Paving the Runway for Standardization of Post-Quantum Cryptography

Lily Chen (SC27 expert, USA)

The cryptography and security mechanisms standardized by SC27 have become the cornerstone for today's global cybersecurity. The mechanisms have been deployed to provide network security, enable e-commerce, establish virtual private networks (VPN) for business and enterprise applications, and block malware invasion of IT devices.

When people consider quantum supremacy, a question appears: will the cryptographic mechanisms being standardized and deployed still be secure when quantum computers become available? This article will discuss quantum impact on the current widely deployed cryptographic mechanisms and introduce approaches being taken by SC27 to prepare for the quantum era.

Cryptography

Quantum computers will accelerate information processing and solve previously infeasible problems thus offering life-changing scientific breakthroughs. However, full scale quantum computers, once available, will impact cybersecurity in a catastrophic way.

The cryptographic primitives standardized by ISO/IEC JTC1 SC27 can be categorized as public-key (a.k.a. asymmetric-key) cryptography and symmetric-key cryptography. For example, "ISO/IEC 18033 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers" specifies public-key cryptography primitives, while "ISO/IEC 18033 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers" specifies symmetric-key cryptography primitives.

At a high level, public-key cryptography is used to provide authenticity of an entity or data and to securely establish symmetric keys. Symmetric-key cryptography, using the established keys, protects the confidentiality and integrity of information. For example, the transport layer security (TLS) protocol uses public-key cryptography to establish keys and to conduct mutual authentication between a client and a server. Then, the actual information being exchanged is protected by symmetric-key cryptographic algorithms using the keys established by public-key processes. Another application of public-key cryptography is using digital signatures for code signing to prevent undetected insertion of malware.

The security of public key cryptography is based on the "hardness" of certain computational problems. For well-known RSA schemes, their security depends on the difficulty of factoring large integers. That is, given a large integer n, find primes p and q such that $n = pq$. This is a hard problem because, as the size of the integer n increases, the complexity of factorization increases exponentially. When n is an appropriately chosen integer of 2048 bits or larger, it requires at least 2^{112} operations to factor n. For classical computers, such complexity means it is practically infeasible to factor.

Quantum Impact

Currently, most of the public-key cryptographic mechanisms standardized in ISO/IEC are either factorization-based, such as signatures specified in "ISO/IEC 14888-2 Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms" or discrete-logarithm-based, such as signatures specified in "ISO/IEC 14888-3 IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms." Both problems have been considered hard for classical computers to solve within a practical time frame. Therefore, the public-key cryptography mechanisms that are based on these problems currently provide sufficient protection from cryptanalysis.

However, in 1994, Peter Shor, an MIT professor, showed how quantum computers can be used to solve both the factorization and discrete logarithm problems in polynomial time. That is, the complexity of factorization increases as a polynomial function of the size of the integer *n*. As a result, the arrival of quantum computers large enough to run Shor's algorithm efficiently will eventually render the security of all widely implemented public-key cryptographic schemes ineffective.

Quantum computers will also impact the security of symmetric-key cryptography. By Grover's algorithm, for a block cipher with 128-bit key, using exhaustive search, the complexity of finding the key will be reduced from 2^{128} to 2^{64}, that is, the square root of 2^{128}. Here 2^{128} is the classical complexity, while 2^{64} is the quantum complexity. Even though we do not have a practical estimate of the quantum computing cost, we can mitigate the quantum attacks on symmetric-key cryptography by increasing its key size.

In summary, the quantum impact to public-key cryptography is catastrophic, while the impact to symmetric-key cryptography can be managed by increasing key sizes. Considering that most symmetric-key cryptography primitives have provided options to use higher key sizes, addressing quantum resistant public-key cryptography is more urgent.

Post-Quantum Cryptography

The cryptographic research community has been looking for quantum resistant cryptographic mechanisms since the beginning of this century. As noted above, some problems are hard for classical computers but not for quantum computers. The challenge is finding problems that are hard for both classical and quantum computers. Fortunately, researchers have identified sets of problems which seem to be hard even for quantum computers (e.g., finding shortest vectors for lattices). Public-key cryptography mechanisms can be designed that rely on these problems. Such mechanisms are referred to as *post-quantum cryptography* (PQC) or quantum-resistant cryptography.

Post-quantum cryptography has been a very active research area in the past decade. Many PQC algorithms have been published in the research literature. The National Institute of Standards and Technology (NIST) in the USA has been conducting a PQC standardization effort since 2016. In the past five years, many submitted candidate algorithms have been analyzed and evaluated by the research community. After considering security, performance, and many other aspects, NIST has narrowed down the candidate pool twice. NIST is now in the third round of this process, with seven finalists and eight alternate candidates. NIST is expected to complete its third round selection in 2022 and release draft PQC standards in the 2022-2023 timeframe.

Together with the NIST standardization effort, international standards organizations have undertaken initiatives to prepare for PQC standardization. Industry is also actively exploring a transition path.

SC27 has more than 30 years history in developing cryptographic standards. Many cryptographic experts from different national bodies have consistently contributed to different standards. The contributors are resourceful and knowledgeable. But considering that post-quantum cryptography is relatively new even for many experts and many algorithms are still under evaluation, it is critical to create opportunities for the experts to get familiar with post-quantum cryptography and be ready to make decisions on standardization.

Standing Document (SD8)

SC27 WG2 started a study period on post-quantum cryptography in October 2015. The study period lasted 24 months with multiple calls for contributions soliciting input from the SC27 experts. As a decision from the study period, WG2 decided to develop a standing document to introduce some basic primitives to be used as a reference for the experts. The standing document should focus on several well-researched categories of post-quantum cryptography.

It is agreed that the standing document must focus on basic concepts and security assumptions in each of the categories of post-quantum cryptography. It needs to introduce the major applicable cryptographic classes. Specific algorithms should be used as examples to illustrate the principles and operations for the experts to understand each category.

SD8 consists of six parts and introduces five categories of the most researched post-quantum cryptographic mechanisms. Here is a high-level description for each part.

- Part 1 provides a general introduction on post-quantum cryptography, including security definitions and performance considerations.
- Part 2 focuses on hash-based signatures. Hash-based signatures are different from other categories in post-quantum cryptography. It is not based on number theory assumptions but on the security of hash functions. It was introduced in the 1970s. Stateful hash-based signatures are essentially one-time signatures. It requires state management to guarantee that each private-key can only be used to sign one message. But on the other hand, it relies on minimal security assumptions. The security properties are better understood.
- Part 3 introduces lattice-based mechanisms. Lattice-based cryptography is an attractive post-quantum cryptography family. Part 3 provides descriptions of the major approaches in building lattice-based mechanisms together with twelve example algorithms for public-key encryption, key exchange, and digital signatures.
- Part 4 introduces code-based cryptography. Like hash-based signatures, code-based cryptosystems have been developed since 1978 using error-correcting codes to build public-key cryptography. This part describes the main structure of code-based encryption algorithms and the security analysis methods.
- Part 5 introduces multivariate cryptosystems. Multivariate cryptography refers to public-key cryptography whose public keys represent a multivariate and nonlinear (usually quadratic) polynomial map. The main computational problem underlying multivariate cryptography is to find preimages for these multivariate polynomial maps. This part described the major variants of multivariate cryptosystems and highlighted attack methods applying to each variant.
- Part 6 introduces a relatively new category, isogeny-based cryptography. The idea of using maps between elliptic curves to build public-key cryptography traces back to 1997, while the first concrete design was proposed about ten years ago. This part introduces the background of isogeny-based cryptography and gives details of an early design of the isogeny-based CRS

system and recent supersingular-isogeny Diffie-Hellman (SIDH) protocol. It also discusses security assumptions and attacks on isogeny-based cryptosystems.

Each part of SD8 is authored by well recognized researchers on the topic. More than eight experts from multiple national bodies and liaison organizations, Belgium, China, Japan, Netherland, USA, PQCrypto, etc., all contributed to SD8. The effort lasted about two years. Since 2020, SD8 has been publicly available at https://www.din.de/en/meta/jtc1sc27/downloads.

During the development of SD8, SC27 WG2 also held tutorial sessions at each working group meeting. The experts who authored SD8 gave tutorial presentations on the different topics corresponding to each part of SD8. The tutorials gave opportunities for the experts to ask questions and helped to make SD8 accessible.

SD8 has played an effective role in preparing SC27 for post-quantum cryptography standardization. It has been shared with liaison organizations such as ETSI TC CYBER WG QSC, ITU-T SG 17, ISO/IEC JTC 1 SC6, and ISO TC 68/SC 2.

As a preparation effort, SC27 also established liaison relationships with post-quantum cryptography research projects such as PQCRYPTO, SAFEcrypto, PRISMACLOUD, FutureTPM, etc. in sharing information on development and practice of post-quantum cryptography.

Moving forward

Through the SD8 effort, SC27 experts have been well-prepared to move forward with standardization of post-quantum cryptography. As a matter of fact, the project for specifying stateful hash-based signatures in “ISO/IEC 14888-4 Information technology — Security techniques — Digital signatures with appendix — Part 4: Stateful hash-based mechanisms” is in the first committee draft stage. Stateful hash-based signatures can be used for code signing as an example of early adoption of post-quantum cryptography.

Standardization of post-quantum cryptography poses challenges to SC27. As a standards subcommittee with a long history of constantly adapting to rapidly advanced technology and applications, SC27 has made great progress in preparing to develop the next generation of cryptographic standards for quantum era.