Special Issue 1

Security in the Era of Quantum Computers : Developments in Post-Quantum Cryptography

Tsuyoshi TAKAGI

abstract

RSA cryptosystem and elliptic curve cryptography, which are currently widely used, are known to be facing the risk of being compromised by a quantum computer. Research on post-quantum cryptography (PQC) has been actively conducted as a study of cryptographic technology that can be used safely even in the era of quantum computers. It is particularly worth mentioning that the National Institute of Standards and Technology (NIST) of the United States started working on a PQC standardization project in 2016 and released information about the cryptosystems that they selected as standard schemes in July 2022. As newly standardized cryptosystems, they selected an encryption scheme called CRYSTALS-Kyber as a choice in the category of lattice-based encryption, CRYSTALS-Dilithium and FALCON as choices in the category of lattice-based digital signatures, and SPHINCS+ as a choice in the category of hash-based signature. This paper provides an overview of the NIST's PQC standardization project and discusses the security and processing performance of these newly selected standard schemes.

Keywords : post-quantum cryptography, lattice-based cryptography, hash-based signature, code-based cryptography, multivariate polynomial cryptography

1. Introduction

The RSA cryptosystem, which is widely used in public key cryptosystems, relies on the difficulty of solving prime factorization problems as the basis for its security. Research on efficiently solving the prime factorization problem has been actively conducted with various attempts that include large-scale computer experiments. The number field sieve is currently known as the most asymptotically fastest algorithm, and its computation time requires sub-exponential to the bit-length of the composite number N. Factorizing a 2048-bit composite number used today into prime factors by the number field sieve, for example, is expected to require a computational time that corresponds to the fully dedicated use of a 10^{27} FLOPS supercomputer for a year. Since the Linpack performance of the currently fastest supercomputer is about 10^{18} FLOPS, 2048-bit prime factorization will take several decades or more even after assuming Moore's law [(1)].

However, in 1994, Shor presented an algorithm that

Tsuyoshi TAKAGI Member (Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Tokyo 113-8656 Japan).
E-mail : takagi@mist.i.u-tokyo.ac.jp
THE JOURNAL OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS Vol.106 No.11 pp.(1)-(6) November 2023

could be used to perform prime factorization at high speed with a quantum computer[2]. The computational time of the Shor's algorithm is polynomial to the bit-length of the composite number N, which means its computational speed is exponentially faster than what could be achieved by the number field sieve (Fig. 1). In other words, when a large-scale quantum computer is used, increasing the bit-length of the composite number N does not significantly increase the difficulty of the prime factorization problem. This presents a state of cryptography being compromised because the RSA cryptosystem can theoretically be broken by a quantum computer.

Moreover, Shor's paper presented another algorithm that could be used with a quantum computer to quickly solve the discrete logarithm problem on which the difficulty of the security of elliptic curve cryptograph had been based. That is to say, when large-scale quantum computers are put to use, the RSA cryptosystem and elliptic curve cryptography that we use today will be compromised. For this reason, active research and development is being conducted on post-quantum cryptography (PQC), which uses mathematical problems that are difficult to solve even with quantum computers.

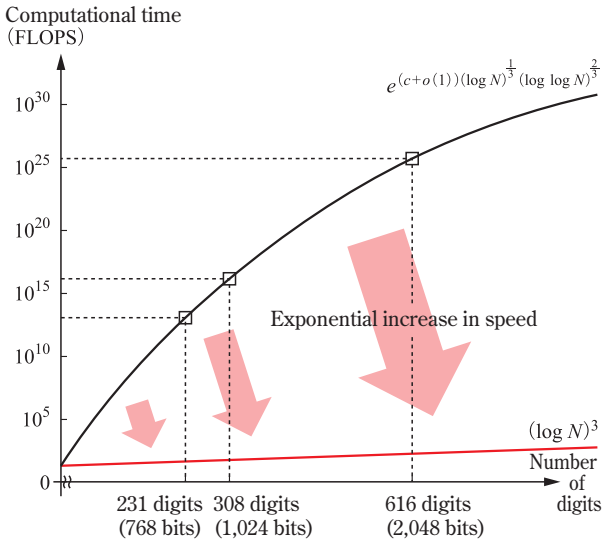

Fig. 1 Computational time achievable by a quantum computer by the use of the Shor's algorithm

2. Post-Quantum Cryptography

Research on public key cryptography that uses computational problems other than prime factorization problems and discrete logarithm problems began already in the second half of the 1970s when the first papers on the RSA cryptosystem were published. In fact, the McEliece cryptosystem, which takes advantage of the properties of error-correcting code, was proposed in 1978. In 1982, the first papers on the Merkle signature, which relies on the onewayness and collision resistance of hash functions, were published. From the first half of the 1980s, research began on multivariate polynomial cryptography, which relies on the difficulty of solving multivariate polynomial problem over a finite field (MQ problem). Furthermore, since the second half of the 1990s, cryptography based on the use of the lattice theory, such as the NTRU cryptosystem, had been proposed, and in 2005, a cryptosystem based on Learning with Errors (LWE) problem was proposed. These are called lattice-based cryptography because their security is based on the difficulty of solving the shortest vector problem (SVP), namely, the difficulty of finding a shortest nonzero vector for a given lattice basis. In addition, papers presenting the idea of isogeny-based cryptography were published in the second half of the 1990s, and in 2006, a cryptography based on the computational difficulty of Ramanujan graphs, which are composed of sequences of isogeny maps of supersingular elliptic curves, was proposed.

These typical mathematical problems are described in NIST-IR 8105 (https://doi.org/10.6028/NIST.IR.8105), a report published by the National Institute of Standards and Technology (NIST) of the United States in 2016, identifying the associated cryptosystems as major candidates for post-quantum cryptography. Table 1 lists these typical post-quantum cryptosystems and the

Table 1 Typical post-quantum cryptography and associated mathematical problems

Cryptography type	Epoch in which its use was proposed	Associated mathematical problems
Code-based cryptography	Since the second half of the 1970s	Problem concerning error correcting code
Hash-based signature	Since the first half of the 1980s	Hash function collision problem
Multivariate polynomial cryptography	Since the first half of the 1980s	Multivariable polynomial problem (MQ problem)
Lattice-based cryptography	Since the second half of the 1990s	Shortest vector problem (SVP)
Isogeny-based cryptography	Since the second half of the 1990s	Isogeny problem

Fig. 2 Group photo from PQCrypto 2016 (international conference)

mathematical problems used in them.

Following these trends, international conferences specifically addressing the subject of post-quantum cryptography (PQCrypto) were started in 2006. Furthermore, in April 2015, the National Institute of Standards and Technology (NIST) of the United States held an NIST Workshop on Cybersecurity in a Post-Quantum World. From 2015, many workshops and international conferences specializing in post-quantum cryptography began to be held. Notably, in February 2016, with the author serving as program chair, the 7th PQCrypto conference (PQCrypto 2016) was held at Nishijin Plaza, Kyushu University[3]. PQCrypto 2016 was eagerly attended by more than 240 participants as NIST presented a plan for the standardization of post-quantum cryptography (Fig. 2).

3. NIST's PQC Standardization Project

In August 2015, the National Security Agency (NSA) of the United States announced a transition to post-quantum cryptography, and then in February 2016, the National Institute of Standards and Technology (NIST) announced a post-quantum cryptography (PQC) standardization plan. PQC standardization by NIST, covering public key cryptographic primitives, involved a public call for proposals on post-quantum versions of public-key encryptions, key exchanges, and digital signatures that have been standardized by SP 800-56 and FIPS PUB 186-4. Information regarding the standardization of post-quantum cryptography by NIST is available on the NIST Post-Quantum Crypto Project homepage (http://nist.gov/pqcrypto).

First, as the standard security evaluation model, *indistinguishability against chosen ciphertext attack* (IND-CCA) was applied to public-key encryptions, and *existential unforgeability against chosen plaintext attack* (EUF-CMA) was applied to digital signatures. The criteria used to evaluate the efficiency of cryptosystems included the sizes of the public key, ciphertext, and signature ; the speed of key generation and of computations involving the use of a public key and a secret key ; and the probability of decryption failure. Furthermore, assuming use in the real world, an evaluation was optionally performed on security against side channel attack, perfect forward secrecy, security against random number reuse attack, and other types of attacks. In addition, the support of a drop-in-replacement was considered desirable so that the newly standardized cryptosystems would be able to easily replace the currently standardized ones. Any party that submitted a proposal to the NIST's PQC standardization project had to attach data from the self-evaluation of security and efficiency performed with respect to the

Table 2 Schemes proposed in response to a public call organized on account of the NIST's PQC standardization project (November 2017)

Lattice-based cryptography (25 proposals) : Compact LWE, CRYSTALS-DILITHIUM, CRYSTALS-KYBER, Ding Key Exchange, DRS, EMBLEM and R. EMBLEM, FALCON, Frodo, HILA5, KINDI, LAC, LIMA, Lizard, LOTUS, NewHope, NTRU-HRSS-KEM, NTRU Prime, NTRUEncrypt, Odd Manhattan, pqNTRUSign, qTESLA, Round2, SABER, Titanium, Three Bears
Code-based cryptography (18 proposals) : BIG QUAKE, BIKE, Classic McEliece, DAGS, Edon-K, HQC, LAKE, LEDAkem, LEDApkc, LOCKER, McNie, NTS-KEM, pqsigRM, QC-MDPC KEM, RaCoSS, Ramstake, RLCE-KEM, RQC
Multivariate polynomial cryptography (10 proposals) : CFPKM, DME, DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow, SRTPI
Hash-based signature (2 proposals) : Gravity-SPHINCS, SPHINCS+
Isogeny-based cryptography (1 proposal) : SIKE
Others (13 proposals) : Giophantus, Guess Again, HK17, Lepton, Mersenne-756839, OKCN/AKCN/CNKE, Ouroboros-R, Picnic, Post-quantum RSAEncryption, Post-quantum RSASignature, RankSign, RVB, WalnutDSA

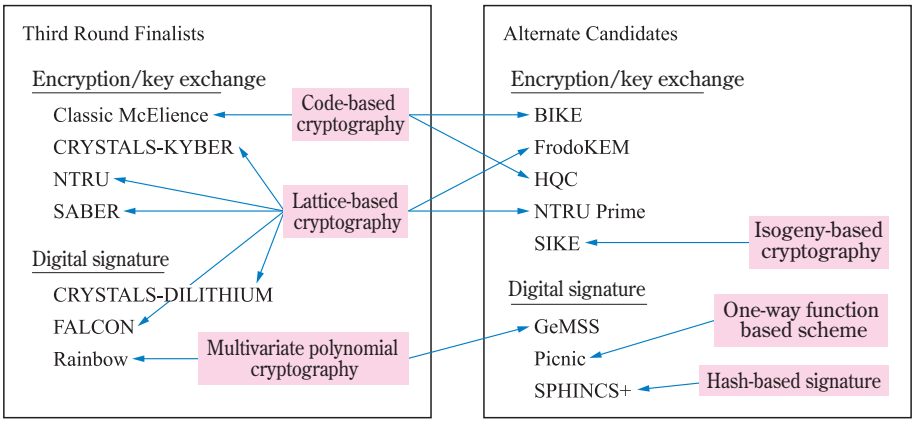

Fig. 3 Cryptosystems selected for evaluation in the third round of the NIST's PQC standardization project (July 2020)

items mentioned above.

The public call organized by NIST on account of the PQC standardization project was closed on November 2017 after collecting 69 proposals that satisfied the conditions for the public call (Table 2). They were composed of 25 proposals on lattice-based cryptography, 18 proposals on code-based cryptography, 10 proposals on multivariate polynomial cryptography, two proposals on hash-based signatures, and one proposal on isogeny-based cryptography. Information about all proposed cryptosystems is available on the NIST PQC Standardization Project homepage. Classifying the proposed cryptosystems by function, there were 49 proposals on public-key encryptions (including key exchanges) and 20 proposals on digital signatures. Proposals were submitted from 25 countries of the world, which were mostly countries in North America and Europe, but included Japan, Korea, China, Taiwan, Singapore, and Australia from the Asia region. The total number of proposers amounted to 278, among which 67 submitted proposals on two or more schemes. From Japan, proposals were submitted by KDDI Research Inc., the Toshiba Research and Development Center, the National Institute of Information and Communications Technology, and our group at the University of Tokyo.

The NIST PQC standardization project is furnished with a mailing list viewable by the public, to which more than 600 emails had been posted by December 2018, showing the result of many active discussions on such topics as the security of the proposed schemes. In January 2019, 26 schemes to proceed to the second round of the PQC standardization project were announced, and in July 2020, the schemes to proceed to the third round were selected (Fig. 3). As the schemes to be evaluated in the third round, seven finalists and eight

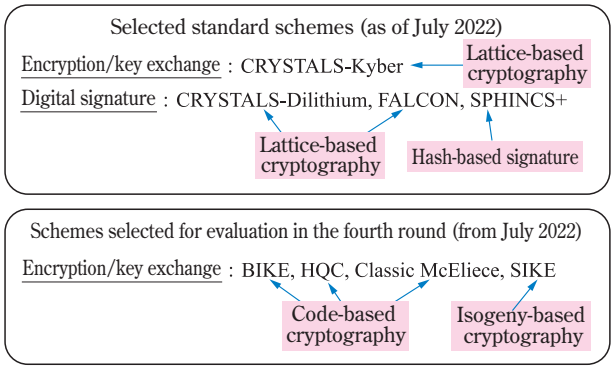

Fig. 4 The PQC standard schemes selected by NIST, and the schemes selected for evaluation in the fourth round of the NIST's PQC standardization project (July 2022)

Table 3 NIST's PQC standardization schedule

December 2017 to December 2018 : First-round evaluation period
January 2019 to July 2020 : Second-round evaluation period
July 2020 to June 2022 : Third-round evaluation period
July 2022 : Selection by NIST of the PQC standard schemes ＊The fourth-round evaluation of encryption schemes began. Another public call was organized to collect more proposals on digital signatures.
2024 : Establishment of standards on the PQC standard schemes selected by NIST
Up to 2030 : The continued use of SP 800-56 and FIPS PUB 186-4 conforming schemes is permitted.

alternate candidates were selected. From among the finalists, lattice-based cryptography was the main schemes along with three encryptions and two digital signatures. As other finalists, a scheme for code-based cryptography and a scheme for multivariate polynomial cryptography were selected. As alternate candidates, an encryption scheme for isogeny-based cryptography, a hash-based signature, and a signature based on symmetric-key cryptography were selected. Instead of selecting only lattice-based cryptography as standard schemes, NIST plans to select some schemes based on basic problems of other kinds as well in consideration of their security and performance characteristics.

They announced the first group for the standardized schemes in July 2022 : the lattice-based scheme CRYSTALS-Kyber as a choice in the category of encryptions/key exchanges, lattice-based schemes CRYSTALS-Dilithium and FALCON as choices in the category of digital signatures, and SPHINCS＋in the category of hash-based signatures (Fig. 4 top). From among the three lattice-based encryptions that were evaluated in the third round, CRYSTALS-Kyber was chosen as the standard scheme because of its computational efficiency and satisfactory level of completeness in discussions about security evaluations. In the category of digital signatures, two lattice-based schemes were selected at the same time, but as the signature length becomes relatively large with CRYSTALS-Dilithium, FALCON may be preferred for a system that requires a smaller signature length. As a hash-based signature, SPHINCS＋achieves high security, but because of the large signature length and a limit to the number of times a signature may be generated, it is intended for limited use, such as software distribution.

At the same time, they announced the schemes to be evaluated in the fourth round : BIKE, HQC, and Classic McEliece as code-based cryptography, and SIKE as isogeny-based cryptography. From among the mentioned three code-based schemes, a standard encryption scheme is going to be selected (Fig. 4 bottom). For SIKE, a polynomial-time cryptanalysis using the structure of high-dimensional manifolds was proposed in August 2022. For digital signatures, NIST organized another public call in the search for schemes that might achieve a shorter signature length and faster signature verification, as a result of which, in July 2023, they published 40 schemes that satisfied the conditions for the public call. Detailed information up to the third round can be found in a report referred to as NIST-IR 8413 (https://doi.org/10.6028/NIST.IR.8413-upd1).

Finally, in 2024, after the collecting of public comments, the schemes that were selected in July 2022 are going to be standardized as NIST PQC standard schemes (ML-KEM, ML-DSA, SLH-DSA). As a transition measure for currently used cryptosystems, they decided that, until 2030, it should be acceptable to continue using the RSA cryptosystem and elliptic curve cryptography that have the security strength of 128, 192, or 256 bits in the classical security level according to SP 800-56 and FIPS PUB186-4 (Table 3). However, since the preparation period before the transition to post-quantum cryptography from 2031 is limited, the hybrid use of the currently popular RSA encryption/elliptic curve cryptography and post-quantum cryptography is also studied.

4. Conclusion

This paper explained the latest trends in post-quantum cryptography, that is to say, cryptography that can be safely used even in the era of quantum computers. This paper, in particular, provided explana-

tions about typical schemes of post-quantum cryptography and presented an overview of the PQC standardization project led by the National Institute of Standards and Technology (NIST) of the United States. In July 2022, they selected three lattice-based schemes and one hash-based signature as NIST PQC standard post-quantum cryptography, and they are in the process of the standardization of additional schemes through the fourth-round evaluation and by selecting from proposals made in response to another public call. Another challenge from now on will be to manage issues associated with the transition to the newly standardized post-quantum cryptosystems.

References

(1) Tsuyoshi Takagi, Cryptography and Quantum Computer, Ohmsha, 2018. (In Japanese)

(2) P. 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.

(3) 7th international workshop on post-quantum cryptography-PQCrypto 2016, T. Takagi, ed., Lect. Notes Comput. Sci., vol. 9606, Springer, 2016.

(Paper accepted on May 31, 2023, and finalized on June 19, 2023.)

Tsuyoshi TAKAGI (member)

In 1993, graduated from the Department of Mathematics, School of Science, Nagoya University. In 1995, completed the master's program at the university's graduate school. Joined Nippon Telegraph and Telephone Corporation in the same year. In 2001, started serving as assistant professor at Technische Universität Darmstadt, Germany. In 2017, started serving as professor at the Graduate School of Information Science and Technology, the University of Tokyo. Engages in research on cryptographic mathematics. Holds the degree of Dr. rer. nat. Receiver of a 2013 Achievement Award from *IEICE* and an award from the Japan Society for the Promotion of Science for the 11th occasion.