography. Quantum information technology has also created new security technologies. The properties of quantum states differ from those of ordinary data, for example, a state is destroyed when measured unnecessarily, and it cannot be copied. By making good use of these different properties, new security technologies can be developed.

2.2 Path to developing the quantum computer

The foremost barrier to constructing quantum computers is their vulnerability to errors. Regarding qubits, it is difficult to reduce errors in the manner of digital data, which is the main information-processing unit used today; accordingly, if the scale of a quantum computer is increased, the computational result will be buried in the noise, and correct calculation will become difficult. The only solution to this problem thus far has been *quantum error correction*. When quantum error correction is applied, if the control of qubits is achieved below a specific error rate within a technically feasible range, the logical error rate of the quantum information in the encoded quantum state can be reduced, and the handling capability of the error can be extended.

Another issue is to increase the size of the qubit. Increasing the scale of qubits while accurately controlling individual qubits at high speed is contradictory and has rarely been achieved with unstable quantum states. A breakthrough in quantum engineering is expected to increase the number of qubits while maintaining accuracy of controlling individual qubits. At SC Labs, we (a subgroup) are participating in the Ministry of Education, Culture, Sports, Science and Technology (MEXT)'s Q-LEAP project, which is involved in the development of superconducting quantum computers. As part of Q-LEAP, we are working on advanced control technology that enables quantum error correction and R&D aiming at expanding the scale of quantum computers.

3. Toward quantum-secure networks

An example of a new security technology that uses quantum information processing is *quantum cryptography* (or *quantum key distribution*). Eavesdropping can be detected if the quantum state is destroyed when measured unnecessarily, so, secure key distribution is possible in principle. However, there are three problems with the current technology: (i) vulnerability to loss, (ii) practically limited communication distance (up to about 100 km), and (iii) inability of networking. The solution to these problems is using a *quantum repeater*, which makes it possible to control quantum states of light and matter with high precision and to correct quantum errors in a manner that can withstand losses. In fact, a quantum repeater is therefore a technology that is fairly comparable with constructing small to medium-scale quantum computers. To implement a quantum repeater, we have to conduct almost the same R&D as that for implementing quantum computers. At SC Labs, we are working on controlling the quantum states of light and atoms with the high precision required for quantum repeaters while increasing the scale of the quantum states that can be handled. SC Labs is also participating in the CREST project of the Japan Science and Technology Agency (JST), in which we are engaged in R&D using cavity quantum electrodynamics—which enables high-precision interaction between light and atoms.

4. Toward quantum-resistant (post-quantum) cryptography: Secure implementation and contribution to standardization

In addition to conventional cryptographic techniques such as RSA cryptography and elliptic-curve cryptography, post-quantum cryptography, which is considered to be durable against quantum cryptography, has been studied for decades. For the most basic functions, namely, encryption and signature schemes, theoretical schemes based on problems that are difficult to solve with quantum computers have been known for a long time. However, the performance of these schemes, such as processing speed and communication traffic, is remarkably inferior to that of RSA cryptography and elliptic-curve cryptography, so these schemes have been determined impractical, and implementations of post-quantum cryptography are scarce.

As the emergence of quantum computers has recently become a visible threat, this threat has finally started to be seriously considered. Proposing and implementing faster and higher-performance post-quantum-cryptography technologies have become important research topics. In particular, in *lattice-based cryptography*, which is regarded as promising for post-quantum cryptography, new schemes have been proposed and implemented by adding several ideas and optimizations to conventional schemes that have strong security foundations, and they have demonstrated performance comparable to that of RSA encryption. Implementation experiments on virtual private network software have also begun [3].

While theoretical security foundations have been thoroughly investigated, vulnerabilities concerning implementation (such as side-channel attacks and fault attacks) have not been considered. Moreover, efficient new schemes often require *sampling from discrete Gaussians distributions* and *rejection sampling*, which are *not* used in the conventional cryptographic schemes; thus, secure implementations of them are new challenges. To address these implementation issues, SC Labs assessed security against implementation attacks, especially against the lattice-based signature scheme, and discovered numerous vulnerabilities [4, 5, 6, 7, 8]. For example, in a previous study [4], which targeted multiple implementations of the BLISS scheme, a fast lattice-based signature, we showed that measuring power consumption and processing time when a signature is generated makes it possible to completely recover the secret key by using algebra and number theory. We are proposing countermeasures and implementation schemes to overcome the above-mentioned vulnerabilities and are verifying their security. We also proposed and implemented lattice-based signature schemes that provide strong security against implementation attacks while maintaining the highest level of performance [9, 10, 11].

The above-mentioned studies had a significant impact on the ongoing post-quantum cryptography standardization process launched by the National Institute of Standards and Technology (NIST) in 2016 (hereafter, NIST Post-Quantum Cryptography (PQC) standardization). In particular, the implementation vulnerabilities of the BLISS scheme [4] are being considered as implementation threats in the design policy of a candidate called Dilithium. According to reported results [4], almost all lattice-based signatures in the NIST PQC standardization avoided sampling from discrete Gaussian distribution. Even after the start of the NIST PQC standardization, SC Labs contributed to the successful results regarding safe implementation of Dilithium and Falcon [6, 8, 10, 11] and to completely defeating and eliminating a scheme with weak security foundations [12].

5. Recent topic 1: Quantum computers and cryptography

5.1 Method for evaluating security of symmetric-key cryptography using a quantum computer

A general-purpose quantum algorithm for secret-key cryptography is not currently known. Therefore, attacks that apply the Grover algorithm or the quantum-random-walk algorithm are known to be best. At SC Labs, we developed methods for evaluating security based on analyzing the internal details of symmetric-key cryptographic schemes. For example, we improved the multi-collision-finding algorithm of hash functions, which was achieved in collaboration with NTT Communication Science Laboratories [13].

Furthermore, anticipating the availability of quantum computers in the future, some adversaries may be now eavesdropping and collecting information. We are also devising safety-assessment methods for estimating the effect of such adversaries [14, 15].

5.2 Technique for security proofs in the presence of quantum computers

Many previous security proofs did not assume that an adversary has a quantum computer. As a result, even if the security is proven, there is a chance that the adversary can breach the security by using a quantum computer. Under such a circumstance, many security-proof techniques that take into account quantum computers have been developed since 2010. SC Labs is also researching such security proofs. Some examples of this research are methods for enhancing the security of post-quantum public-key cryptography [16, 17], quantum security of hash functions [18], quantum security of symmetric-key cryptography with the Feistel structure [19], and general lower-bound evaluation of attacks on hash functions when precomputation is allowed [20].

6. Recent topic 2: ABE

Although public-key cryptography can be divided into several main themes, this article focuses on one, *attribute-based cryptography with practical efficiency*. For public-key cryptography, a sender of information encrypts the information with a recipient's public key into a ciphertext and only the recipient who has the corresponding private key can decipher the ciphertext to access the information. ABE schemes allow the sender to freely specify the recipient without limiting the information to a single recipient. More specifically, a policy is embedded in the ciphertext, and attributes of the recipient are embedded in the secret key. A recipient can then receive information only if their attributes match the policy in the ciphertext. Therefore, the logic is embedded in the ciphertext and secret key, and it is possible to restrict information exchange.

Many ABE schemes have been proposed; nevertheless, they are insufficient in terms of implementing them in actual systems. One problem is scalability of attributes. Many ABEs require that all attributes used are determined at the initialization of a system, that is, we can thereafter no longer add attributes. To attain scalability, it is desirable to be able to add attributes at any time. Another problem is data size. In the case of some methods, the size of the ciphertext increases in proportion to the size of the embedded policy and number of attributes used. This dependence has been undesirable because it occupies storage. Therefore, various performance criteria have been considered in regard to actual use; however, an ABE scheme that reaches practically desirable levels in relation to all those criteria had not yet been proposed. Given this situation, we developed an ABE scheme that possesses all the properties desirable in terms of practicality.

References

[1] P. W. Shor, "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM J. Comput., Vol. 26, No. 5, pp. 1484–1509, 1997.

[2] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum Supremacy Using a Programmable Superconducting Processor," Nature, Vol. 574, pp. 505–510, 2019.

[3] Post-quantum Cryptography VPN, https://github.com/Microsoft/PQCrypto-VPN

[4] T. Espitau, P.-A. Fouque, B. Gerard, and M. Tibouchi, "Side-channel Attacks on BLISS Lattice-based Signatures: Exploiting Branch Tracing against strongSwan and Electromagnetic Emanations in Microcontrollers," Proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1857–1874, Dallas, Texas, USA, Oct. 2017.

[5] J. Bootle, C. Delaplace, T. Espitau, P.-A. Fouque, and M. Tibouchi, "LWE Without Modular Reduction and Improved Side-channel Attacks against BLISS," Advances in Cryptology, ASIACRYPT 2018, LNCS, Vol. 11272, pp. 494–524, Springer, 2018.

[6] T. Espitau, P.-A. Fouque, B. Gérard, and M. Tibouchi, "Loop-abort Faults on Lattice-based Signature Schemes and Key Exchange Protocols," IEEE Trans. Comput., Vol. 67, No. 11, pp. 1535–1549, 2018.

[7] M. Tibouchi and A. Wallet, "One Bit Is All It Takes: A Devastating Timing Attack on BLISS's Non-constant Time Sign Flips," Journal of Mathematical Cryptology, Special Issue on MathCrypt 2019, De Gruyter, to appear.

[8] P.-A. Fouque, P. Kirchner, M. Tibouchi, A. Wallet, and Y. Yu, "Uprooting the Falcon Tree?: How to Recover Secret Keys from Gram-Schmidt Norms," IACR Cryptology ePrint Archive, Report 2019/1180, 2019.

[9] G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, B. Grégoire, M. Rossi, and M. Tibouchi, "Masking the GLP Lattice-based Signature Scheme at Any Order," Advances in Cryptology – EUROCRYPT 2018, LNCS,

Vol. 10821, pp. 354–384, Springer, 2018.

[10] P.-A. Fouque, B. Gérard, V. Migliore, and M. Tibouchi, "Masking Dilithium: Efficient Implementation and Side-channel Evaluation," Applied Cryptography and Network Security, ACNS 2019, LNCS, Vol. 11464, pp. 344–362, Springer, 2019.

[11] G. Barthe, S. Belaid, T. Espitau, P.-A. Fouque, M. Rossi, and M. Tibouchi, "GALACTICS: Gaussian Sampling for Lattice-based Constant-time Implementation of Cryptographic Signatures, Revisited," Proc. of ACM CCS 2019, pp. 2147–2164, London, UK, Nov. 2019.

[12] J. Bootle, M. Tibouchi, and K. Xagawa, "Cryptanalysis of Compact-LWE," Topics in Cryptology – CT-RSA 2018, LNCS, Vol. 10808, pp. 80–97, Springer, 2018.

[13] A. Hosoyamada, Y. Sasaki, S. Tani, and K. Xagawa, "Improved Quantum Multicollision-finding Algorithm," Post-Quantum Cryptography, PQCrypto 2019, LNCS, Vol. 11505, pp. 350–367, Springer, 2019.

[14] A. Hosoyamada and Y. Sasaki, "Cryptanalysis against Symmetric-key Schemes with Online Classical Queries and Offline Quantum Computations," Topics in Cryptology, CT-RSA 2018, LNCS, Vol. 10808, pp. 198–218, Springer, 2018.

[15] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher, "Quantum Attacks without Superposition Queries: The Offline Simon's Algorithm," Advances in Cryptology, ASIACRYPT 2019, LNCS, Vol. 11921, pp 552–583, Springer, 2019.

[16] T. Saito, K. Xagawa, and T. Yamakawa, "Tightly-secure Key-encapsulation Mechanism in the Quantum Random Oracle Model," Advances in Cryptology, EUROCRYPT 2018, Part III, LNCS, Vol. 10822, pp. 520–551, 2018.

[17] K. Xagawa and T. Yamakawa, "(Tightly) QCCA-secure Key-encapsulation Mechanism in the Quantum Random Oracle Model," Post-Quantum Cryptography, PQCrypto 2019, LNCS, Vol. 11505, pp. 249–268, Springer, 2019.

[18] A. Hosoyamada and K. Yasuda, "Building Quantum-one-way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions," Advances in Cryptology, ASIACRYPT 2018, Part I, LNCS, Vol. 11272, pp. 275–304, 2018.

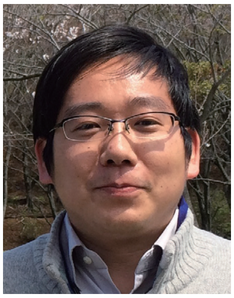
[19] A. Hosoyamada and T. Iwata, "4-Round Luby-Rackoff Construction is a qPRP," Advances in Cryptology, ASIACRYPT 2019, LNCS, Vol. 11921, pp. 145–174, Springer, 2019.

[20] M. Hhan, K. Xagawa, and T. Yamakawa, "Quantum Random Oracle Model with Auxiliary Input," Advances in Cryptology, ASIACRYPT 2019, LNCS, Vol. 11921, pp 584–614, Springer, 2019.

Masayuki Abe

Senior Distinguished Researcher, NTT Secure Platform Laboratories.

He received a Ph.D. from the University of Tokyo in 2002 and has been at NTT since 1992. Currently, he is a senior distinguished research scientist at NTT Secure Platform Laboratories. He served as a program chair for CT-RSA'07, ACM ASIACCS'08, and Asiacrypt'10. His research interests include digital signatures, public-key encryption, and efficient instantiation of cryptographic protocols.



Yuuki Tokunaga

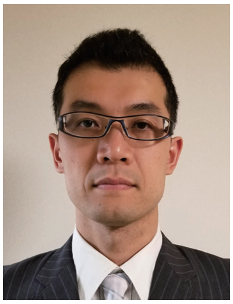
Distinguished Researcher, NTT Secure Platform Laboratories.

He received a Ph.D. in science from Osaka University in 2007. He joined NTT in 2001, where he has been conducting research toward the realization of fault-tolerant universal quantum computing and long-distance secure quantum network.

Mehdi Tibouchi

Distinguished Researcher, NTT Secure Platform Laboratories.

An alumni of The École Normale Supérieure, Paris, France. He joined NTT in 2011 after obtaining his Ph.D. in computer science from Univ. Paris VII and Univ. Luxembourg. He is currently a distinguished researcher at NTT Secure Platform Laboratories. His research interests cover various mathematical aspects of public-key cryptography and cryptanalysis.



Ryo Nishimaki

Distinguished Researcher, Data Security Project, NTT Secure Platform Laboratories.

He received a B.E. and M.I. from Kyoto University and a D.S. from Tokyo Institute of Technology in 2005, 2007, and 2010. He joined NTT in 2007, where he has been focusing on design and foundation of cryptography. He is currently researching cryptography and information security at NTT Secure Platform Laboratories.

Keita Xagawa

Scientist, NTT Secure Platform Laboratories.

He received a B.S. from Kyoto University and an M.S. and D.S. from Tokyo Institute of Technology in 2005, 2007, and 2010. He joined NTT in 2010, where he has been focusing on algebraic algorithms and provable security in cryptography. He is currently researching cryptography and information security at NTT Secure Platform Laboratories.