Research Trends in Post-quantum Cryptography

Keita Xagawa

Abstract

The growing recognition that quantum computers are soon to be a reality is driving research into post-quantum cryptography. This article introduces the Post-Quantum Cryptography Standardization project of the National Institute of Standards and Technology (NIST) in the United States, which is playing a core role in the research and development of post-quantum cryptography, and introduces NTT initiatives and independent research related to that project.

Keywords: cryptographic technology, post-quantum security, quantum computer

1. Post-quantum cryptographic technology

Today, a great deal of highly confidential information such as personal data and credit card numbers is being exchanged on the Internet. For this reason, cryptographic systems such as symmetric-key cryptography and public-key cryptography are being used to conceal the contents of such transmissions. In addition, authentication technologies such as digital signatures and message authentication codes (MACs) are being used to authenticate the other party and the content of the received message. Certain algorithms have found widespread use in public-key cryptography and digital signatures, namely cryptographic algorithms based on the difficulty of the factorization problem (RSA (Rivest-Shamir-Adleman) encryption, RSA signatures, etc.) and those based on the difficulty of the discrete logarithm problem (Diffie–Hellman key exchange, elliptic-curve Diffie–Hellman key exchange, Digital Signature Algorithm (DSA), etc.).

In 1994, Peter Shor, then of Bell Laboratories, proposed efficient algorithms using a quantum computer for solving these two problems. Consequently, if a quantum computer that can perform large-scale calculations in a stable manner can be built, cryptographic algorithms that are now in widespread use will no longer be secure. This is why the research, development, and standardization of cryptographic algorithms that a quantum computer cannot break or tamper with have become quite active as efforts continue to successfully develop a quantum computer. Within public-key cryptographic technology, cryptographic algorithms that have been designed based on problems for which quantum computers are considered to be weak in solving are referred to as post-quantum (public-key) cryptography.

2. Standardization trends in post-quantum cryptography

On the question of whether it is necessary to start a migration to post-quantum cryptographic algorithms, we refer to the formula proposed by Michele Mosca, co-founder and deputy director of the Institute for Quantum Computing, University of Waterloo, Ontario, Canada, as described below. Let us define x, y, and z as follows:

- x = number of years desired to maintain the security of generated information
- y = number of years needed to migrate to post-quantum cryptographic algorithms (research and development, standardization, and dissemination)
- z = number of years until a large-scale quantum computer is built

If x + y > z, ciphertext created after y years based on the thinking that “I want to keep this information secret for at least x years” may be cracked by a quantum

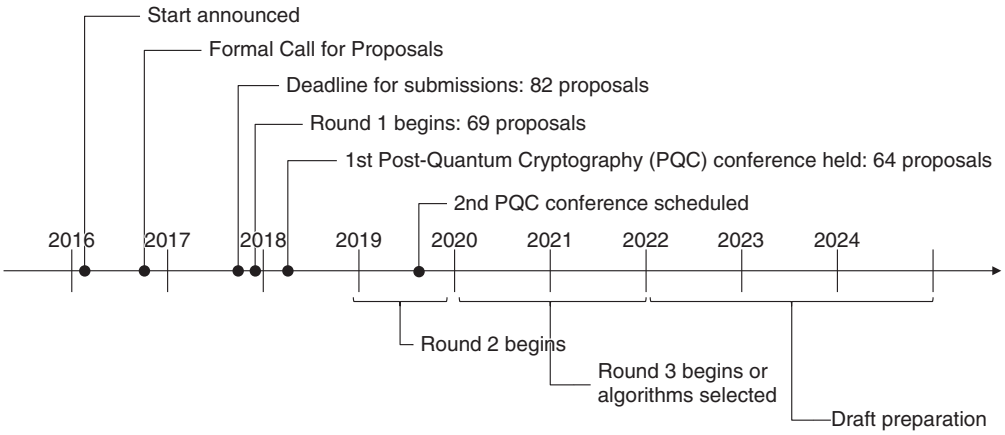

Fig. 1. Timeline of NIST project.

computer in less than x years. Accordingly, if it is thought that x + y > z is true at the present time, there is a need to study closely the standardization of and migration to post-quantum cryptographic technology.

Under the assumption that z number of years from today's state of quantum computer development is likely to be within a realistic range, organizations and standardization bodies in various countries are moving forward with migration studies, as outlined below.

- In Japan, the Cryptography Research and Evaluation Committees (CRYPTREC)* issued a report in 2014 on post-quantum cryptography titled "Survey on the Difficulty of Lattice Problems, etc."
- In the United States, the National Institute of Standards and Technology (NIST) began holding workshops in spring 2015 and announced in 2016 that it would commence standardization activities toward post-quantum public-key cryptographic techniques.
- Also in the United States, the National Security Agency (NSA) declared in August 2015 its intention to migrate its Suite B, the set of cryptographic algorithms for protecting classified information, to post-quantum cryptographic algorithms in the not too distant future.
- The European Telecommunications Standards Institute (ETSI) has been holding annual workshops on quantum cryptography and post-quantum cryptography since 2013.
- The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have been holding study periods on post-quantum cryptography since 2015.
- The Internet Engineering Task Force (IETF) as well is overseeing a post-quantum signature project and is beginning to release results as request for comments (RFCs) (e.g., RFC 8391: XMSS: eXtended Merkle Signature Scheme).

Among these activities, we introduce here the NIST Post-Quantum Cryptography Standardization project, which is having a major impact on cryptographic technology standardization around the world.

3. NIST Post-Quantum Cryptography Standardization Project

The NIST Post-Quantum Cryptography Standardization Project began in earnest in 2016 with the aim of selecting and standardizing post-quantum cryptographic algorithms in the three categories of digital signature, public-key encryption, and key establishment.

The timeline for this project is summarized below (**Fig. 1**).

- February 2016: Announcement of the start of the Post-Quantum Cryptography Standardization Project
- August 2016: Release of NISTIR 8105, Report on Post-Quantum Cryptography
- August 2016: RFCs on Submission Requirements and Evaluation Criteria
- December 2016: Formal Call for Proposals

* CRYPTREC: A project established to evaluate and monitor the security of e-Government recommended ciphers and to survey and study appropriate implementation and operation methods of cryptographic techniques.

- November 2017: Deadline for submissions
- December 2017: Examination of documents and forms; Round 1 begins
- April 2018: First Post-Quantum Cryptography (PQC) Standardization Conference
- 2018/2019: Round 2 begins
- August 2019: Second PQC Standardization Conference (plan)
- 2020/2021: Round 3 begins or algorithms to be selected
- 2022/2024: Draft preparation to be completed

A total of 82 proposals were submitted by the deadline in November 2017; of these, 23 concerned digital signatures and 59 concerned encryption and key-encapsulation mechanisms. After an examination of documents and forms was conducted, Round 1 began in December 2017, at which time 69 proposals remained. However, 5 proposals were later withdrawn, resulting in a total of 64 proposals at present—19 for digital signatures and 45 for encryption and key-encapsulation mechanisms.

As mentioned above, the results of examining documents and forms left 69 candidate algorithms for Round 1. These candidates are not necessarily secure simply by reaching Round 1.

Immediately after the release of Round 1 candidates, lively discussions took place on the security of each method via the NIST pqc mailing list.

Among these candidates, many were shown to be breakable as summarized below.

- Guess Again (encryption, other)
- RaCoSS (signature, code)
- RVB (encryption, other) → withdrawn
- HK17 (encryption, other) → withdrawn
- CFPKM (encryption, multivariate polynomials)
- SRTPI (encryption, multivariate polynomials) → withdrawn
- Edon-K (encryption, code) → withdrawn
- Compact LWE (encryption, lattice)
- WalnutDSA (encryption, other)
- RankSign (signature, code) → withdrawn

It should be kept in mind that security evaluation techniques are expected to be improved going forward to Round 2.

4. NTT initiatives

NTT did not submit an original algorithm to these NIST Post-Quantum Cryptography Standardization activities. However, NTT is participating by making proposals for security enhancement techniques and security evaluation from a third-party standpoint and is working with other project members to ensure that suitable algorithms can be selected.

Furthermore, though the NIST Post-Quantum Cryptography Standardization Project is focused only on post-quantum public-key cryptographic algorithms, NTT is independently researching post-quantum symmetric-key cryptography as well.

4.1 Security enhancement technique

For secure communications to be carried out in the real world, public-key encryption algorithms must provide a level of security that is strong enough not only to conceal the message itself but also to prevent messages from being tampered with. Technically speaking, this is called chosen-ciphertext attack (CCA) security. At present, CCA security is considered to be an essential requirement for the realistic use of public-key encryption algorithms.

In this regard, techniques for converting a public-key encryption algorithm without CCA security to a public-key encryption algorithm with CCA security have been researched for some time, but it was not until 2010 that research began in order to determine whether such techniques were secure enough to counter attacks using a quantum computer. It was found that these techniques could indeed be effective against quantum computers but only with a drop in efficiency. However, no security enhancement technique that was effective against quantum computers without sacrificing efficiency was known to exist.

With this being the case, NTT developed a new technique that improves security by converting a post-quantum public-key encryption algorithm without CCA security to a post-quantum public-key encryption algorithm with CCA security [1].

This development makes it possible to configure a post-quantum public-key encryption algorithm according to the highest global standards with high efficiency. In addition, the technique has broad utility, enabling it to be applied to a variety of existing post-quantum public-key cryptographic schemes. It was found that it could be applied to at least seven of the candidate algorithms in the NIST Post-Quantum Cryptography Standardization Project.

The use of post-quantum public-key encryption algorithms based on this technology will enable cryptographic communications at about the same load as existing methods even in the post-quantum era.

4.2 Security evaluation from the outside

A cryptographic algorithm called Giophantus is one of the 69 candidate algorithms evaluated in the

NIST standardization project. This algorithm was originally presented in a paper under the name Indeterminate Equation Cryptosystem (IEC). The security of this scheme, while proven to be secure, is dependent on the difficulty of a certain problem. In this regard, large size parameters are required to ensure that the underlying problem is difficult. However, since IEC was designed so that the key size and ciphertext length would be short, the underlying problem with small size parameters was an issue.

Against this background, we proposed a new attack technique that could degrade security for small size parameters [2]. The results of an experiment using this attack technique revealed that practical cryptanalysis could be performed in 30–40 seconds on a desktop personal computer. As a result of this study, parameters for the Giophantus version of IEC submitted to NIST were significantly revised.

4.3 Post-quantum symmetric-key cryptographic technology

(1) Security evaluation techniques

A general-purpose quantum algorithm for attacking symmetric-key cryptography is presently unknown. Consequently, an attack that applies computer scientist L. K. Grover's algorithm for searching a database is currently known to be the most effective. For this reason, quantum attack techniques surpassing the Grover algorithm are being devised by analyzing in detail the inner workings of symmetric-key cryptography, and security evaluations using these techniques are being performed. At NTT, we have obtained results surpassing those of existing research by combining meet-in-the-middle attacks and quantum algorithms [3, 4].

It is also known that security can break down for some symmetric-key ciphers and MACs in cases where the attacker can access a cryptographic algorithm or MAC algorithm in a quantum manner. NTT has also been researching attacks of this kind and has shown that some symmetric-key ciphers can be broken by quantum related-key attacks [5].

(2) Security-proving technique

As described above, it is extremely important that the security of symmetric-key cryptography be assessed and proven considering the existence of attackers that instigate quantum-type accesses. NTT has developed a technique that proves the post-quantum security of hash functions even when attackers carry out quantum queries [6].

5. Future development

We plan to create a portfolio of security enhancement and security evaluation techniques and to continue studying the development and deployment of secure cryptographic communication technologies even after the successful development of quantum computers.

References

[1] T. Saito, K. Xagawa, and T. Yamakawa, "Tightly-secure Key-encapsulation Mechanism in the Quantum Random Oracle Model," Proc. of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018), Part III, Lecture Notes in Computer Science (LNCS), Vol. 10822, pp. 520–551, 2018.

[2] K. Xagawa, "Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017," Proc. of the 9th International Conference on Post-Quantum Cryptography (PQCrypto 2018), LNCS, Vol. 10786, pp. 142–161, 2018.

[3] A. Hosoyamada and Y. Sasaki, "Cryptanalysis against Symmetric-key Schemes with Online Classical Queries and Offline Quantum Computations," Proc. of CT-RSA (Cryptographers' Track at the RSA Conference) 2018, LNCS, Vol. 10808, pp. 198–218, 2018.

[4] A. Hosoyamada and Y. Sasaki, "Quantum Demiric-Selçuk Meet-in-the-middle Attacks: Applications to 6-Round Generic Feistel Constructions," Proc. of the 11th Conference on Security and Cryptography for Networks (SCN 2018), LNCS, Vol. 11035, pp. 386–403, 2018.

[5] A. Hosoyamada and K. Aoki, "On Quantum Related-key Attacks on Iterated Even-Mansour Ciphers," Proc. of the 12th International Workshop on Security (IWSEC2017), LNCS, Vol. 10418, pp. 3–18, 2017.

[6] A. Hosoyamada and K. Yasuda, "Building Quantum-one-way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions," Proc. of the 24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018), Part I, LNCS, Vol. 11272, pp. 275–304, 2018.

Keita Xagawa
Scientist, Data Security Project, 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. His research work focuses on algebraic algorithms and provable security in cryptography. He is presently researching cryptography and information security at NTT Secure Platform Laboratories.