Special Issue 12

Issues for the Transition to Post-Quantum Cryptography

Tadahiko ITO

abstract

In modern society, a wide variety of information is protected with various cryptographic mechanisms. Among these cryptographic mechanisms, there are some that can be broken by a quantum computer of the future, that is to say, mechanisms that are not quantum resistant. It is desirable that such cryptographic mechanisms be replaced by quantum resident cryptographic mechanisms before the Cryptographically Relevant Quantum Computer, that can break them appear. However, the migration of cryptographic algorithms generally requires high costs in terms of time and resource. Since, in particular, the transition to post-quantum cryptography is expected to be on an unprecedented scale, it should desirably be carried out in a well-planned manner after careful preparation. This paper discusses challenges in effectively carrying out the transition to quantum resident cryptographic mechanisms and the schemes that may facilitate the transition.

Keywords：post-quantum cryptography, cryptographic algorithm migration, data governance

1. Introduction

In modern society, public key cryptography is used to protect a variety of information, and it is expected that it will continue to be used for even more diverse purposes in the future[(1)]. However, it has been pointed out that there is a threat of Cryptographically Relevant Quantum Computer (CRQC) in the future, and existing public key cryptography can be compromised (broken) by them[(2)-(6)].

There are several ways to deal with the threat with CRQC, but the most generally applicable and fundamental solution is to replace existing public-key cryptographic algorithms with post-quantum cryptographic algorithms[(7)], that is, to carry out transition to post-quantum cryptographic algorithms. However, to say the least, transition to post-quantum cryptographic algorithms cannot be completed by simply switching implemented algorithms. Transitions will be needed concurrently for various processes in the domains of operation and data management. Moreover, a variety of cryptographic technologies are widely used in society. Therefore, the transition of all those public key cryptography to post-quantum cryptography is likely to require a very long time and great resource, and there is no guarantee that it can be accomplished at reasonable cost.

Considering such circumstances, this paper will summarize the issues that are currently attracting the attention of the standardization sector and other

Tadahiko ITO Nonmember (Intelligent Systems Laboratory, SECOM CO., LTD.)
E-mail tadahi-ito@secom.co.jp
THE JOURNAL OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS Vol.106 No.11 pp.(1)-(7) November 2023

stakeholders from four perspectives : understanding the emerging situation, infrastructure migration, data management, and priority setting. The author will also discuss important points to be considered in order to be able to effectively prepare against the threat of codebreaking by quantum computers.

2. Issues around Understanding the Emerging Situation

This section discusses issues around understanding the emerging situation.

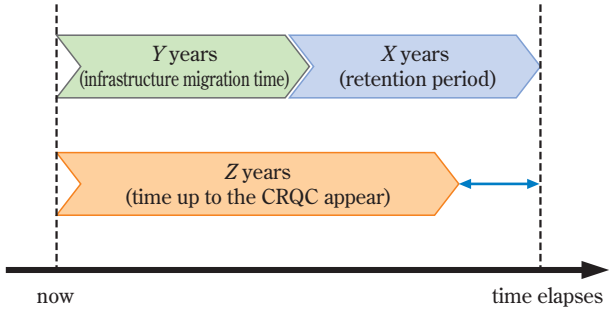

Fig. 1 Sum of the infrastructure migration time and the retention period versus the time up to the CRQC appear Derived from a paper by Mosca [8].

Issue 1-1 : Difficulty in predicting when CRQC appear and will be able to break codes

The probability of public key cryptography widely used today being compromised in the near future by attacks attempted with a quantum computer is considered small [2].

However, as Michele Mosca [8] has pointed out, we need some care if the time required to replace the executed cryptographic processes (hereafter referred to as "infrastructure migration time") plus the time over which protection by cryptography is expected for the data (hereafter referred to as "retention period") is longer than the time up to the CRQC appear. (See Fig. 1.)

If it is possible to predict with a high degree of accuracy when CRQC appear, it should be possible to a certain degree to make a risk assessment based on the timing of possible attacks and the impact of a successful attack that could be made at that point. However, on account of the possibility of innovative technological developments, there are currently many uncertainties in predictions about the development of quantum technology, making it difficult to foretell when an attack will become possible. This makes it difficult to assess the risks and develop migration plans accordingly.

Parallel implementation of relevant approaches that include the following three is considered a valid policy for effectively dealing with this issue : (1) start the transition to post-quantum cryptography as early as possible, (2) take measures to shorten the infrastructure migration time and retention period, and (3) keep on monitoring trends in the development of quantum technology.

Although NSA [Note 1] seem to have been mainly recommending (1) above [3], this choice is likely to increase the total transition cost if quantum technology progresses only slowly or if vulnerabilities are found in the standardized post-quantum cryptographic mechanisms. One should note that the total cost can become very great if (1) is applied as the sole approach for any information, including those of lower importance information.

Issue 1-2 : Information system managers are not quite aware of the cryptographic algorithms used by the information systems they manage.

As a result of the advanced development of cryptographic mechanisms, it has become possible for both users and managers of information systems to use cryptographic mechanisms without being aware of the details (or even of the existence in certain cases). Allowing people to use a variety of cryptographic mechanism without being aware of them is a remarkable aspect of the development of cryptographic mechanisms, but it can also be an obstacle to the successful planning of a transition. For example, an information system manager may not be able to identify cryptographic modules need to be renewed and, therefore, may not be able to formulate a migration plan.

As an approach that may be helpful in effectively dealing with this issue, information system managers may use discovery tools [9] to scan through the information systems that they manage to identify cryptographic algorithms used in them as well as software supply chain management mechanisms, such as those that have been developed around the Software Bill of Materials (SBOM).

Issue 1-3 : There are datasets for which an excessively long retention period has been given as well as

(Note 1) Stands for the National Security Agency of the United States.

datasets for which the retention period is not defined.

As has been mentioned in relation to Issue 1-1, whether or not a thought needs to be given to the possibility of the currently used cryptography being compromised in future, trying to find out whether we need care, depends on the sum of the infrastructure migration time and the retention period.

For example, if the data are for temporary authentication, the retention period is likely to be very short, and the need for migration will depend mostly on the infrastructure migration time. With the number of variables influencing actions reduced from three to two, the difficulty in organizing actions is expected to be lower.

On the other hand, data designated for permanent storage, for example, will need to be continuously protected beyond the time when CRQC appear. Therefore, it is likely in that case that a threat from quantum computers need to be cared. Generally, if it becomes common practice within an organization to set an extremely long retention time for data that do not need to be protected, the migration costs for that organization will further increase. This is expected to increase the difficulty in organizing actions.

The above problem arises also when datasets for which a retention period is undefined need to be handled as data designated for *permanent storage* for some reason.

To deal successfully with this issue, organizations need to appropriately practice the lifecycle management of data, trying to set the retention period appropriately in consideration of the cost for protection, and ensuring that data are eventually erased or made available for open access at an appropriate time. But then, what should be considered appropriate in this context? This will be discussed later as Issue 3-2.

3. Issues around Infrastructure Migration

This section discusses issues around infrastructure migration.

Issue 2-1 : Actions for products with low cryptographic agility

Generally, the infrastructure migration time will be relatively short if the following conditions are satisfied : the information system targeted for infrastructure migration uses standard protocols, the cryptographic module uses standard protocols, its APIs has been appropriately defined, interoperability is ensured, and the firmware including cryptographic circuits can be updated online. Conversely, when these conditions are not satisfied, the infrastructure migration time tends to be long.

In case, owing to the presence of a large number of related stakeholders, there exist interdependencies among the policies of different stakeholders, many steps may have to be taken before those interdependencies are resolved, further prolonging the infrastructure migration time.

To be able to deal effectively with this issue, information system managers may take action to have their information systems advance toward more cryptographic agility, allowing quick migration of cryptographic protocols.

Issue 2-2 : Increases in data sizes and computation volumes.

Post-quantum cryptographic algorithms consume more resources than existing public key cryptographic algorithms in at least one of the following : the data sizes of encryption keys, the data sizes of digital signatures, or the computation volume requirement.

Because of this, it has been pointed out [11] that there will be a problem, for example, with Server Hello of current specifications in TLS communication [10] since the post-quantum encryption certificates used for a server authentication process may not be stored in a single payload due to a limit to the amount of data that can be stored in the payload. Furthermore, the number of connections that can be processed simultaneously by a single Web server may decrease for such reasons as increased computation volume and deficiency in the performance of hardware acceleration circuits.

As measures to address these issues, the former problem may be resolved by the modification of protocol specifications and the latter problem by replacement by hardware of higher performance. Regarding the modification of protocol specifications, one must take note that a long time may pass before the new protocols that should replace the current ones become widely available. Regarding hardware replacement, a long time is likely to pass before replacement if the policy requires the use of hardware that has been certified under a certain program (such as CMVP [Note 2]) and hardware that satisfies the requirement does not exist yet at the

(Note 2) Stands for Cryptographic Module Validation Program.

time of planning.

Issue 2-3 : Hash processing becomes inseparable from digital signature processing.

In the case of digital signatures implemented using existing public key cryptographic algorithms (like RSA (Note 3) and ECDSA (Note 4)), the hash value of the data to be signed is calculated, and only *after* that is an asymmetric operation performed on the hash value. However, in the case of the post-quantum cryptographic mechanism that is left now as the candidate of standardization by NIST (Note 5), it is not easy to separate these two processes during the implementation of digital signatures [12].

Taking advantage that the hash operation is separable from the asymmetric operation, existing information systems often perform those operations in different environments. When an environment of particularly high security is demanded, performing the data management and hash calculation processes in a relatively low security environment while performing the key management and asymmetric operation in a relatively high security environment is a common implementation style. In that setting, Although the network connecting the two environments may be slow, there is no particular problem for the transfer of hash values.

If the post-quantum cryptographic algorithm that is left now as the candidate of standardization by NIST is to be implemented to such information systems, the computations required by digital key processing, which used to be done at two different places, likely to be done at one place, requiring major changes to the architecture. Moreover, it is possible, for example, that the degree of separation between data management authority and key management authority may drop from the current state of being quite distinct, possibly affecting governance and policy.

Issue 2-4 : Cryptographic protocols may rely on properties specific to DH-type key sharing.

Recently, when key establishment is done under communication protocols, such as TLS, it is considered desirable to implement key exchange with DH (Note 6) rather than relying on encryption by RSA. As the current TLS Cipher Setting Guidelines [13] strongly recommends the use of ECDHE (Note 7) and DHE (Note 8), offering Perfect Forward Secrecy for key exchange, such DH-type key sharing is widely used.

However, if the DH key sharing mechanism has to be implemented using the post-quantum cryptographic technique that is left now (in the category of encryption methods) as the candidate of standardization by NIST, modifications beyond the boundary of the encryption module may be required.

Since the frequency of delay in communications performed under DH-based protocols is expected to increase, it has been pointed out [11], for example, that, while the implementation of DH-based Authenticated Key Exchange requires 0.5 RTT (round-trip time), the implementation of KEM (Note 9) based Authenticated Key Exchange will require 1 RTT.

Depending on the choice of approach to modification, change of policy and/or additional functions may be required.

Issue 2-5 : Control over the status of encryption key (e.g., limiting the number of times an encryption key can be used)

Some post-quantum cryptographic algorithms impose a limit on the number of times an encryption key can be used, but some applications may require the use of an encryption key beyond that limit. Several problems may occur when a cryptographic module in an existing information system, which does not impose any limit on the number of times an encryption key can be used, is renewed with a post-quantum cryptographic algorithm that imposes a limit on the number of times an encryption key can be used.

For example, when an on-premises HSM (Note 10) is used, the user may need to add an operation to track the number of times a key has been used.

When an algorithm like LMS (Note 11) that requires status management is run on HSM, the status in the HSM in

(Note 3) A public key algorithm named after Rivest, Shamir, Adleman.
(Note 4) Stands for Elliptic Curve Digital Signature Algorithm.
(Note 5) Stands for National Institute of Standards and Technology of the United States.
(Note 6) A public key algorithm named after Diffie, Hellman.
(Note 7) Stands for Elliptic Curve Diffie-Hellman Ephemeral, where "ephemeral" signifies the temporary use of a disposable key.
(Note 8) Stands for Diffie-Hellman Ephemeral, where "ephemeral" signifies the temporary use of a disposable key.
(Note 9) Stands for Key Encapsulation Mechanisms.
(Note 10) Stands for Hardware Security Module, which is to say, hardware that performs encryption key management and cryptographic processing.
(Note 11) Stands for Leighton-Micali Signature, a hash function based digital signature method.

operating service and the status in HSMs in backup systems must be synchronized by some means where the frequency of communication between the HSM in operating service and HSMs in backup systems may increase significantly. Some backup systems are kept in very strictly isolated environments and are intended to be used only in severe crises. If synchronization with such systems has to be performed (frequently, depending on case), various precautions will be required.

Issue 2-6 : Intellectual property clearance

When standardizing post-quantum cryptographic algorithms, NIST performs investigations on intellectual properties involved in the use of the cryptographic algorithms to make sure that they do not impede the use of those cryptographic algorithms. It is surmised that, as a result of such investigations, it will be unlikely for any party implementing the postquantum cryptographic algorithms to inadvertently commit intellectual property right infringement at least in the United States.

However, the NIST's capability in such investigations is likely to be somewhat limited in regions outside the United States. Providers of services to multiple countries, for example, may perform additional investigations before starting to use the post-quantum cryptographic algorithms.

Issue 2-7 : Policy migration

During the period of transition from an old system to a new system with the renewal of cryptographic algorithms, a common practice is to run the new and old systems in parallel. However, there is an issue in how to deal with differences in outputs between the new system and the old system.

For example, consider a case where the same content is given two types of digital signatures : one implemented using an existing algorithm and another using a post-quantum cryptographic algorithm. Then, if the verification result differs between the two digital signatures, namely, one accepted while another is rejected, how this should be treated can differ from case to case. That is to say, one might decide that the two digital signatures must both be accepted before access is permitted, or one might decide that access should be permitted when either one of the digital signatures is accepted. On one hand, one may decide to rely more on the digital signature implemented using the post-quantum cryptographic algorithm based on the reasoning that the old algorithm is strongly under the threat of being compromised. On the other hand, one may conversely decide to rely more on the existing algorithm based on the reasoning that the post-quantum cryptographic algorithm, being still young, has not been sufficiently evaluated. Which of these decisions to adopt will depend on the development trends of related technologies, for example. Therefore, the practice of deciding on the policy already in the design stage, which has been common in the design of existing information systems, is expected to become hardly applicable. Because of such concerns, it would be more effective in the design of information systems that make use of post-quantum digital signatures to be prepared to dynamically renew and transition the policy concerning signature verification (which of the above-mentioned decisions to be adopted) from time to time in consideration of trends in society.

Note that, as the number of stakeholders included in the expected verifiers increases, the dynamic renewal of the signature verification policy and the policy transition become more difficult.

4. Data Management Issues

This section discusses issues around data management.

Issue 3-1 : Need to assess the value of cryptographically protected data

As mentioned at the beginning of this paper, replacing all of the public key cryptography that is widely used in society by post-quantum cryptography is likely to require an extremely long time and great resource. A situation like this requires setting priorities and taking action in order according to priority. Information that would be particularly useful in setting priorities includes the value of the data being protected and the length of time the data should be retained. The value of data can rise and fall as a result of changes in society and with the passage of time, but if data are classified appropriately, it should help timely and effective assessment of the value of the data. On the other hand, if the data being protected have not been categorized, it will be difficult to estimate the impact of a data leak, for example, and it will also be difficult to set priorities.

Data classification is a very important element in strengthening governance, and its importance in properly operating a zero-trust network has also been pointed out[14]. Therefore, allocating a budget to data

classification can be expected to have benefits beyond the context of post-quantum preparedness.

Issue 3-2 : Inadequacy in data lifecycle management

It is extremely important to implement appropriate life cycle management for every set of data so that it may eventually be erased, made available for open access, or archived after anonymous processing at the appropriate times, and making them no longer protected by cryptography. Data placed under appropriate lifecycle management would be expected to allow cryptography renewal at reasonable cost.

On the other hand, as has been mentioned in relation to Issue 1-3, if it becomes common practice within an organization to set an extremely long retention time for data that do not need to be protected, the migration costs for that organization will further increase. Thus, inadequacy in data lifecycle management can be a serious issue hindering the smooth transition to post-quantum cryptography.

5. Priority Setting Issue

This section discusses the priority setting issue.

Issue 4 : Priority setting

As has been stated repeatedly in this paper, replacing all of the public key cryptography that is widely used in society by post-quantum cryptography is likely to require an extremely long time and great resource. Setting priorities is essential to being able to take action effectively in such a situation. However, setting priorities appropriately requires a variety of specialized knowledge.

For example, a system that solely handles data for authentication purposes, for which the retention period is extremely short, may require nothing more than the implementation of measures to improve cryptographic agility (on account of Issue 2-1) and the monitoring of trends in the development of quantum computers. On the other hand, where there is a need to protect valuable data for a long time, it may be advisable to first complete the classification of data and then to take action giving higher priorities to data with longer retention periods.

Also note that some of the solutions presented in this paper cannot be implemented until post-quantum cryptography is standardized or implemented, while others, such as data classification, can be implemented immediately. Therefore, when setting priorities, it is desirable to take into account the possible start time.

6. Conclusion

The transition to post-quantum cryptography is expected to be a prolonged effort requiring a long time and great resource. Since, at present, the prospects for the development of quantum-related technologies are not clear, actions must be taken on the basis of uncertain grounds. Evaluating the balance between costs and effects in such circumstances involves many difficulties. However, we must not neglect preparations for efficient renewal in cryptography. Specifically, in the academic sector, efforts should be made to ascertain trends in the development of quantum computers and to study mechanisms that enable safe and more efficient data protection. In the industry sector, it is recommended that managers regularly monitor the status of the information systems that they manage, set priorities for migration, and then prepare for transition to new cryptographic algorithms and make efforts to strengthen data governance. May this paper be of some help in pursuing such initiatives.

References

文　　献

（1） 伊藤忠彦，国井裕樹，“暗号鍵管理によるデータ保護効率の観点から見たトラストや暗号技術の発展とこれから，” 2023 Symposium on Cryptography and Information Security, no. 2B4-3, Jan. 2023.

（2） CRYPTREC, 注意喚起情報，“現在の量子コンピュータによる暗号技術の安全性への影響，” CRYPTREC ER-0001-2019, 2020.

（3） National Security Agency, “Announcing the commercial national security algorithm suite 2.0,” U/OO/194427-22, 2022.

（4） M. Pecen, “Chairman's report for 2018 : ETSI cyber working group for quantum safe cryptography,” presentation at ETSI/IQC Quantum Safe Workshop, European Telecommunications Standards Institute, 2018.

（5） 伊藤忠彦，“量子コンピュータの公開鍵基盤に与える影響と対策，” 2018 Symposium on Cryptography and Information Security, no. 3A3-6, Jan. 2018.

（6） 伊藤忠彦，宇根正志，清藤武暢，“量子コンピュータによる脅威を見据えた暗号の移行対応，” institute for Monetary and Economic Studies, Bank of Japan, IMES discussion paper series, 2019-J-15, Aug. 2019.

（7） NIST, “Report on post-quantum cryptography,” NISTIR 8105, 2016.

（8） M. Mosca, “Cybersecurity in a quantum world : will we be ready? workshop on cybersecurity in a post-quantum world,” April 2015. https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

（9） NIST NCCoE, “Migration to post-quantum cryptography : preparation for considering the implementation and adoption of quantum safe cryptography,” NIST SP1800-38A, 2023.

（10） E. Rescorla, “The transport layer security (TLS) protocol version 1.3,” IETF RFC 8446, 2018.

（11） M. Ounsworth, “PQC at the internet engineering task force (IETF),” Post-Quantum Cryptography Conference, Ottawa, Canada, March 2023.

(12) J. Xiao and T. Ito, "Performance comparisons and migration analyses of lattice-based cryptosystems on hardware security module," Cryptology ePrint Archive, Paper 2020/990, Jan. 2021 (revised).
(13) CRYPTREC, "TLS 暗号設定ガイドライン," CRYPTREC GL-3001-3.0.1, 2020.
(14) NIST NCCoE, "Implementing data classification practices," NIST SP 1800-39A, 2023.

(Paper accepted on June 1, 2023, and finalized on June 16, 2023.)

Tadahiko ITO

In 2005, completed the master's program at the Graduate School of Science and Engineering, the University of Tsukuba. In 2012, withdrew from graduate school after the completion of credits at the Doctoral Program of Systems and Information Engineering, the University of Tsukuba. Joined SECOM CO., LTD., in the same year. Since then, engaged in research, policy management, and standardization in the fields of root certification authorities and cryptographic key management. Currently serves as senior researcher at the company's Intelligent Systems Laboratory. Member of the CRYPTREC Cryptographic Technology Research Working Group (Post-quantum Cryptography). Has engaged in the authoring of IETF RFC 8813, IETF RFC 9295, IETF RFC 9336, and other publications.