Towards migration to secure information infrastructures even in quantum computers era

White Paper on Migration to Post-Quantum Cryptography

Cyber Security Department,
NTT DATA Group Corporation, Japan
E-mail: security-contact@kits.nttdata.co.jp

Publication Date: October 3, 2023

This document was created by NTT DATA Group Corporation with the support from NTT Social Informatics Laboratories.

Table of Contents

1. Introduction

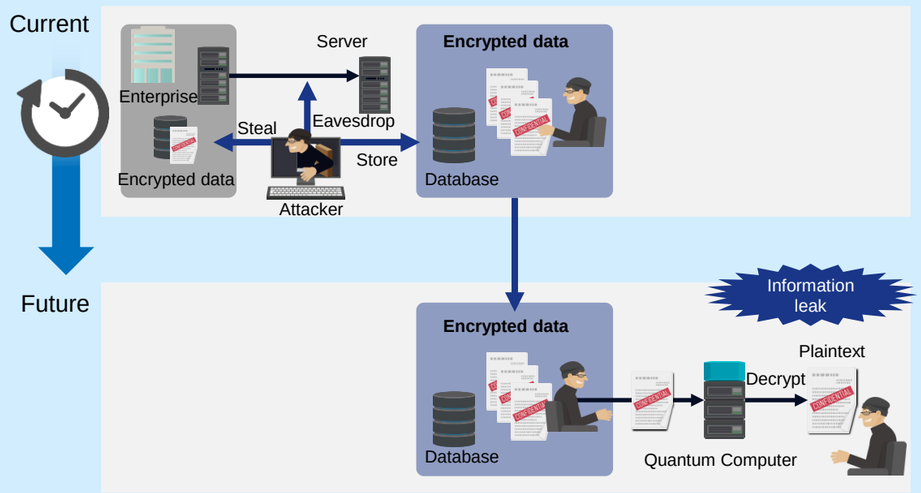
IT systems and cryptographic technologies

In recent years, cryptographic technologies are widely used as a base in IT systems. For example, **encryption** is used to protect information by making it look like meaningless data even if data flowing on communication paths or data stored in storage is eavesdropped or stolen by an attacker. In addition, **digital signatures** are used to ensure that data was created by yourself and it has not been tampered. Both encryption and digital signatures are typical cryptographic technologies that support today's society.

On the other hand, in recent years, **quantum computer** implementation technology has made remarkable progress. Quantum computers have a potential to make it possible to perform calculations in a short period of time, which conventionally could not be completed within a realistic timeframe, and are expected to be applied to research such as AI and drug discovery. However, in general, when a new technology appears, threats from attacks that exploit that technology also appear. In other words, it is feared that cryptographic technologies will be broken by quantum computers in the future.

Attackers take a long-term view and try to crack the cipher successfully. Even if it is not possible to break the encryption because the performance of quantum computers is not sufficient at present, **“Store now, decrypt later attack”**, which will try to decrypt the encryption when the performance of quantum computers improves in the future, are starting to be seen as a threat (Figure 1). This attack is also known as “Capture now, decrypt later attack” or “Harvest now, decrypt later attack”.

Figure 1: Store now, decrypt later attack



Conventional threat was supercomputer

Conventional threat: Improving performance of supercomputers

Before explaining threats posed by quantum computers, let us explain an existing threat. It should be noted that this conventional threat has not been superseded by the quantum computer threat, it still exists. For cryptographic technologies, the conventional threat has been supercomputers. Given its speed of performance, recommended values for key lengths used for encryption and digital signatures have been estimated.

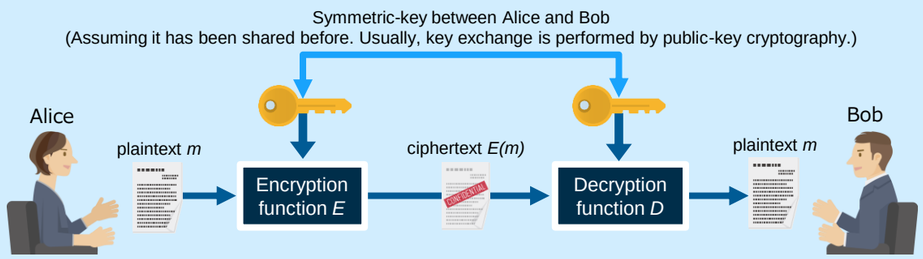
For example, **RSA cryptosystem** is one of the public-key cryptosystems that has encryption and digital signature functions. RSA cryptosystem is designed based on the difficulty of prime factorization of large numbers of digits. In other words, RSA cryptosystem will be broken if prime factorization with a large number of digits can be solved easily.

(Column) Cryptographic Technologies

■ What is Symmetric-key Cryptography?

In symmetric-key cryptography, keys for encryption and decryption are the same. First, a sender and a receiver share the symmetric-key data in some secure way. It is necessary to secretly manage symmetric-keys for each communication partner. In general, the processing speed of symmetric-key cryptography is much faster than that of public-key cryptography. Therefore, symmetric-key cryptography is used for normal encryption purposes, while public-key cryptography is used to share the symmetric-key between two parties.

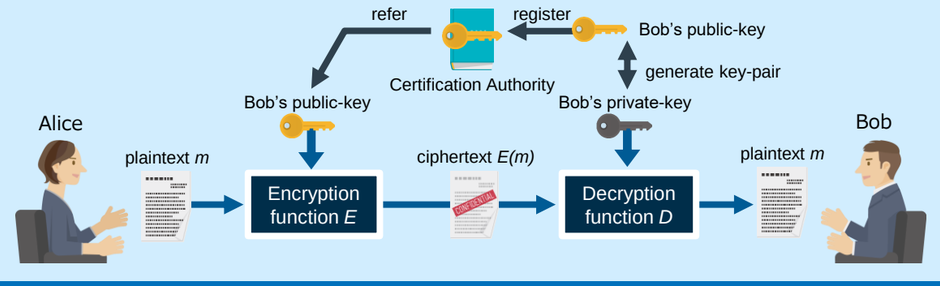
Figure 2: Symmetric-key Cryptography



■ What is Public-key Cryptography?

In public-key cryptography, the key for encryption and the key for decryption are different. You publish the key for encryption (public-key) and keep the key for decryption (private-key) secret. There is no need to secretly manage keys for each communication partner. Security relies on mathematical problems that are computationally difficult to solve.

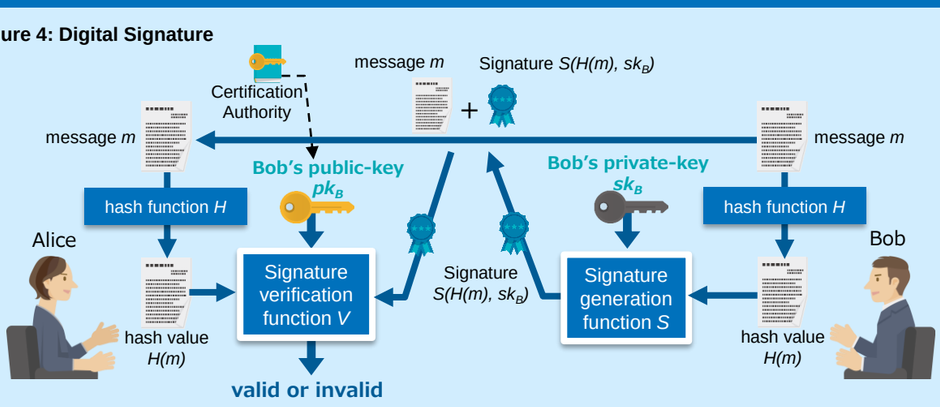
Figure 3: Public-key Cryptography



■ What is Digital Signature?

Digital signatures use the cryptographic idea of public-key cryptography in reverse. A sender uses sender's private-key to create a signature on a message and a receiver verifies the validity of the signature by using sender's public-key. If the result of signature verification is valid, it is guaranteed that the message has not been tampered with (namely, **integrity**). Furthermore, since the only person who can generate a correct signature is the person who holds the private-key, if the signature exists, the claim that it has not signed cannot be accepted (namely, **non-repudiation**).

Figure 4: Digital Signature



Extending the key length was sufficient as a conventional countermeasure

Conventional measures: Extension of key length

The traditional countermeasure against supercomputer threats has been to increase the key length (number of bits) used for encryption and digital signatures. In fact, symmetric-key lengths for RSA encryption have been extended to 512 bits, 1024 bits, 2048 bits, and so on. You might think that it would be better to use a long key from the beginning, but that would make the encryption process and the decryption process for a user who has a legitimate key take a lot of time. , safety is excessively met while convenience is compromised. Therefore, the appropriate key length can be derived by considering the performance of computers at that time and the performance of computers predicted about 30 years from now.

The US NIST (National Institute of Standards and Technology) publishes the security strength for each key length of symmetric-key cryptography and public-key cryptography using a common scale called "**bit security“** (Table 1, 2). Currently, 80-bit security strength (equivalent to 1024-bit key security in RSA, one of the public-key cryptosystems) is disallowed to use.

Table 1: Comparable security strengths of symmetric block cipher and asymmetric-key algorithms

Security Strength	Symmetric Key Algorithms	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
≤ 80 (Not currently available)	2TDEA	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f = 512+

* The security-strength estimates will be significantly affected when quantum computing becomes a practical consideration.

Table 2: Security strength time frames

Security Strength		Through 2030	2031 and Beyond
< 112	Applying protection	Disallowed	
	Processing	Legacy use*	
112	Applying protection	Acceptable	Disallowed
	Processing		Legacy use*
128	Applying protection and processing information that is already protected	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

* “Legacy use” means that an algorithm or key length may be used because of its use in legacy applications (i.e., the algorithm or key length can be used to process cryptographically protected data).

Source: National Institute of Standards and Technology, “SP800-57 Recommendation for Key Management Part 1:General (Revision 5),” 2020.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

Quantum computers are the new threat

2. Necessity for migration to Post-Quantum Cryptography (PQC)

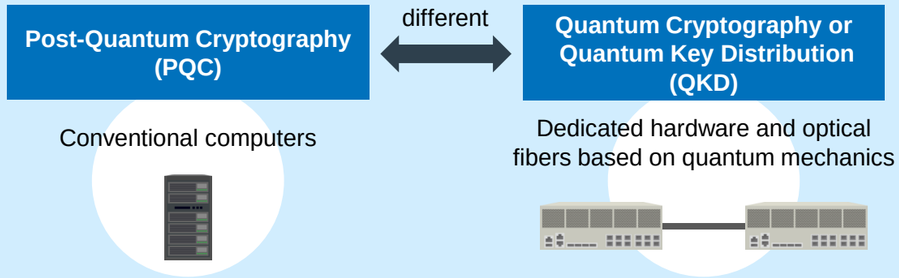
What is PQC and what is it different from?

Post-Quantum Cryptography (PQC) is a general term for cryptographic technologies that are difficult to decrypt or tamper with even with quantum computers. In general, it refers to multiple public-key cryptographic algorithm groups that are being standardized by the US NIST, which will be described later.

A technology different from PQC is **Quantum Key Distribution (QKD)** (Fig. 5). QKD is a key distribution technology that uses dedicated hardware and optical fiber based on quantum mechanics. Encrypted communication that utilizes as is called Quantum Cryptography. If there is no contextual confusion, QKD is sometimes simply referred to as "quantum cryptography" and vice versa, and tends to be ambiguous in its meaning. Also, historically, the concept of QKD and quantum cryptography predates PQC, having been announced in 1984.

In addition, since both PQC and QKD include the word “quantum” in their terms, we tend to imagine that something is processed using a quantum computer, but they do not do any processing on the quantum computer. Conventional computers are called "classical computers" in contrast to quantum computers, and PQC is realized as an algorithm that operates on classical computers. QKD consists of dedicated hardware based on quantum mechanics (transmitter and receiver) and optical fiber, and looks like a network switch or router, a hardware device that fits in a server rack.

Figure 5: Difference between PQC and QKD



The root cause of the threat “quantum algorithm” already exists

"Shore's Algorithm" for Solving Prime Factorization and Discrete Logarithm Problems

Not all cryptography can be broken by quantum computers. Here, we are aware of the existence of quantum algorithms and try to understand them.

First, to process something on a classical computer, you need to give the computer a program. The part of the program that performs essential calculations for a certain purpose is sometimes called the “algorithm of XX”. For example, “Algorithm to calculate the average value”.

Similarly, the part of a quantum computer that uses properties unique to quantum to perform calculations much more efficiently than a classical computer is called a **quantum algorithm**. In fact, **“Shor's Algorithm**” has already been proposed as a quantum algorithm for efficiently solving prime factorization and discrete logarithm problems. This existence is a direct threat to public-key cryptography such as RSA cryptosystem and elliptic curve cryptography. In 1994, when “Shor's Algorithm” was proposed, it had a great impact on the academic world, but quantum computer hardware technology was still in its infancy, and it was seen as a future threat in the industrial world. In recent years, however, it can be seen that the threat is growing little by little as the implementation technology of quantum computers progresses.

Table 3 summarizes the types of quantum algorithms that threaten AES, which is currently the mainstream of symmetric-key cryptography, and RSA cryptosystem and elliptic curve cryptography, which are public-key cryptography, as well as the degree of impact and desirable countermeasures.

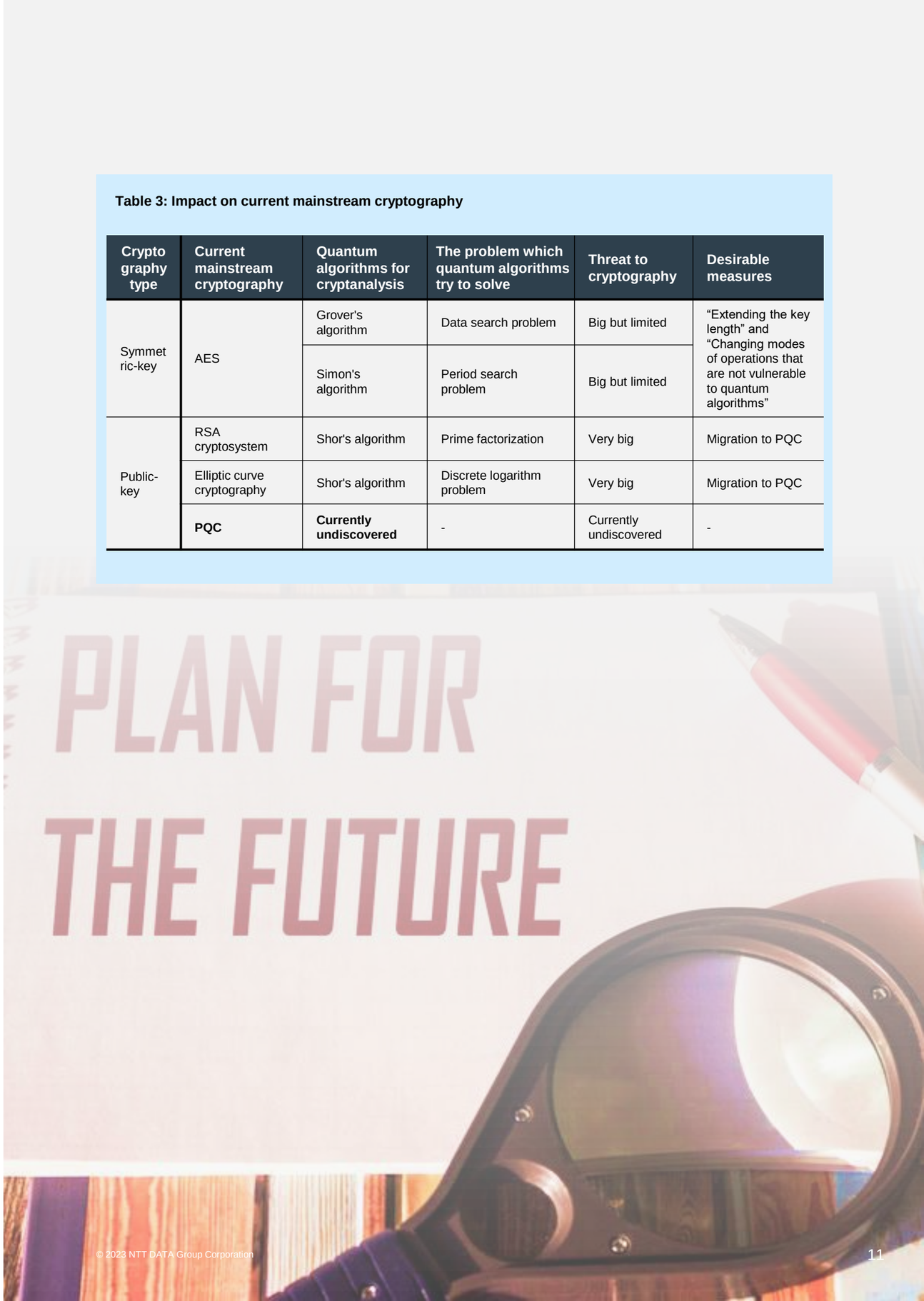
Symmetric-key cryptography AES is greatly influenced by quantum algorithms that efficiently solve data search and periodic search problems, but to a limited extent. Extending the key length of AES makes it resistant to quantum computers. Here, AES has only three key lengths to choose from: 128, 192, and 256 bits, so 256 bits, which is the longest, may be the best choice.

RSA and elliptic curve cryptography, which are public-key cryptosystems, are destructively affected by Shor's algorithm, so a shift to PQC is an essential countermeasure rather than adopting key length extension.

PQC belongs to public-key cryptography and can be considered that no quantum algorithm for cryptanalysis is currently discovered.

Table 3: Impact on current mainstream cryptography

Cryptography type	Current mainstream cryptography	Quantum algorithms for cryptanalysis	The problem which quantum algorithms try to solve	Threat to cryptography	Desirable measures
Symmetric-key	AES	Grover's algorithm	Data search problem	Big but limited	“Extending the key length” and “Changing modes of operations that are not vulnerable to quantum algorithms”
		Simon's algorithm	Period search problem	Big but limited	
Public-key	RSA cryptosystem	Shor's algorithm	Prime factorization	Very big	Migration to PQC
	Elliptic curve cryptography	Shor's algorithm	Discrete logarithm problem	Very big	Migration to PQC
	PQC	**Currently undiscovered**	-	Currently undiscovered	-



US Leads PQC Standardization

Responses of various countries to the threat of quantum computers

In response to the threat of quantum computers, various countries have begun efforts to transfer cryptographic technology (Table 4). In particular, the United States has taken the lead and has been promoting PQC standardization activities since 2016.

Table 4: Country response

Country or Region	Responses
US	• Assume that by 2030 there will be a quantum computer that can break RSA cryptosystem with a key length of 2048 bits*1 • Plan to migrate federal cryptosystems to PQC by 2035 *2 • Started PQC standardization activities in 2016 *3
EU	• ETSI released two technical reports to support US NIST standards for PQC*4 • SOG-IS will define specifications for agreed quantum-resistant algorithms in the future*5
Japan	• CRYPTREC has released cryptographic technology guidelines of PQC*6 • CRYPTREC has published a research trend report on PQC*7

*1 NIST, “NISTIR 8105: Report on Post-Quantum Cryptography”, 2016.
https://csrc.nist.gov/pubs/ir/8105/final
*2 The White House, “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”, May 4, 2022.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
*3 NIST, Post-Quantum Cryptography Standardization.
https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
*4 ETSI TR 103 616 V1.1.1 (2021-09) “Quantum-Safe Signatures”, and ETSI TR 103 823 V1.1.1 (2021-09) “Quantum-Safe Public Key Encryption and Key Encapsulation”.
https://www.etsi.org/newsroom/news/1981-2021-10-etsi-releases-two-technical-reports-to-support-us-nist-standards-for-post-quantum-cryptography
*5 SOG-IS Crypto Working Group, SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.3, February 2023.
https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf
*6 CRYPTREC, cryptographic technology guidelines of PQC (in Japanese)
*7 CRYPTREC, research trend report on PQC (in Japanese)

U.S. Executive Order (EO) and OMB memorandum

On May 4, 2022, U.S. President Joe Biden signed an executive order to establish and popularize new robust cryptographic technologies that are resistant to quantum computers, and its memorandum*1 was released.

Furthermore, in accordance with the executive order, the OMB (United States Office of Management and Budget) has issued specific instructions to each administrative agency, and its memorandum*2 has been made public on November 18, 2022 (Table 5).

Table 5: OMB memorandum, APPENDIX A: Interim Benchmarks

Event / Activity	Actions following publication	Responsible Body
Designate cryptographic inventory and migration lead	Within 30 days	All agencies
Release instructions for the collection and transmission of inventory	Within 90 days	ONCD
Release instructions for funding assessments	Within 90 days	ONCD
Establish a mechanism to enable the exchange of PQC testing information and best practices	Within 180 days	NIST
Release strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC	Within 1 year	CISA
Submit cryptographic system inventory	By May 4, 2023 and annually thereafter	All agencies except the Department of Defense and agencies in the Intelligence Community
Submit funding assessments	30 days after submission of cryptographic system inventory, and annually thereafter	All agencies except the Department of Defense and agencies in the Intelligence Community
Report testing of pre-standardized PQC	Ongoing	All agencies

*1 National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, White House.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
*2 Memorandum for the Heads of Executive Departments and Agencies, Office of Management and Budget.
https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

Four schemes have been decided as PQC standards, and further evaluations will continue

Status of Standardization of PQC by NIST

NIST started PQC standardization in 2016 and is still working on it[*1-6]. PQC standardization began with public offerings in three categories: "Public-Key Encryption", "Key Encapsulation Mechanisms (KEM)", and "Digital Signatures". After that, through three to four stages of screening evaluation, the proposal schemes are gradually narrowed down, and the policy is to finally select not one scheme but multiple schemes. The term “Key Encapsulation Mechanism (KEM)" is a term that has been widely used in the academic literature and is not familiar to people, so this document refers to it as “Key exchange (KEM)”.

69 schemes were accepted in December 2017, 26 methods advanced to the 2nd round evaluation based on the results of the 1st round evaluation in January 2019, and 15 methods received the 3rd round evaluation based on the results of the 2nd round evaluation in July 2020 (Fig. 6). On July 5, 2022, the results of the 3rd round evaluation were announced. Then, “CRYSTALS-KYBER” as a standard scheme of Public-Key Encryption and key exchange (KEM) categories, and “CRYSTALS-Dilithium”, "FALCON" and "SPHINCS+“ as three standard schemes of “Digital Signatures”, were selected (Table 6).

At the same time, “BIKE”, “Classic McEliece”, “HQC” in Public-Key Encryption and key exchange (KEM) categories were put on hold for standardization in the third round of evaluation. It was shown that the 4th round evaluation would be additionally conducted, and that at least one of them would be added to the standard.

*1 NIST, NIST IR 8105, Report on Post-Quantum Cryptography, April 2016.
https://csrc.nist.gov/publications/detail/nistir/8105/final
*2 NIST, Post-Quantum Cryptography, Workshops and Timeline.
https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline
*3 NIST, Post-Quantum Cryptography, Round 3 Submissions
https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions
*4 NIST, Post-Quantum Cryptography, Selected Algorithms 2022.
https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022
*5 NIST, Post-Quantum Cryptography, Round 4 Submissions
https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions
*6 NIST, Post-Quantum Cryptography: Digital Signature Schemes, Round 1 Additional Signatures
https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

Figure 6: NIST Standardization Schedule for Post-Quantum Cryptography

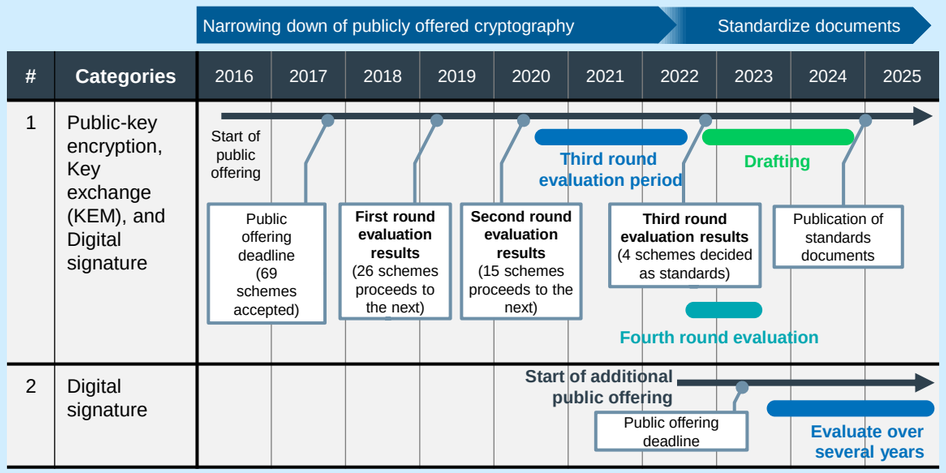


Table 6: Status of Standardization of PQC by NIST

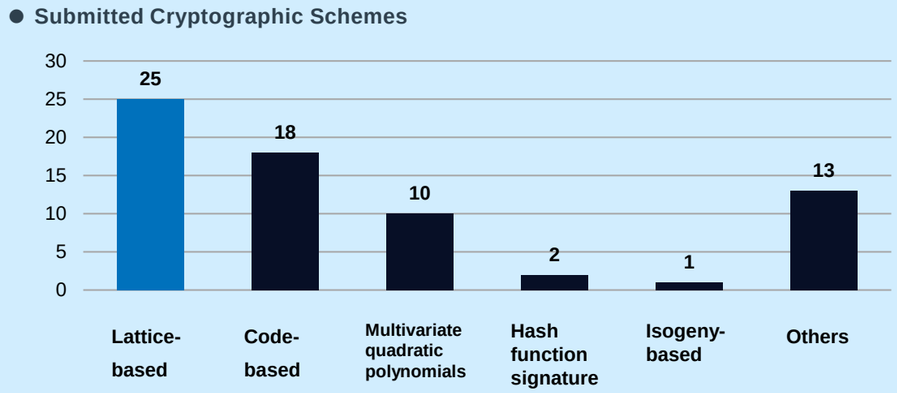
	Public-key encryption and Key exchange (KEM)	Digital signature
Determined as standards	**CRYSTALS-KYBER**	**CRYSTALS-Dilithium** **FALCON** **SPHINCS+**
Additional evaluation in the 4th round	BIKE Classic McEliece HQC	-
1st round evaluation through additional public offering	-	**(Code-based Signatures)** CROSS, Enhanced pqsigRM, FuLeeca, LESS, MEDS, Wave **(Isogeny Signatures)** SQIsign **(Lattice-based Signatures)** EagleSign, EHTv3 and EHTv4, HAETAE, HAWK, HuFu, Raccoon, SQUIRRELS **(MPC-in-the-Head Signatures)** Biscuit, MIRA, MiRitH, MQOM, PERK, RYDE, SDitH **(Multivariate Signatures)** 3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX **(Symmetric-based Signatures)** AIMer, Ascon-Sign, FAEST, SPHINCS-alpha **(Other Signatures)** ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon, Xifrat1-Sign.I

Many lattice cryptography in the process of PQC standardization

Lattice-based cryptography occupying the majority in submitted cryptographic schemes

An analysis of the distribution of the 69 publicly offered ciphers accepted for PQC standardization reveals a variety of difficult problems related to "lattice" in mathematics (collectively referred to as the "lattice problem" in this document). There were 25 methods based on safety (Fig. 7). In fact, among the four schemes determined by the PQC standard, three schemes, "CRYSTALS-KYBER", "CRYSTALS-Dilithium", and "FALCON", belong to lattice cryptography whose security is based on lattice problems.

Figure 7: 69 schemes that made it to the 1st round of PQC standardization evaluation



Even in the methods that advanced to the 2nd and 3rd rounds of evaluation, the trend of many lattice ciphers did not change (Fig. 8).

From this phenomenon, we can read that there are many lattice-based cryptography researchers in the world. The fact that there are many researchers in a specific field means that various cryptographic techniques will devise from that field. At the same time, it can be expected that there will also be many researchers who will evaluate its security which will give us a certain level of confidence in its security. In fact, the security of RSA cryptography, elliptic curve cryptography, etc. has been trusted because the prime factorization / discrete logarithm problem had been studied by many researchers for many years.

Therefore, when deciding on a cryptographic algorithm when migrating to PQC in the future, it can be considered desirable to list a cryptographic algorithm belonging to lattice cryptography as one of the options from the perspective of security.

Figure 8: NIST PQC standardization round 2 evaluation results (15 methods advanced to round 3 evaluation)

The number in parentheses represents the number in the box.

		Lattice-based cryptography (7 entries)	Code-based cryptography (3 entries)	Multivariate quadratic polynomials cryptography (2 entries)	Hash function signature (1 entry)	Isogeny-based cryptography (1 entry)	Others (1 entry)
Public-key encryption and Key exchange (KEM)	Finalist	(3): CRYSTALS-KYBER, NTRU (NTRU-HRSS-KEM + NTRUEncrypt), SABER	(1): Classic McEliece	-	-	-	-
	Alternative candidate	(2): Frodo-KEM, NTRU Prime	(2): BIKE, HQC	-	-	(1): SIKE	-
Digital signature	Finalist	(2): CRYSTALS-Dilithium, FALCON	-	(1): Rainbow	-	-	-
	Alternative candidate	-	-	(1): GeMSS	(1): SPHINCS+	-	(1): Picnic

What should I be aware of when migrating to PQC?

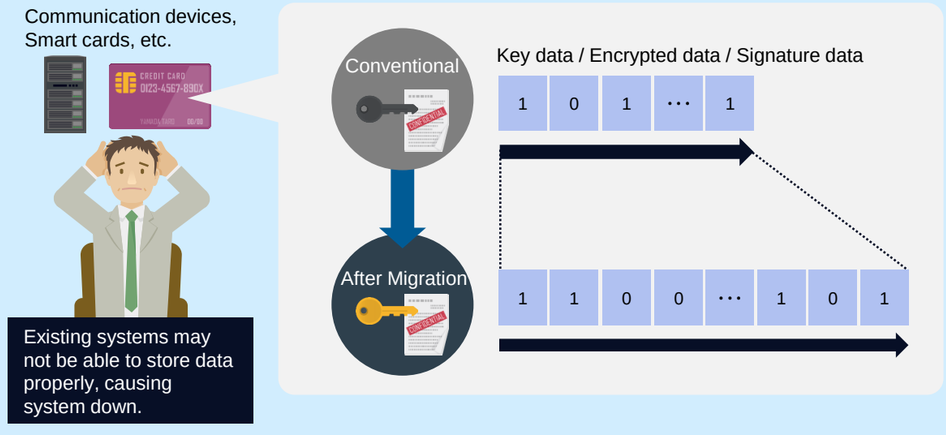
3. Focal points when migrating to PQC

The followings are points to remember when formulating a migration plan to PQC.

- **Point #1: Data size may increase**

In each PQC algorithm, the sizes of key data, encrypted data, and signature data are larger than those of conventional cryptosystems. If the program is not designed with these sizes in mind, data may not be stored correctly in memory, IC cards, etc., and the system may terminate abnormally (Fig. 9).

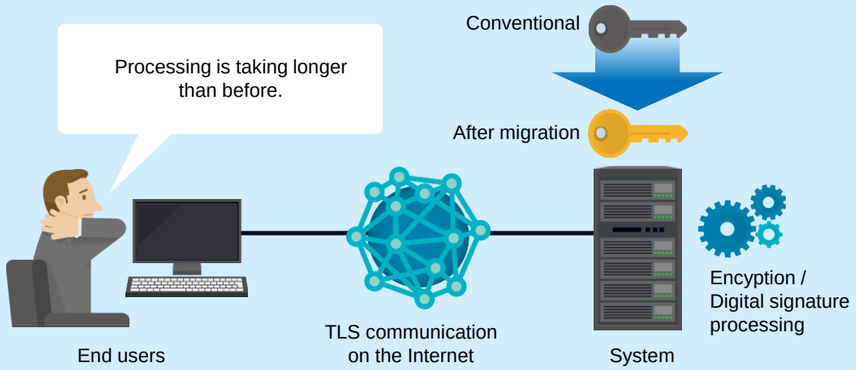
Figure 9: Point #1: Data size may increase



● Point #2: Processing speed may be slow

For each PQC algorithm, the key generation speed and encryption processing speed may be faster or slower than before. If it slows down, the waiting time experienced by system users will increase and convenience may decrease. Particularly, caution is required in cases where TLS session construction is repeated many times and in resource-saving environments such as IoT devices (Fig. 10).

Figure 10: Point #2: Processing speed may be slow



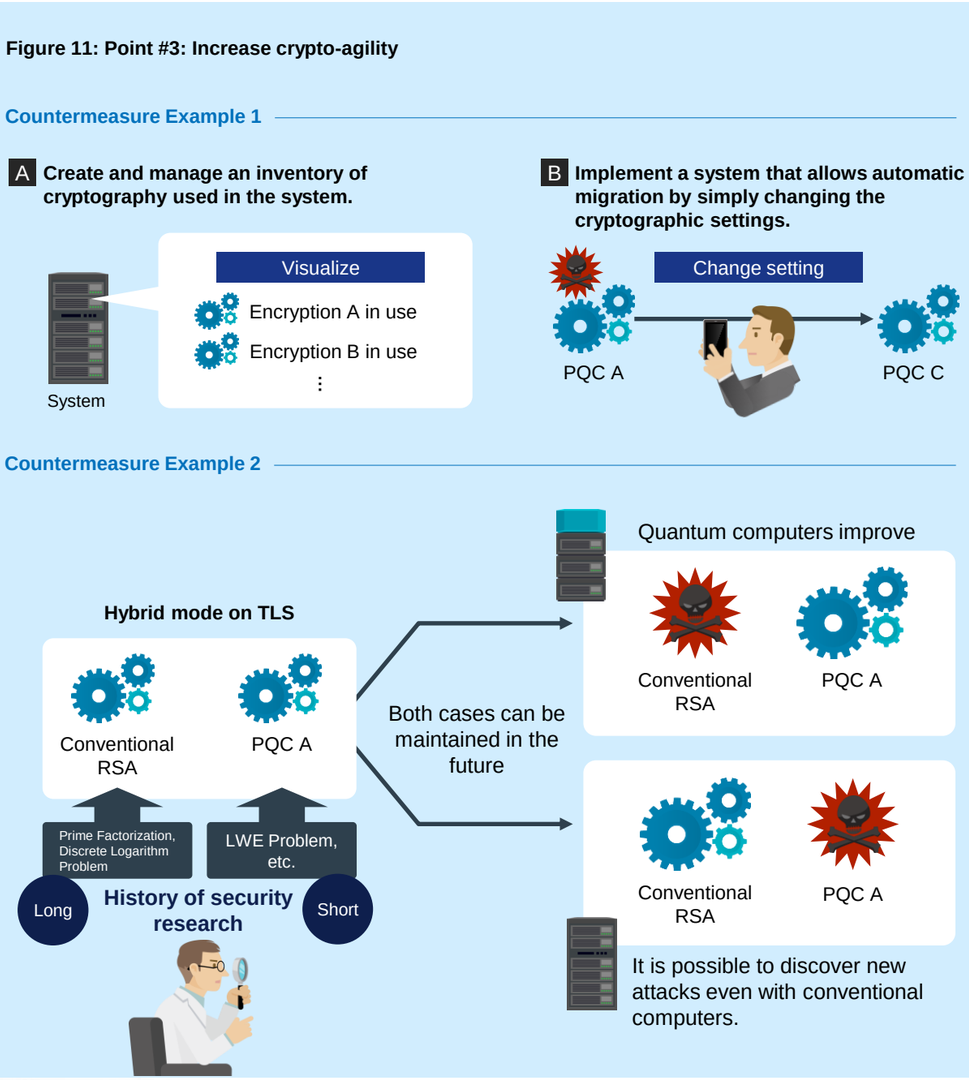
● Point #3: Increase crypto-agility

Although the security of each PQC algorithm has been fully verified by NIST, its history is shorter than that of conventional RSA, etc., so there is always a possibility of attacks being discovered in the future. The following are two examples of countermeasures for anticipated attacks.

The first example is to visualize the encryption method used in the system and design and implement it so that it can be easily migrated to another encryption method. This idea is called **crypto-agility**.

The second example is also an example of implementing crypto agility, but consider adopting a **hybrid mode** for TLS. Hybrid mode is a concept that combines two different encryption methods in parallel. For example, if the conventional RSA encryption and encryption scheme A with PQC are designed and implemented in hybrid mode, even if the RSA encryption is compromised in the future or the PQC encryption scheme A is compromised in the future, System safety can be maintained (Fig. 11).

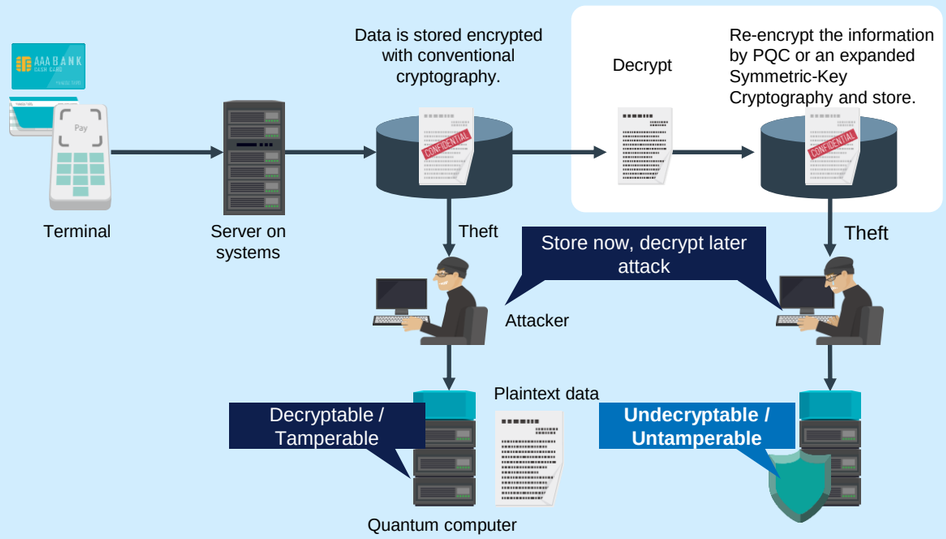
Figure 11: Point #3: Increase crypto-agility



● **Point #4: Consider re-encrypting if encrypted data is stored in the system**

If encrypted confidential information is stored in the system (including the case where symmetric-key cryptography is encrypted by public-key cryptography), it is necessary to consider re-encryption by PQC or symmetric-key cryptography in which the key is expanded. That could be a countermeasure against “store now, decrypt later attacks” (Fig. 12).

Figure 12: Point #4: If encrypted data is stored in the system, it is necessary to consider re-encryption

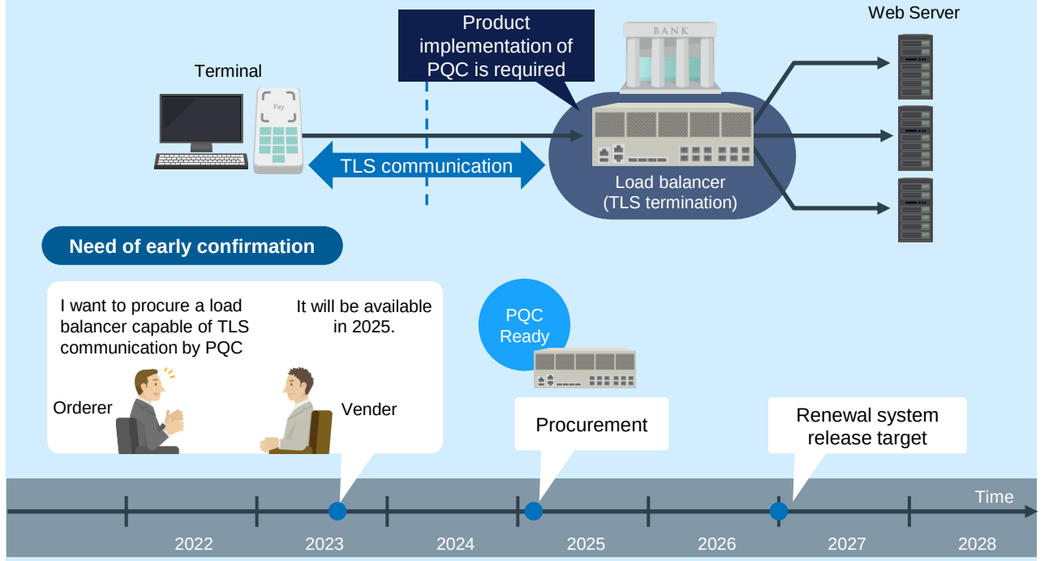


● **Point #5: If using TLS hardware, is there enough time for procurement?**

If TLS communication is terminated at the load balancer, the load balancer must be updated to support PQC because its cryptographic library resides on the load balancer hardware.

We have to grasp the procurement timing and determine whether we can make it in time for system renewal. For that reason, it is necessary to confirm with the load balancer vendor at an early stage about the timing of sales, etc. . (Fig. 13).

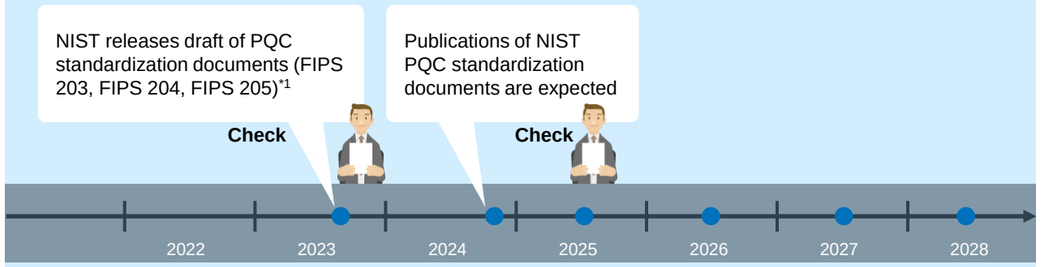
Figure 13: Point #5: If using TLS hardware, is there enough time for procurement?



● Point #6: Continuous collection of information published by NIST, SOG-IS, etc.

Even after considering the migration plan to PQC, it is necessary to pay attention to the information released by NIST and SOG-IS based on the update status of PQC safety evaluation (Fig. 14). Currently, NIST plans to publish a standardization document for post-quantum computer cryptography (PQC) around 2024 to 2025, and we need to continue to update the information.

Figure 14: Point #6: Continuous collection of information published by NIST, SOG-IS, etc.



*1 NIST, Comments Requested on Three Draft FIPS for Post-Quantum Cryptography
https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography

● Point #7: Understand the PQC functions provided by the cloud service provider

Using PQC functions provided as a service by cloud service providers (CSPs) may be an option if there is a plan to migrate all or part of the system to clouds in the next system renewal. Therefore, we should grasp the PQC development plan and current status on the CSP and decide whether to utilize the PQC related services provided by the CSP (Table 7).

PQC-related services that CSPs may provide include key management services (KMS), certificate issuing services, HSM services, and encrypted communication services. You should consider whether to utilize the services mentioned above, utilize a third-party PQC library, or a combination of both.

Table 7: Information about post-quantum computer cryptography published by major cloud service providers

AWS	• AWS Key Management Service (AWS KMS) and AWS Certificate Manager (ACM) now support PQC cryptographic algorithms CRYSTALS-KYBER, BIKE, and SIKE*1 • When connecting to AWS Secrets Manager, we now support establishing TLS in hybrid mode that combines traditional key sharing and PQC's cryptographic algorithm CRYSTALS-KYBER*2 • Participated in “Open Quantum Safe Project*3” to help develop “liboqs” library designed to promote PQC*4
Google	• SPHINCS+, which Google applied to NIST for PQC standardization, has been selected as a standard. Additionally, two entries, Classic McEliece and BIKE, progressed to the fourth round of evaluation.*5
Microsoft	• Participated in “Open Quantum Safe Project” to help develop “liboqs” library designed to promote PQC*6

*1 AWS, “AWS KMS and ACM now support the latest hybrid post-quantum TLS ciphers”, March 16th, 2022.
https://aws.amazon.com/about-aws/whats-new/2022/03/aws-kms-acm-support-latest-hybrid-post-quantum-tls-ciphers/
*2 AWS, “AWS Secrets Manager connections now support the latest hybrid post-quantum TLS with Kyber”, August 2, 2022.
https://aws.amazon.com/about-aws/whats-new/2022/08/aws-secrets-manager-connections-support-hybrid-post-quantum-tls-kyber/
*3 The Open Quantum Safe (OQS) project
https://openquantumsafe.org/
*4 AWS, Post Quantum Cryptography, Bringing quantum resistance to AWS services and customers
https://aws.amazon.com/security/post-quantum-cryptography/
*5 Google, “How Google is preparing for a post-quantum world”, July 7, 2022.
https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world
*6 Microsoft Research, Post-quantum Cryptography
https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

Understand the urgency of migration

4. When and how to migrate?

Mosca's theorem

NIST introduced Mosca's theorem to intuitively understand the urgency of migration to PQC. Mosca's theorem was put forward by Professor Michele Mosca at the University of Waterloo, Canada. Mosca's theorem defines *x, y, z* as the following number of years.

- *x*: Number of years you want the data to remain hidden using current cryptography
- *y*: Number of years required to build a secure cryptographic infrastructure against quantum computer attacks
- *z*: Number of years it will take for a quantum computer to break existing cryptography

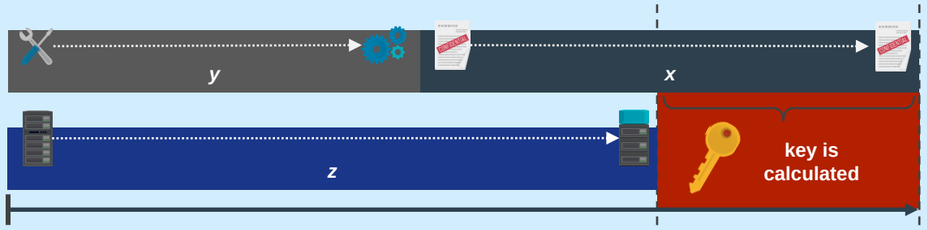
If "*x* + *y* > *z*", then there is a problem and migrating to PQC should be considered (Fig. 15). This is because the data that will be encrypted *y* years from now with "safety storage period: *x* years" may be decrypted by a quantum computer after *z* years from now without satisfying the safe storage period of *x* years.

Figure 15: Mosca's theorem

Mosca's theorem :

x	The number of years you want your data to be kept secret by current cryptography
y	Years required to build a secure cryptographic infrastructure against quantum computer attacks
z	How many years it will take for a quantum computer to break existing cryptography

In the above case, if *x* + *y* > *z*, then there is a problem.



Source: NIST, The Beginning of the End: The First NIST PQC Standards
https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

Example)

- Based on the prescribed storage period for electronic data, we set the number of years for which data should be kept confidential to 25 years. (*x*=25)
- Based on the experience of infrastructure development so far, we predicted that the number of years required to build a PQC cryptographic infrastructure will be 20 years. (*y*=20)
- He predicted that a quantum computer that can break RSA encryption would appear and become widespread 30 years from now. (*z*=30)

Since *x* + *y* = 25 + 20 > 30 (=*z*), there is an urgent need to consider migrating to PQC.

Migration to Post-Quantum Cryptography

NTT DATA has defined a migration process to PQC as a way to smoothly migrate from existing cryptography to PQC.

Migration process to PQC

1 Grasping the current situation

- Identify what information is encrypted on your IT systems and where it exists.
- Understand the cryptographic specifications such as the current cryptographic algorithm, key length, and block cipher modes of operations.
- Evaluate the impact of migration. **(Points #1 and #2)**

2 Prioritization

- Evaluate the confidentiality and importance of the information held on the IT system, as well as the period for which it should be stored safely, and prioritize items to be migrated.
- Based on Mosca's theorem, consider the impact of the “store now, decrypt later attack” and the need for migration.

3 Considering migration timing

- Consider whether you need to re-encrypt data that is encrypted and stored on your IT systems. **(Point #4)**
- When terminating TLS communication at a load balancer, find out when a load balancer that supports PQC can be procured. **(Point #5)**
- For customers and development projects, visualize the plan with a Gantt chart and coordinate the migration image.

4 Considering migration method

- Bring crypto-agility into your development process and consider whether to apply a hybrid mode of a conventional cryptography and a PQC to TLS communication. **(Point #3)**
- Decide the encryption algorithm and key length by referring to the latest guidelines of NIST and SOG-IS. **(Point #6)**
- Consider whether to utilize PQC functionality provided by a cloud service provider, utilize a third-party PQC library, or utilize both. **(Point #7)**

NTT DATA Group helps customers migration to PQC

Due to the rapid development of information technology, our lives and businesses are becoming more and more digital, and the importance of data is increasing. Companies now handle a lot of confidential information, and protecting that information is essential. Risk management for cyber security has become one of the most important management issues.

The cryptographic technology used in current IT systems may be deciphered in the future with the development of quantum computers. The move to post-quantum computer cryptography (PQC) is therefore a key challenge for companies that handle sensitive information. Companies need to have a proper plan for the migration to PQC in view of the development of quantum computers.

NTT DATA Group utilizes advanced technology to realize forward-looking business transformation together with customers. Furthermore, we aim to become a long-term trusted partner for our customers by realizing business innovation and solving social issues together. In order to protect customer information, we have experts with extensive knowledge and experience in cryptographic technology including PQC.