Carnegie Mellon University
Software Engineering Institute

POST-QUANTUM CRYPTOGRAPHY AND IMPLICATIONS FOR SYSTEM ACQUISITION

Robert Cunningham, Linda Parker Gates, Fred Schenker, Eileen Wrubel

April 2021

Abstract

The US National Institute of Standards and Technology (NIST) is running an open standardization process to select the next generation of public-key cryptosystems. These new cryptosystems are designed to be resistant to attacks from large-scale quantum computers, if such systems can be built. NIST's schedule has the draft standards becoming available in 2022/2024, and has announced a small number of round three candidates that can be experimented with, so it is time for the acquisition community to start to develop an acquisition strategy for select current and future systems. Careful planning to ensure *crypto agility* in today's systems will save the US Government and our closest allies significant money, and it will also enable a more rapid transition to post-quantum cryptography, ensuring the security of systems and communications. This paper provides pointers for a post-quantum framework for near-term and long-term acquisitions, and provides initial ideas to help acquisition professionals.

Introduction and Motivation

Public-key cryptosystems are widely used today to enable secure communication and authentication. The most widely used public-key systems: RSA (based on the difficulty of factoring large bi-prime numbers) and Diffie-Hellman and Elliptic Curve Cryptography (ECC) (based on the difficulty of the discrete log problem), will be broken if a sufficiently powerful quantum computer can be built. To address this, the US National Institute of Standards and Technology (NIST) is running a standardization process to select the next generation of public-key cryptosystems. New algorithms are being designed for key-establishment and encryption as well as for digital signatures. These new cryptosystems are designed to be resistant to attacks from large-scale quantum computers, if such systems can be built [1]. Recent advances [2] and announced plans [3] show evidence of progress and planning to build increasingly larger quantum computers.

While we don't know when systems of sufficient scale and capability will be available to break today's cryptography, experience shows that it takes a long time to deploy our modern cryptographic algorithms. For example, it has taken years to see adoption of SHA-2 [4] and nearly a decade to adopt ECDSA after standardization.

The NIST standardization process includes time to experiment with the proposed algorithms, to find weaknesses and to assess the overhead associated with the new algorithms. The algorithms have been evaluated against criteria that includes security (is the new algorithm at least as secure as past classical algorithms?), performance (can the operation be performed rapidly, using storage equal or less than earlier algorithms?), design (how easy is it to directly replace earlier ciphers?). Other desirable properties are also considered, including support for perfect forward security, side-channel attack resistance, and flexibility[5]. The goal is to have a design amenable

to *cryptographic agility*, which means that one cypher suite can easily be replaced by another, without making significant changes to the system's infrastructure. After multiple, careful rounds of proposals, we now know that "no exact drop-in replacements have been proposed for currently deployed cryptosystems," so "future standards could specify multiple algorithms for each cryptographic primitive according to the requirements of different applications, especially to deal with nonideal characteristics such as large signature size or large keys" [6].

Doing this will require both organizational agility to anticipate and prepare for such an upgrade, and technological agility through careful software design, so the system enables easy changes [7]. (For other criteria and recommendations to speed uptake, see [8].)

The key challenge for acquisition specialists is ensuring that there is sufficient crypto agility in the systems we acquire today. This is impacted most by differences in processing power, storage, and transmitted data [5]. The impact has been demonstrated to be noticeable but modest – something that can be addressed with additional storage and with small increases in latency without requiring substantially different hardware. We observe that a consistent finding when using the post-quantum cryptography algorithms that have made it to the latest round is that they require additional computation than the predecessor algorithms. For example, Transfer Layer Security latency with the new algorithms range between 1-300% vs. the old algorithms [9], while web server throughput decreases by around 1.5x to 1.2x when serving different sized web pages [10]. In addition, they require more data to be transmitted [11]. Recently, researchers have started to estimate the space required to implement these algorithms on FPGAs [12], and to measure the performance of these algorithms on embedded systems. For these systems, the large signature sizes required by, for example, the SPHINCS post-quantum digital signature algorithm could be an issue [13].

Now that NIST has announced a small number of round three candidates, it is time for the acquisition community to start to think about how this will affect current and future systems. Careful planning today will save money and enable a more rapid transition in the future. This paper provides a framework for thinking about near-term and long-term acquisitions, and provides initial ideas to help acquisition professionals.

Problem

The US Government purchases many systems that incorporate modern cryptography. Some of these systems are used for relatively short periods of time (~5 years) or are easy to upgrade, because the general-purpose processors will support new algorithms. Examples of these systems include laptop and desktop computers. These systems can be purchased without taking any special action with regard to post-quantum cryptography.

Some systems last much longer and are often harder to upgrade. Examples of these are "Internet of Things" devices, aircraft, satellites and special-purpose embedded systems. These systems may use special purpose processors (e.g., ASICs and FPGAs) to perform cryptographic tasks, and they may not be sufficiently fast or have sufficient memory to store or process data for the new algorithms.

The post-quantum effectiveness of DoD systems should be considered in at least three types of cryptographic system acquisition and maintenance scenarios.

Legacy: Systems that last from now until new standards are announced, when the legacy public-key algorithms need to be supported.

Both: Systems that last during a time when both legacy and new algorithms need to be supported, to ensure all systems can communicate.

PQC: Systems that need only support post-quantum algorithms.

We anticipate that long-lived systems acquired or being upgraded today will fall into the "Both" case, which will have the most requirements.

Recommendations

First, the acquisition specialist has to determine which scenario they fall into by considering the lifetime of the system and the ease of upgrading that system.

If it's the *legacy* scenario because of a short lifetime or easy upgradeability, then no special acquisition language is required. However, the acquisition specialist should ensure that the system provider offers the best available security, following best practices.

The Internet Engineering Task Force (IETF) has developed useful best practice guidelines for ensuring that any Internet protocol cryptographic cipher suite can be upgraded [14]. These guidelines require that all protocols using cryptographic algorithms be designed with a mechanism to identify the algorithm or suite that is being used. It also requires that the supported key sizes be defined. Also required is that the identification mechanism be protected against integrity attacks, to prevent a man-in-the-middle attack that changes the selected suite from a secure suite to an insecure suite. Gartner also offers recommendations for designing cryptographic systems, including having developers use crypto-agile frameworks like Microsoft's recently released Cryptography API: Next Generation (CNG), and adding requirements to ensure that crypto keys are not hard-coded into an application [15].

If the system to be acquired will need to either support *both* or *PQC*, then the acquisition approach needs to consider the requirements for those conditions. These systems are likely to be embedded, real-time, safety critical computing platforms, and the transition will require careful planning and coordination, following relevant acquisition guidelines.

The following steps are recommended:

- First, verify that the system uses legacy public key cryptography. Public key cryptography is used most often for authenticating (signing and verifying) and for symmetric key establishment. These are often used for software updates and for connecting with one of a large number of devices or users, respectively.
- Next, ensure that the system is designed using best practices, such as those described by the IETF and Gartner. It may be appropriate to include the best practices as part of the acquisition documentation.

Then, ensure that the system can be upgraded, as part of the standard block upgrade. Include the ability to upgrade to post-quantum cryptographic alternatives as a requirement on the current system.

The DoD Instruction for acquisition [16] includes support for a software acquisition pathway includes modern software development processes, including Agile Software Development. It may be possible to require that multiple cryptographic suites be acquired and the transition process be demonstrated at one of the system milestones.

In many ways this leverages acquisition approaches used for system upgrades before. Here is an example of system upgrade acquisition language, modified only slightly to support upgrades to post-quantum cryptography:

> *Embedded Vehicle Reprogramming (EVR)*
> *The contractor shall ensure that EVR performs Line Replaceable Unit (LRU) reprogramming through [Specific bus] data bus communication media. The contractor shall develop the EVR application software to allow for growth of reprogramming capabilities to include new LRUs.*
>
> *The contractor shall develop EVR software in order to detect the current firmware version installed on each computing platform and compare it with the version found in the Embedded Software Package (ESP) on the Solid-State Hard Drive (SSHD). The contractor shall make the EVR software application in parallel to maintain all the existing capabilities of EVR software application.*
>
> *The contractor shall verify load module using a digital signature before allowing reprogramming to initiate in order to prevent unauthorized software or corrupted software from being installed in a LRU. LRU load modules that fail the digital signature verification will not be allowed to be installed.*
>
> *Support will be provided for upgrading the digital signature algorithm to a future algorithm defined by the NIST Post-quantum cryptography PQC effort. The upgrade process must support both algorithms, and there must be support for subsequently supporting only the PQC signature after today's algorithm is deprecated.*

In many organizations that acquire and support cyber-physical platforms, there is a cybersecurity office. The expected effort to investigate quantum-safe solutions for the platforms should be coordinated through this office. The actual work may be specific to a particular program, and performed by the cyber staff of the program office, but the results will apply to all of the PEO's platforms. As the quantum-safe solutions are implemented, there will no doubt be unique verification and validation activities required by the Government oversight agency. The lessons learned from the initial implementations will be valuable for the PEO.

Summary

NIST has announced plans to start standardizing post-quantum cryptography as soon as 2022. Some prior cryptographic algorithm suite transition has taken decades to complete. The time is now to start preparing

for that transition, by ensuring that long-lived systems purchased today that rely on public-key cryptography can be upgraded with post-quantum cryptographic algorithms at a future date.

References

[1] G. Alagic *et al.*, "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," NIST, 2020.

[2] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature,* vol. 574, no. 7779, pp. 505-510, 2019/10/01 2019, doi: 10.1038/s41586-019-1666-5.

[3] K. Wehden, I. Faro, and J. Gambetta. "IBM's roadmap for building an open quantum software ecosystem." https://www.ibm.com/blogs/research/2021/02/quantum-development-roadmap/ (accessed.

[4] E. Crockett, C. Paquin, and D. Stebila, "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH," presented at the NIST 2nd Post-Quantum Cryptography Standardization Conference, 2019.

[5] D. Moody, "The 2nd Round of the NIST PQC Standardization Process," presented at the NIST PQC Standardization Workshop, 2019. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/the-2nd-round-of-the-nist-pqc-standardization-proc/images-media/moody-opening-remarks.pdf.

[6] L. Chen, "Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?," *IEEE Security & Privacy,* vol. 15, no. 4, pp. 51-57, 2017, doi: 10.1109/MSP.2017.3151339.

[7] J. Henrey. "What is Crypto-Agility?" https://www.cryptomathic.com/news-events/blog/what-is-crypto-agility (accessed 12 April, 2021).

[8] M. J. D. Vermeer and E. D. Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," 2020.

[9] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH," presented at the CoNEXT, 2020.

[10] J. W. Bos *et al.*, "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE," presented at the ACM CCS, 2016.

[11] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," presented at the IEEE Symposium on Security and Privacy, 2015.

[12] T. Oder and T. Guneysu, "Implementing the NewHope-Simple Key Exchange on Low-Cost FPGAs," presented at the LATINCRYPT, 2019.

[13] K. Bürstinghaus-Steinbach, C. Krauß, R. Niederhagen, and M. Schneider, "Post-Quantum TLS on Embedded Systems," presented at the ASIA CCS, 2020.

[14] R. Housley, "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms," 2015.

[15] M. Horvath and D. Mahdi, "Better Safe than Sorry: Preparing for Crypto-Agility," Gartner, 2019.

[16] OUSD (A&S), "DOD Instruction 5000.02: Operation of the Adaptive Acquisition Framework," 2020.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0365