# Getting Ready for Post-Quantum Cryptography:

## *Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms*

William Barker
*Dakota Consulting*
*Gaithersburg, MD*

William Polk
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Murugiah Souppaya
*Computer Security Division*
*Information Technology Laboratory*

May 26, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.05262020-draft

National Institute of
Standards and Technology
U.S. Department of Commerce

## Abstract

Cryptographic technologies are used throughout government and industry to authenticate the source and protect the confidentiality and integrity of information that we communicate and store. The paper describes the impact of quantum computing technology on classical cryptography, particularly on public-key cryptographic systems. This paper also introduces adoption challenges associated with post-quantum cryptography after the standardization process is completed. Planning requirements for migration to post-quantum cryptography are discussed. The paper concludes with NIST's next steps for helping with the migration to post-quantum cryptography.

## Keywords

cryptography; crypto agility; crypto transition; digital signatures; post-quantum cryptography; public-key encryption; key establishment mechanism (KEM); quantum resistant; quantum safe.

## Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

## Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the National Cybersecurity Center of Excellence (NCCoE) and Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

## Public Comment Period: *May 26, 2020 through June 30, 2020*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: applied-crypto-pqc@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

## Table of Contents

# Cryptographic Technologies

Cryptographic technologies are used throughout government and industry to authenticate the source and protect the confidentiality and integrity of information that we communicate and store. Cryptographic technologies include a broad range of protocols, schemes, and infrastructures, but they rely on a relatively small collection of cryptographic algorithms. Cryptographic algorithms are the information transformation engines at the heart of these cryptographic technologies.

Cryptographic algorithms are mathematical functions that transform data, generally using a variable, or key, to protect information. The protection of these key variables is essential to the continued security of the protected data. In the case of symmetric cryptographic algorithms, the same key is used by both the originator and recipient of cryptographically protected information. Symmetric keys must remain secret to maintain confidentiality; anyone with the key can recover the unprotected data. Asymmetric algorithms require the originator to use one key and the recipient to use a different but related key. One of these asymmetric keys (the private key) must be kept secret, but the other key (the public key) can be made public without degrading the security of the cryptographic process. These asymmetric algorithms are commonly called public-key algorithms.

Symmetric algorithms offer efficient processing for confidentiality and integrity, but key management (i.e., establishing and maintaining secrets known only to the communicating parties) poses a challenge. Symmetric algorithms offer weak proofs of origin since either party to an exchange can calculate the transformation. Asymmetric algorithms generally require more processing operations and time than are practical for providing confidentiality protection for more than very small volumes of data. However, these algorithms are practical for cryptographic key establishment and digital signature processes. In the case of public-key cryptography, one of the keys in a pair can be made public, and distribution of private keys is not needed. Asymmetric key algorithms can be used to establish pairwise keys and authenticate an entity and/or data source in many-to-many communications without demanding a secret channel for key distribution. As a result, most cryptographic entity or data source authentication and key establishment functions use public-key cryptography.

## Impact of Quantum Computing Technology on Classical Cryptography

From time to time, the discovery of a cryptographic weakness, constraints imposed by dependent technologies, or advances in the technologies that support cryptanalysis make it necessary to replace a legacy cryptographic algorithm. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. While some components of some systems tend to be replaced by improved components on a relatively frequent basis (e.g., cell phones), other components are expected to remain in place for a decade or more (e.g., components in electricity generation and distribution systems). Communications interoperability and records archiving requirements introduce additional constraints on system components. As a general rule, cryptographic algorithms cannot be replaced until all components of a system are prepared to process the replacement. Updates to protocols, schemes, and infrastructures must often be implemented when introducing new cryptographic algorithms. Consequently, algorithm replacement can be extremely disruptive and often takes decades to complete.

Continued progress in the development of quantum computing—a technology required to support cryptanalysis using Shor's algorithm—foreshadows a particularly disruptive cryptographic transition. All widely used public-key cryptographic algorithms are theoretically vulnerable to attacks based on Shor's algorithm, but the algorithm depends upon operations that can only be achieved by a large-scale quantum computer. Practical quantum computing, when available to cyber adversaries, will break the security of nearly all modern public-key cryptographic systems.

Consequently, all secret symmetric keys and private asymmetric keys that are now protected using current public-key algorithms as well as the information protected under those keys will be subject to exposure. This includes all recorded communications and other stored information protected by those public-key algorithms. Any information still considered to be private or otherwise sensitive will be vulnerable to exposure. The same is true with respect to an undetected modification of the information.

Once exploitation of Shor's algorithm becomes practical, protecting stored keys and data will require re-encrypting with a quantum-resistant algorithm and deleting or physically securing "old" copies (e.g., backups). Integrity and sources of information will become unreliable unless they are processed or encapsulated (e.g., re-signed or timestamped) using a mechanism that is not vulnerable to quantum computing-based attacks. Nothing can be done to protect the confidentiality of encrypted material that was stored by an adversary before re-processing.

Many cryptographic researchers have contributed to the development of algorithms whose security is not degraded by Shor's algorithm or other known quantum computing algorithms. These algorithms are sometimes referred to as quantum-resistant, but our understanding of quantum computing's capabilities is almost certainly incomplete. This paper refers to cryptographic algorithms designed for a world with practical quantum computing as "post-quantum algorithms."

# Post-Quantum Cryptography

As reflected in NIST's April 2016 *Report on Post-Quantum Cryptography* (NISTIR 8105[1]), work on the development of post-quantum public-key cryptographic standards is underway, and the algorithm selection process is well in-hand.[2] Algorithm selection is expected to be completed in the next year or two, and work on standards and implementation guidelines will proceed expeditiously. However, experience has shown that, in the best case, 5 to 15 or more years following the publication of cryptographic standards will elapse before a full implementation of those standards is completed. Unfortunately, the implementation of post-quantum public-key standards is likely to be more problematic than the introduction of new, classical cryptographic algorithms. In the absence of significant implementation planning, it may be decades before the community replaces most of the vulnerable public-key systems currently in use.

The most critical functions that currently require public-key cryptography are key establishment (i.e., the secure generation, acquisition, and management of keys) and digital signature applications. It would be ideal to have "drop-in" replacements for quantum-vulnerable algorithms (e.g., RSA and Diffie-Helman) for each of these purposes. There are multiple candidate classes for post-quantum cryptography (e.g., solving the shortest vector problem in a lattice, learning with errors, solving systems of multivariate quadratic equations over finite fields, finding isogenies between elliptic curves, decoding problems in an error-correcting code, stateful and stateless hash-based signatures, and signatures using symmetric-key primitives). Unfortunately, each of the candidate post-quantum algorithm classes has at least one requirement for secure implementation that makes drop-in replacement unsuitable.

For example, some candidates have excessively large signature sizes, involve excessive processing, require very large public and/or private keys, require operations that are asymmetric between sending and receiving parties and require the responder to generate a message based on the initiator's public value, and/or involve other uncertainties with respect to computational results. Depending on the algorithm and the operation using that algorithm, secure implementation may need to address issues such as public-key validation, public-key re-use, decryption failure even when all parameters are correctly implemented, and the need to select new auxiliary functions (e.g., hash functions used with public-key algorithms for digital signature). Even where secure operation is possible, performance and scalability issues may demand significant modifications to protocols and infrastructures.

[1] Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner RA, Smith-Tone D (2016) *Report on Post-Quantum Cryptography*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8105. https://doi.org/10.6028/NIST.IR.8105.

[2] National Institute of Standards and Technology (2020) *Post-Quantum Cryptography*. Available at: https://www.nist.gov/pqcrypto.

## Challenges Associated with Post-Quantum Cryptography

As discussed in Lidong Chen's article, "Cryptography Standards in Quantum Time: New wine in an old wineskin?",[3] it is likely that future post-quantum cryptographic standards will specify multiple algorithms for different applications because of differing implementation constraints (e.g., sensitivity to large signature size or large keys). For example, the signature or key size might not be a problem for some applications but be unacceptable in others. In such cases, NIST standards could recognize the need for different applications to deploy different algorithms. On the other hand, existing protocols might need to be modified to handle larger signatures or key sizes (e.g., using message segmentation). Implementations of new applications will need to accommodate the demands of post-quantum cryptography and allow the new schemes to adapt to them. In fact, post-quantum cryptographic requirements may actually shape some future application standards.

The replacement of algorithms generally requires changing or replacing cryptographic libraries, implementation validation tools, hardware that implements or accelerates algorithm performance, dependent operating system and applications code, communications devices and protocols, and user and administrative procedures. Security standards, procedures, and best practice documentation need to be changed or replaced as do installation, configuration, and administration documentation. When a decision is made to replace an algorithm, it is necessary to develop a playbook that takes all of these factors into consideration. Some elements of the playbook are dependent on the characteristics of the algorithm(s) being replaced and the characteristics of the replacement algorithm(s). Other elements necessary to the development of a detailed migration playbook (e.g., discovery and documentation of systems, applications, protocols, and other infrastructure and usage elements that use or are dependent on the algorithm(s) being replaced) can be determined before the replacement algorithms are finally selected and documented.

In any case, a prerequisite for migrating from the current set of public-key algorithms to post-quantum algorithms is to identify where and for what purpose public-key cryptography is being used. Public-key cryptography has been integrated into existing computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures, and access control mechanisms. Information technology and operations technology systems are dependent on public-key cryptography, but many have no inventory of where that cryptography is used. This makes it difficult to determine where and with what priority post-quantum algorithms will need to replace the current public-key systems. Tools are urgently needed to facilitate the discovery of where and how public-key cryptography is being used in existing technology infrastructures. Examples of some uses of public-key cryptography include:

- Digital signatures used to provide source authentication and integrity authentication as well as support the non-repudiation of messages, documents, or stored data

[3] Chen L (2017) Cryptography Standards in Quantum Time: New Wine in an Old Wineskin? *IEEE Security & Privacy* 15(4):51-57. https://doi.org/10.1109/MSP.2017.3151339

- Identity authentication processes used to establish an authenticated communication session or authorization to perform some action
- Key transport of symmetric keys (e.g., key-wrapping keys, data encryption keys, and message authentication keys) and, optionally, other keying material (e.g., initialization vectors)
- Privilege authorization processes

Similarly, cybersecurity standards and guidelines and the operational directives and mandates derived from them generally specify or presume the use of public-key cryptography. There is currently no inventory that can guide updates to the standards, guidelines, and regulations necessary to accommodate the migration to post-quantum cryptography.

## Planning for Migration to Post-Quantum Cryptography

Determining where migration to post-quantum cryptography will be required involves certain initial discovery steps for the development of migration roadmaps. These include the identification of affected IT standards by traditional standards-developing organizations (SDOs) and consortia and the identification of critical applications and protocols on both an enterprise and sector-wide basis. Examples include:

- Outreach to standards organizations to raise awareness of necessary algorithm and dependent protocol changes (e.g. IETF, ISO/IEC, ANSI/INCITS X9, TCG)
- Discovery of all instances where Federal Information Processing Standards[4] and NIST Special Publication 800-series documents[5] will need to be updated or replaced
- Identification of automated discovery tools to assist organizations in identifying where and how public-key cryptography is being used in systems that are connected to data centers and distributed network infrastructures
- Development of an inventory of where and for what public-key cryptography is being used in key enterprises

Once SDOs and consortia have discovered the set of standards rendered insecure by quantum computing (e.g., standards reliant on RSA signatures) or incomplete due to the introduction of post-quantum algorithms (e.g., configuration guidelines), they can begin the process of prioritizing work. In addition, standards bodies may wish to develop implementation strategies to guide future work. For example, architectural documents for a post-quantum version of a critical protocol could be developed after identifying an appropriate candidate algorithm class (e.g., lattice algorithms) even before the specific algorithm has been selected.

Once an enterprise has discovered where and for what it is employing public-key cryptography, the organization can determine the use characteristics, such as:

- Current key sizes and hardware/software limits on future key sizes and signature sizes
- Latency and throughput thresholds
- Processes and protocols used for crypto negotiation
- Current key establishment handshake protocols
- Where each cryptographic process is taking place in the stack
- How each cryptographic process is invoked (e.g., a call to a crypto library, using a process embedded in the operating system, calling to an application, using cryptography as a service)
- Supplier(s) and owner(s) of each cryptographic hardware/software/process
- Source(s) of keys and certificates
- Contractual and legal conditions imposed by and on the supplier
- Intellectual property impacts of the migration

---

[4] See https://csrc.nist.gov/publications/fips.
[5] See https://csrc.nist.gov/publications/sp800.

- Sensitivity of the information that is being protected

This work could be extended to sector-specific use characteristics once sufficient enterprises have performed this discovery step to ensure representative results.

Once these characteristics have been identified, it may be possible to postulate future requirements and priorities. It is possible that derivation of requirements can be assisted by using the current libraries for anticipated post-quantum algorithms and conformance tools (e.g., known answer tests for anticipated post-quantum algorithms). Cryptographic algorithm migrations need to be orchestrated. Any migration playbook will need to consider interoperability requirements as well as the sensitivity of the information. Any development of enterprise requirements and priorities needs to take user requirements and customer requirements into consideration.

Once future requirements have been postulated, the results can be used to identify appropriate algorithms from the set that is selected for standardization. Where the requirements are defined early enough, they can be fed into the standards development and coordination process and the processes for developing implementation guidelines, recommendations, and protocols. Where it is not currently underway, the initial discovery effort should begin as soon as possible.

We cannot accurately predict when a quantum computer capable of executing Shor's algorithm will be available to adversaries, but we need to be prepared for it as many years in advance as is practical. As previously stated, when that day comes, all secret and private keys that are protected using the current public-key algorithms—and all available information protected under those keys—will be subject to exposure. We need to determine where, why, and with what priority vulnerable public-key algorithms will need to be replaced, and we need to understand the constraints that apply to specific use cases. These initial steps in developing and implementing algorithm migration playbooks can and should begin immediately.

## Next Steps

NIST is planning to hold a public workshop in the near future to address these and other considerations associated with the development of roadmaps for migrating from legacy cryptographic algorithms to replacement algorithms. The final paper and the findings from the workshop will help NIST and industry partners develop guidance for a migration playbook.

We invite your participation in the Cryptographic Applications community of interest and your suggestions regarding this white paper, workshops, and other near-term activities like the migration playbook. Please join the community of interest by sending an email to applied-crypto-pqc@nist.gov.