Trends in Post-Quantum Cryptography: Cryptosystems for the Quantum Computing Era

Naoyuki Shinohara
Senior Researcher
Security Fundamentals Laboratory
Cybersecurity Research Institute
National Institute of Information and
Communications Technology

Shiho Moriai
Director
Security Fundamentals Laboratory
Cybersecurity Research Institute
National Institute of Information and
Communications Technology

1. Introduction

Cryptography is one of the familiar basic technologies that supports modern society. For example, online retailers, card payments, travel cards and wireless LANs all depend on the use of cryptography. Today, RSA and elliptic curve cryptography (ECC) are the most widely used public-key cryptosystems. Quantum computers have been actively developed in recent years, and are expected to be used in a wide variety of fields. However, the development of large-scale quantum computers will cause a major reduction in the security of RSA and ECC. To address this issue, work is under way to develop and standardize post-quantum cryptography (PQC) technology that is secure against not only conventional computers but also quantum computers. This paper introduces the global trends in this field.

2. The impact of quantum computing on the security of current public-key cryptosystems

The security of public-key cryptosystems that are currently in use or under development is guaranteed based on the difficulty of solving particular mathematical problems by using computers. For example, in RSA (the most widely used public-key cryptosystem), two prime numbers of equal bit length are used as the private key, and the composite number obtained by multiplying them together is publicly distributed as the public key. Anyone who can decompose this composite number into its prime factors will be able to obtain the private key and break the RSA cryptosystem. Another widely used public-key cryptosystem is ECC, the security of which hangs on the difficulty of computing discrete logarithms on elliptic curves. That is, it is possible to obtain a secret key in this cryptosystem by solving a discrete logarithm problem on an elliptic curve. The ongoing development of quantum computers threatens the security of RSA and ECC because a quantum computing algorithm proposed by Peter Shor in 1994 can be used to solve integer factorization problems and discrete logarithm problems efficiently.

In experimental demonstrations of Shor's algorithm to perform integer factorization on a quantum computer, the current world record is the factorization of 21 (=3×7), so for the time being, quantum computers do not pose a serious threat to RSA or ECC. However, according to Internal Report 8105 published by the US National Institute of Standards and Technology (NIST) in 2016, it was stated that although it is not clear when scalable quantum computers will be implemented, quantum computer researchers estimate that quantum computers capable of factorizing 2048-bit RSA public keys may be built by 2030. Against this background, there is a need for cryptographic techniques that are secure against both conventional computers and quantum computers, and efforts are being made to rapidly develop and standardize post-quantum cryptography (PQC) techniques.

3. Development and standardization of post-quantum cryptography

Most of the cryptographic techniques currently in use took almost 20 years to gain widespread acceptance after they were first proposed. Since standardized post-quantum cryptography is expected to become available by 2030, it was therefore necessary to begin developing and standardizing post-quantum cryptography techniques from about 2010. Although post-quantum cryptography research and development has a long history, the first international academic conference focusing on post-quantum cryptography (PQCrypto) took place in 2006. The ninth PQCrypto conference was held in 2018, so it can be said that the development of post-quantum cryptography gained momentum just in time.

The domestic and international efforts to standardize PQC are introduced below (see Figure. 1). In 2015, the US National Security Agency (NSA) announced that it was planning to switch to post-quantum cryptography. The NIST also announced a call for proposals for post-quantum cryptography techniques in 2016, and by the November 30, 2017 deadline, they had received 82 submissions from around the world. 69 of these were announced as complete and proper submissions, and five were subsequently withdrawn (see Figure. 2). NIST is evaluating the candidate cryptosystems in terms of security, implementation performance and so on, and plans to release a draft post-quantum cryptography standard some time in 2022–2024. In Europe, the European Telecommunications Standards Institute (ETSI) is conducting surveys and other studies related to post-quantum cryptography. In the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC JTC 1/SC27 has started discussions aimed at the standardization of PQC.

Efforts to standardize post-quantum cryptography are also being made in Japan. Four organizations — the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, the National Institute of Information and Communications Technology (NICT) and the Information-technology Promotion Agency (IPA) — serve as the secretariat of the CRYPTREC (Cryptography Research and Evaluation

Figure 1: PQC standardization trends in Japan and overseas

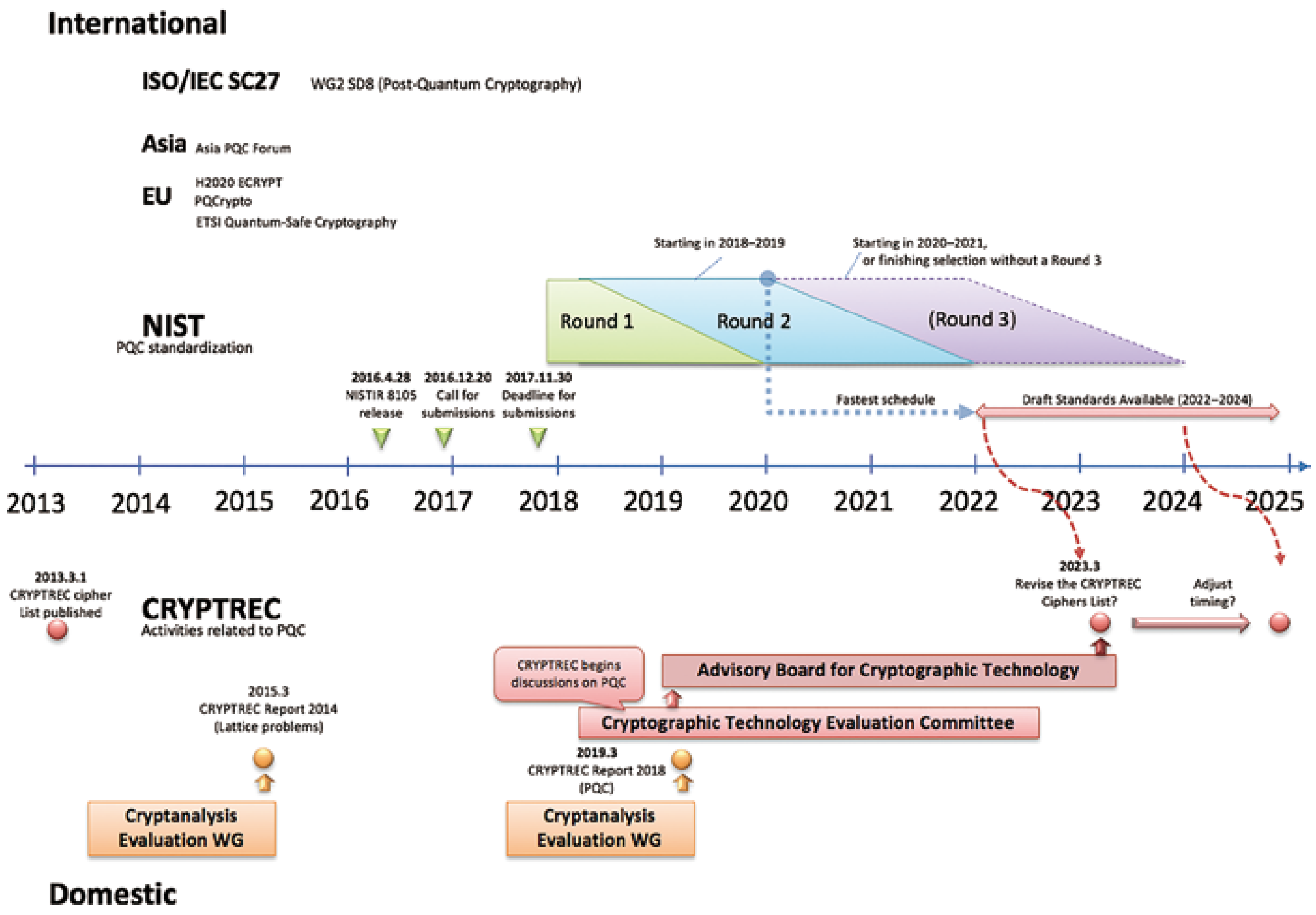
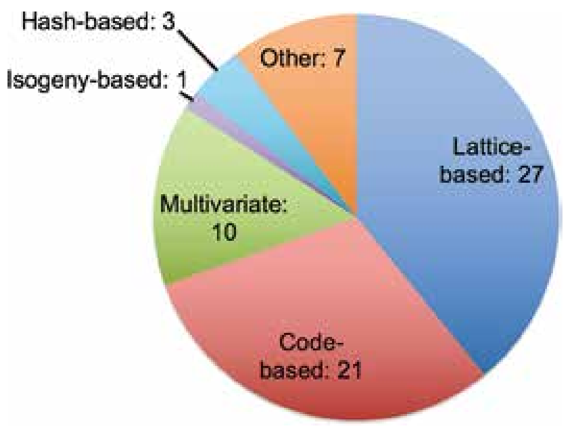


Figure 2: The 69 PQC candidates being considered for standardization by NIST(classified by base technology)



Committees) project, which evaluates and examines the security of a list of ciphers to be consulted by all government ministries when procuring information systems (the e-Government Recommended Ciphers List), and is conducting surveys and studies of appropriate methods for the implementation and operation of cryptography. Since 2014, with a view to standardizing post-quantum cryptography, we have been surveying research trends regarding lattice-based cryptography (a promising candidate for post-quantum cryptography), and the mathematical problems related to the security of this technique (lattice problems), and we have published technical reports summarizing our findings. Besides lattice-based cryptography, there are several other promising candidates for post-quantum cryptography. These include code-based cryptography, multivariate cryptography, and isogeny-based cryptography. At CRYPTREC, we have been surveying these four post-quantum cryptography techniques since 2017, and in 2019 we plan to publish a technical report summarizing our findings.

4. Development of the LOTUS post-quantum cryptosystem at NICT

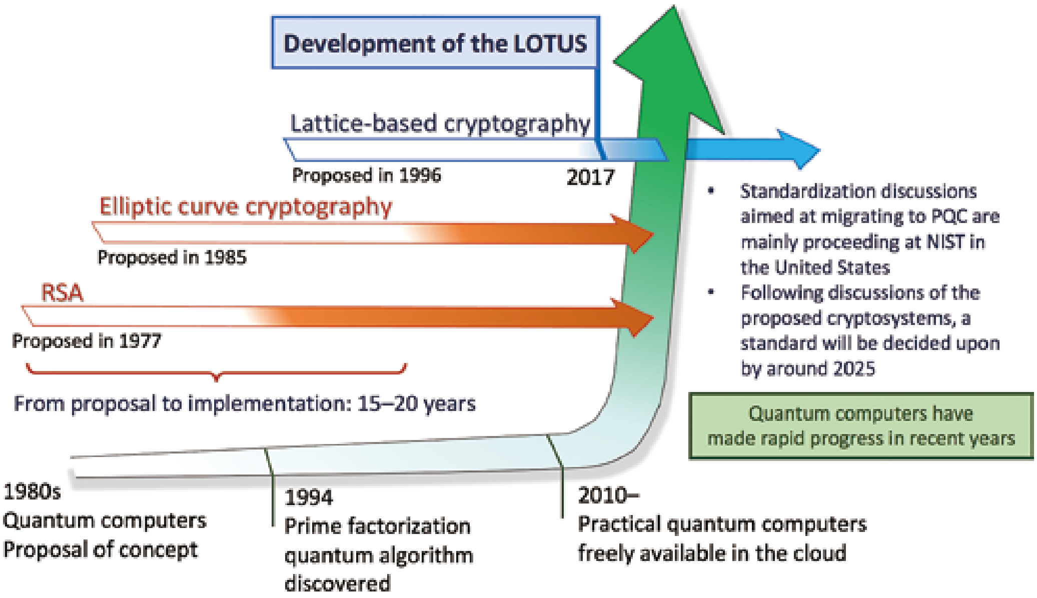
NICT has spent many years developing cryptographic techniques and researching the evaluation of their security. Regarding post-quantum cryptography, we developed a new lattice-based public key cryptosystem called LOTUS, which we proposed to NIST's post-quantum cryptography standardization project in 2017 (see Figure. 3). This scheme was announced as a complete and proper submission, and so far, no major security flaws have been discovered. The evaluation of this scheme as a candidate for standardization is continuing.

LOTUS is not only secure against quantum computers, but also has versatility, making it suitable for use in wide range of applications including web browsers and databases. Versatility is a concept related to the overall security of a cryptosystem comprising a combination of multiple cryptographic techniques. Cryptographic techniques must first of all be individually secure. Furthermore, when they are used in practice, they may be combined with other cryptographic techniques. It is necessary that these combinations do not give rise to vulnerabilities. When combining cryptosystems that lack versatility, it is generally difficult to guarantee the security of entire system, even if each component is secure.

When using a cryptosystem that lacks this property, any mistakes made when combining these elements is liable to introduce vulnerabilities capable of being exploited by an attacker, and the entire system will be at risk of being broken. Guaranteeing the security of the entire system involves a two-step procedure where the security of each individual cipher is first proved, and then the security of the whole cryptosystem is proved. However, it can take experts several days to verify a complicated system, and this complexity can also cause problems such as an increased likelihood of errors. At the design stage of a cryptosystem, the property of versatility makes it possible to avoid such dangers. The security of a system that combines cryptosystems with versatility can be proved mathematically, which means the step of proving the overall system's security can be omitted. In the LOTUS system developed at NICT, we have added data corruption resistance to the basic lattice cryptography by incorporating a mechanism that checks the structure of ciphertexts when they are decrypted. This checking mechanism has been mathematically proven to have versatility that allows it to be combined with other cryptosystems, which means this cipher can be used in diverse situations in society by incorporating it into various different systems.

At the same time, we have also developed a security evaluation method for lattice-based cryptosystems, which has made it possible to set parameters suitable for long-term use of the cryptosystem. Since this security evaluation method can also evaluate other lattice-based cryptosystems, we now believe it can contribute to fair security evaluations by providing a unified basis for the evaluation of proposed candidate systems in the NIST standardization project.

■ **Figure 3: The LOTUS**


Development of the LOTUS
Lattice-based cryptography
Proposed in 1996
2017
Elliptic curve cryptography
Proposed in 1985
RSA
Proposed in 1977
From proposal to implementation: 15–20 years
• Standardization discussions aimed at migrating to PQC are mainly proceeding at NIST in the United States
• Following discussions of the proposed cryptosystems, a standard will be decided upon by around 2025
Quantum computers have made rapid progress in recent years
1980s Quantum computers Proposal of concept
1994 Prime factorization quantum algorithm discovered
2010– Practical quantum computers freely available in the cloud