White paper:

Quantum Computing Threat: NIST PQC standards are here... how can you keep ahead?

PQShield
Updated July 2022

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

1 Background

1.1 RSA and ECC are quantumly broken

The mathematical problems that underpin RSA and Elliptic Cryptography (ECC) are easy for quantum computers to solve using Shor's algorithm (polynomial-time solvable). 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 The HNDL attack and the dangerous three unknowns

The HNDL Attack: *Cryptography 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. In the case of quantum attacks, this is a devastating threat - all our data will be vulnerable. This is known as a 'Harvest Now, Decrypt Later' attack.*

There are three unknowns that forced intelligence agencies including the NSA to take practical action in their fight against quantum-powered attacks. Those three unknowns are as follows:

- With the unprecedented level of investment in the quantum computing field, no one can perfectly estimate the arrival date of a Cryptographically Relevant Quantum Computer (CRQC) that can break RSA and ECC.
- Early developers of CRQC might have enough motivation to keep it secret.
- Most organisations still have no clear transition roadmaps to post-quantum cryptography and therefore have no idea how long this transition will take.

1.3 New cryptography standards

The NIST (U.S. National Institute of Standards and Technology) Post-Quantum Cryptography (PQC) Project has been running since 2016 and announced its first ever PQC standards in July 2022. This project standardized new key establishment (KYBER) and 3 digital signature algorithms (FALCON, Dilithium, and SPHINCS+) that have been designed to resist attacks from quantum computers.

These new algorithms will gradually replace current classical-security RSA and Elliptic Cryptography (ECDH, ECDSA) standards in applications. This is the biggest change in our cryptography standards ever.

1.4 The change is being mandated

The current position of the NCSC (the UK's National Cyber Security Centre) and the NSA (the US 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.

In January and May 2022, White House memos called for US government agencies to identify any encryption not compliant with quantum-proof standards and provide a timeline towards transition. Separately, the French national security agency (ANSSI) recommended the immediate introduction of post-quantum defenses throughout the private sector, and Germany's BSI endorsed the use of post-quantum cryptography.

These new standards will therefore become a requirement for all those doing business with the US government and other governments across the world, likely within 3 years. All multi-national companies must prepare for this business change, as well as the technical needs.

1.5 What's at stake?

There are three key factors to consider:

1. Your and your customers' sensitive data, and the 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.

1.6 Time for action

According to the NIST National Cybersecurity Center of Excellence (NCCoE), which 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 its white paper on **Getting Ready for Post-Quantum Cryptography**:

"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 outlined 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 FIPS-certified solutions to be used in combination with one or more NIST post-quantum cryptosystem 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 transi-

tion between different standards, but also for a quicker response to any advances in the cryptanalysis 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 the potential use of hardware-software co-design to improve security and performance.
2. System scans via appropriate tools. For instance, you need 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 biggest change to cryptography in a generation, and the largest transition ever undertaken.

It takes a tremendous amount of cryptographic expertise, spanning hardware, software and hardware/software codesign, to be able to review, analyze and assess the existing security and cryptographic architectures that your company has across its hardware and software systems.

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 new NIST standards of post-quantum cryptography while maintaining interoperability and backward compatibility, but without compromising security.

About PQShield

Cryptography standards for hardware and software: PQShield is a world leader in the development of new cryptography standards. PQShield's researchers and advisory board contributed to **all** of the first international PQC NIST standards announced in July 2022.

PQShield's researchers and engineers have also led multiple projects for the Crypto Task Group at the open source hardware architecture RISC-V (e.g. TRNG, AES-ISE, etc.) and contributed to the Internet Engineering Task Force (IETF), GlobalPlatform and World Economic Forum (WEF), to name but a few.

Team and international presence: PQShield is the only cybersecurity company that can demonstrate quantum-safe cryptography on chips, in applications, and in the cloud - our solutions are already in the hands of progressive large customers such as Microchip, Collins Aerospace and Bosch.

Headquartered in the UK, with teams in the United States, France, Belgium, the Netherlands and Japan, our team is made up of many world class researchers, mathematicians and engineers – giving us the highest concentration of cryptography experts in the industry.

PQC-ready products: Our expert team has not only fed into these new global standards, but also developed significant IP for own solutions and product portfolio. These research, hardware and software IPs can be combined into use case specific implementations for chips, applications or the cloud. *For example*, PQShield can provide the following;

- FIPS 140-3 ready software IP: PQCryptoLib

  Our hybrid cryptographic library, PQCryptoLib, was the first ever submitted to be validated by the NIST Cryptographic Module Validation Program for FIPS 140-3. It consists of a library of modern cryptographic primitives designed with crypto-agility in mind to help companies transition smoothly and securely to the quantum-era, e.g., it provides support for classical and hybrid key derivation and for implementation within the TLS key schedule, supporting multiple PQC algorithms as well as many classical schemes.

- Post-quantum hardware IP: PQSubSys

  PQSubSys is a modular Hardware-Software CoDesign which delivers a post-quantum secured isolated execution environment, complete with PQC hardware co-processor, side channel protection, RISC-V crypto extensions, classical entropy source, AES and SHA2 instructions and firmware support for AES, DRBG, SHA2, HMAC, KDF and Key Wrap.

To discover more about the first PQC standards and how to implement them in your software or hardware environment in a crypto-agile way, 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							
...							