PQSHIELD

Think openly, build securely

White paper:

Quantum Computing Threat: How to Keep Ahead

PQShield

February 2021

| www.pqshield.com | PQShield Ltd, Oxford, OX2 7HT, UK

Cryptographic agility and a clear roadmap to the upcoming NIST standards are key to a smooth and secure transition.

1 Background

1.1 New Cryptography Standards

The NIST (U.S. National Institute of Standards and Technology) Post-Quantum Cryptography (PQC) Project has been running since 2016 and is now in its third, final evaluation round. This project standardizes new key establishment and digital signature algorithms that have been designed to be resistant against attacks by quantum computers. These new algorithms are intended to replace current classical-security RSA and Elliptic Cryptography (ECDH, ECDSA) standards in applications.

The particular mathematical problems that RSA and Elliptic Cryptography are based on are easy (polynomial-time solvable) for quantum computers. Unless complemented with quantum-safe cryptography, this will allow for the forgery of digital signatures (integrity compromise) and decryption of previously encrypted data (confidentiality compromise) in the future. This is a heightened risk for organizations that need to secure data for long periods of time; government organizations that handle and secure classified information have largely been the drivers of the post-quantum standardization and its adoption in the field, but banks, financial services, healthcare providers, those developing intellectual property and many others increasingly feel the need to ensure that they can protect their customers and IP – now and in the future.

1.2 Quantum Threat and Post-Quantum Cryptography

The current position of NCSC (UK's National Cyber Security Centre) and NSA (USA's National Security Agency) is that **the best mitigation against the threat of quantum computers is quantum-safe cryptography, also known as post-quantum cryptography (PQC)**. These mechanisms can be implemented using classical computers.

While the initial driver for the current NIST standardization process is post-quantum cryptography, it is expected that their new standards will become a requirement for all those doing business with the US government, and likely more widely across the world, within 3-5 years. Therefore, companies must be preparing for this business requirement, as well as the technical needs.

1.3 What's at Stake?

There are three key factors to consider:

1. Your and your customers' sensitive data, and privacy regulations with which you must comply.
2. Your future software-based security solutions that are currently being designed, and that are not Crypto-Agile. (see definition in section 2)

3. Your hardware-based solutions that have a long lifespan and that can't be updated once deployed.

Cryptography often breaks retrospectively. Important and sensitive data, even when encrypted, is constantly being stored by would-be attackers with the aim of deciphering it one day. With quantum attacks, this will be possible, and all our data will be vulnerable. This is known as *harvest now, decrypt later*.

1.4 Time for action?

According to the NIST National Cybersecurity Center of Excellence (NCCoE), that is leading the development of practices for the transition from our legacy RSA/ECC to post-quantum cryptography, the time to act is now:

> *"It is critical to **begin planning** for the replacement of hardware, software, and services that use public-key algorithms **now** so that the information is protected from future attacks"* (NCCoE, August, 2020).

This was neatly summarized by NIST in their white paper on **Getting Ready for Post-Quantum Cryptography** as follows;

"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." (NIST CyberSecurity April 2020)

There are many parts of your ecosystem that will be impacted by the change of NIST 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." (NIST CyberSecurity April 2020)

The quantum threat, its impact, and its urgency are clearly emphasized by international standardization bodies like NIST. Let's dive into the best approach for an efficient and cost effective quantum computing threat strategy that we believe companies from different sectors, including critical national infrastructure, OEMs, and others (including Banking, telecommunications, insurance, pharmaceutical, and more) should be following.

2 Roadmap to PQC

We now present a comprehensive approach for an effective Quantum Computing Threat Strategy. We start by defining hybrid/dual cryptography solutions and Crypto-Agility.

2.1 Hybrid/Dual Cryptography Solutions

NIST, which also issues industry standard FIPS certification guidelines for hardware and software cryptographic modules, approved the use of hybrid key-establishment and dual signatures in FIPS mode. So, what are they, and why are they needed?

In the transition phase, NIST allowed for combining FIPS certified solutions to be used in combination with one or more post-quantum candidates to get the best of both worlds; gaining the quantum-resistant assurance of PQC algorithms while keeping solutions FIPS certified. This is possible even before the NIST standardization process is complete, as well as in the transition phase between the standards, and is particularly important where long-lasting confidentiality and integrity are required.

2.2 Crypto-Agility

Switching from one cryptosystem to another within a given security solution may seem trivial, but is highly unlikely to be a simple drop-in task. It depends on how a certain algorithm is used/embedded into your existing security architecture and the limitations of your infrastructure. Crypto-Agile solutions smoothly allow for the replacement of deprecated algorithms, for the use of hybrid-dual solutions, and for the change in parameter sets of certain cryptosystems including their key size, ciphertext size, running time, signature size, etc. Crypto-Agility not only allows for a smooth transition between different standards, but also for a quicker response to any advances in the crypt-analysis field, with minimal disruption to the overall system.

Crypto-Agility is a mechanism by which companies can implement Hybrid-Dual Cryptography Solutions, and therefore upgrade to post-quantum cryptography safely and securely, over a reasonable period of time.

2.3 Analysis – understand your starting point

The process of migrating to Crypto-Agile systems starts with an analysis of the currently deployed systems. During this phase, post-quantum cryptography experts need to work hand-in-hand with organizations with a common goal: to identify parts of the systems that are not Crypto-Agile and to prioritize systems that must be future proofed. This process may include the following actions:

1. Security architecture review considering best practices looking at the system's reconfigurability, or potential use of hardware-software co-design to improve security and performance.
2. System scans via appropriate tools. For instance, one needs to scan TLS services in order to create an inventory of cryptographic schemes used for encryption and authentication.
3. System design that examines the applicability of using alternative, cost-effective solutions, for example, migration to cloud-hosted systems.

The output of this process should be a report containing an inventory of cryptographic solutions used by the system, a prioritized list of actions to be taken and solutions or tools to be considered.

The analysis should take into account challenges related to backward compatibility and interoperability with legacy systems or devices. The analysis should also account for adoption of hybrid systems to couple conventional public-key algorithms with post-quantum primitives to provide additional security assurance and compliance with standards such as FIPS 140-3.

2.4 Agile Implementation

Once the analysis phase is complete and the areas for correction identified, you need to provide cryptographic implementations to support changes needed. This should be done with minimal disruption to the running systems.

You will need software implementation of appropriate cryptographic libraries and APIs, designed to enable Crypto-Agility across a broad variety of requirements. The API should be able to switch between hybrid and classical key-exchange and signature schemes in a simple and efficient manner. Applications using those libraries/APIs can easily switch between hybrid and classical cryptographic schemes, by updating the cryptographic profile. Such an approach makes future transitions cost-effective; whether there is a newer version of a certain encryption scheme, a different algorithm, or a more efficient hardware-accelerated implementation, the switch can be done by updating either the configurations or the version of crypto libraries/APIs. No code changes related to the integration should be required. Such a framework can be used in each stage of the migration process - from experimentation to deployment.

Through this process, you can achieve Crypto-Agility, ensuring that you are ahead of the standards, maintaining highly secure platforms, and minimizing the cost and disruption to your company and your clients.

3 Conclusion

As NIST NCCoE recommends, the preparation for a smooth migration to PQC should start now. This is the largest change that has ever happened to the cryptography infrastructure. It takes a tremendous cryptographic expertise from hardware to software, to hardware/software co-design to be able to review, analyze, and assess the existing security/cryptography architectures that your company has across software and hardware. Moreover, any regulatory requirements that you must comply with to protect your and customers' sensitive data will have to be incorporated into the analysis. Based on the results, you will be able to develop a specific quantum threat strategy that fits your company -inevitably, this will include a post-quantum cryptography roadmap. You will then need a suitable set of Crypto-Agile solutions that would allow for a timely and smooth transition to the upcoming NIST standards of post-quantum cryptography while maintaining interoperability and backward compatibility, but without compromising security.

About PQShield

PQShield is a world leader in the development of new cryptography standards. It is leading multiple NIST finalists in post-quantum cryptography, leading projects for the Crypto Task Group at RISC-V (e.g. TRNG, AES-ISE, etc.) and contributing to the Internet Engineering Task Force (IETF).

PQShield has unrivalled expertise in evaluating cryptographic solutions deployed in large companies and across multiple systems. Alongside the expertise of some of the world's leading cryptographers, PQShield has developed a variety of tools for scanning existing services and identifying the full scope of the existing cryptographic deployment.

In order to deliver genuine Crypto-Agility, PQShield provides software solutions for mobile and server technologies (inc. PKI, TLS, VPN, HSM firmware, etc.), embedded systems (having developed a unique hardware-based secure element), and applications (including a post-quantum secure end-to-end encrypted messaging protocol). PQShield's implementations of post-quantum PKI, VPN, TLS, etc. rely on a framework that offers the maximum level of Crypto-Agility. PQShield's cryptography solutions are already in the hands of OEM customers such as Bosch.

The seven NIST PQC finalist algorithms (announced on July 22, 2020) include four key establishment algorithms and three digital signature algorithms. PQShield has a detailed understanding of all of these algorithms, having a team that has been involved in their evaluation for many years. Two of the algorithms list PQShield's crypto team members as authors; however, PQShield is an algorithm-agnostic vendor. We can provide algorithm selection guidance and also hardware and software and technology.

To discover more about Crypto-Agility and how to implement it in your environment, please contact us at contact@pqshield.com.

Table 1: Cryptography Inventory- An Example

Solution	Priority	Data type/storage	Software	Hardware	Agile	Standards	Certification
Example	H/M/L	(not) ephemeral/Cloud, etc.	✓	✗	✗	NIST, IETF..	FIPS, CC, ETSI..
TLS							
Digital Certificates							
Smart Card							
Authentication Tokens							
TEE							
HSM							
VPN							
Remote Terminal							
Cloud Services							
Secure File Transfer							
Document Management Sys.							
Backup Systems							
...							