Post-Quantum Cryptographic Migration Challenges for Embedded Devices

NXP Post-Quantum Cryptography Team

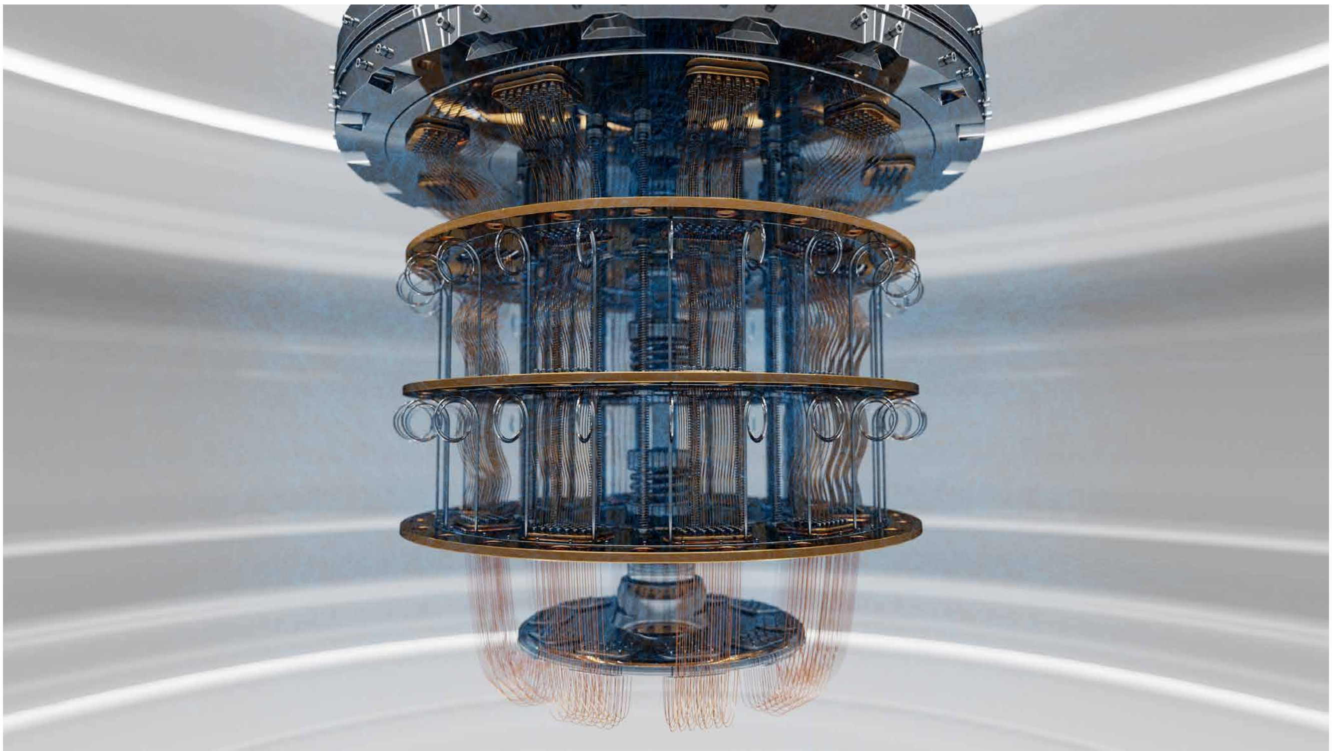


Table of Contents

White paper

Post-quantum cryptography

Executive Summary

As the digital landscape evolves, the expected arrival of quantum computing presents both opportunities and challenges, particularly in the realm of cryptography. Traditional cryptographic algorithms, designed to withstand attacks from classical computers, may become vulnerable in the face of quantum computing power. Embedded devices, which are crucial components of our modern technologic landscape, face unique migration challenges in adopting post-quantum cryptography (PQC) solutions.

This white paper explores the migration challenges to implement PQC on embedded devices. It addresses the limitations imposed by the resource-constrained nature inherent to embedded systems, including computational power, memory, and energy consumption. Furthermore, it examines the upcoming PQC standards, along with the integration complexities and performance trade-offs associated with transitioning to quantum-safe algorithms. Key considerations include the need for memory-aware, efficient implementations that minimize computational overhead while maintaining security guarantees against side-channel and fault attacks. This highlights the need for dedicated hardware solutions for resource-constrained devices.

Ultimately, successful migration to post-quantum cryptography on embedded devices requires a multidisciplinary approach, encompassing cryptographic research, hardware design, software development, and system integration. By addressing these challenges proactively, NXP is leading the way to ensure the resilience of embedded systems against emerging threats posed by quantum computing.

Security in our Digital Society

Generations have grown up in a world where computers are an essential part of day-to-day life. In this modern world, cybersecurity forms one of the key cornerstones to build trust. Security is often taken for granted. On the one hand, so-called symmetric key algorithms, such as the Advanced Encryption Standard (AES)[1], use the same key to encrypt or decrypt data and are typically used for efficient encryption of data. On the other hand, public-key algorithms, which consist of a public as well as a private key, can be used to exchange symmetric keys or produce digital signatures. Examples of the currently deployed public-key algorithms are RSA (named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman) and Elliptic Curve Cryptography (ECC)[2]. People might not realize that they make use of these cryptographic standards dozens, if not hundreds of times a day when browsing the internet, making a payment online or with a banking card, or by simply sending a message using their favorite messaging application on their phone.

A New Computing Paradigm

However, the prospect of quantum computing triggers a fundamental shift in computing and security principles. Quantum computers make use of quantum-mechanical properties such as superposition and entanglement to manipulate quantum bits (so-called “qubits”) by quantum gates. There has been slow but steady progress in the use of qubits, from the first experimental demonstration of a quantum algorithm working on two physical qubits in 1998[3] to the use of 1,121 qubits demonstrated by IBM in December 2023[4]. But the quantity of qubits being used is only one part of the story. The emphasis of research has shifted, with the aim of producing high-rate quantum error correction. IBM’s roadmap promises a “quantum system with 200 qubits capable of running 100 million gates” by the end of this decade[5].

Such commercial predictions are supported by government guidelines that can be used for risk assessment. For example, the BSI, the German Federal Office for Information Security, predicts that “cryptographically relevant quantum computers will be available early in the 2030s”[6]. A large and stable general-purpose quantum computer holds the promise to perform certain complex calculations that are intractable to the strongest supercomputers one can build. This general-purpose quantum computer has the potential to find solutions faster in many areas that are challenging today, such as materials science and pharmaceuticals. However, there are other, less positive implications, including the ability to shake the foundations of the security solutions we currently use.

As far back as 1994, Peter Shor of the Massachusetts Institute of Technology (MIT)[7] published a quantum algorithm that would undermine the security of the majority of public-key cryptographic systems used today, and in 1996, a quantum algorithm developed by the computer scientist Lov Grover[8] has a potentially significant effect on the security of symmetric cryptography and hash functions. This means that the currently used cryptographic keys or data encrypted today might be compromised whenever quantum computers become reality.

Post-Quantum Cryptography

Although limited quantum computing devices exist today, the progress of innovation has been rapid. The potential threat of large-scale impact on society has led to widespread initiatives to develop new cryptographic algorithms and standards that are expected to be secure against attacks using quantum computers.

One possible path forward is to create cryptographic methods and protocols based on quantum-mechanical principles, while not necessarily referencing the use of a quantum computer (see QKD sidebar).

Another way forward is collectively referred to as “quantum-safe cryptography” or “post-quantum cryptography,” which we will abbreviate as PQC. PQC attempts to build security solutions that can withstand attacks from both classical as well as quantum computers but does not require any quantum-enabled devices. PQC is designed to run on all the computers, IoT devices and smartcards already deployed in today’s world.

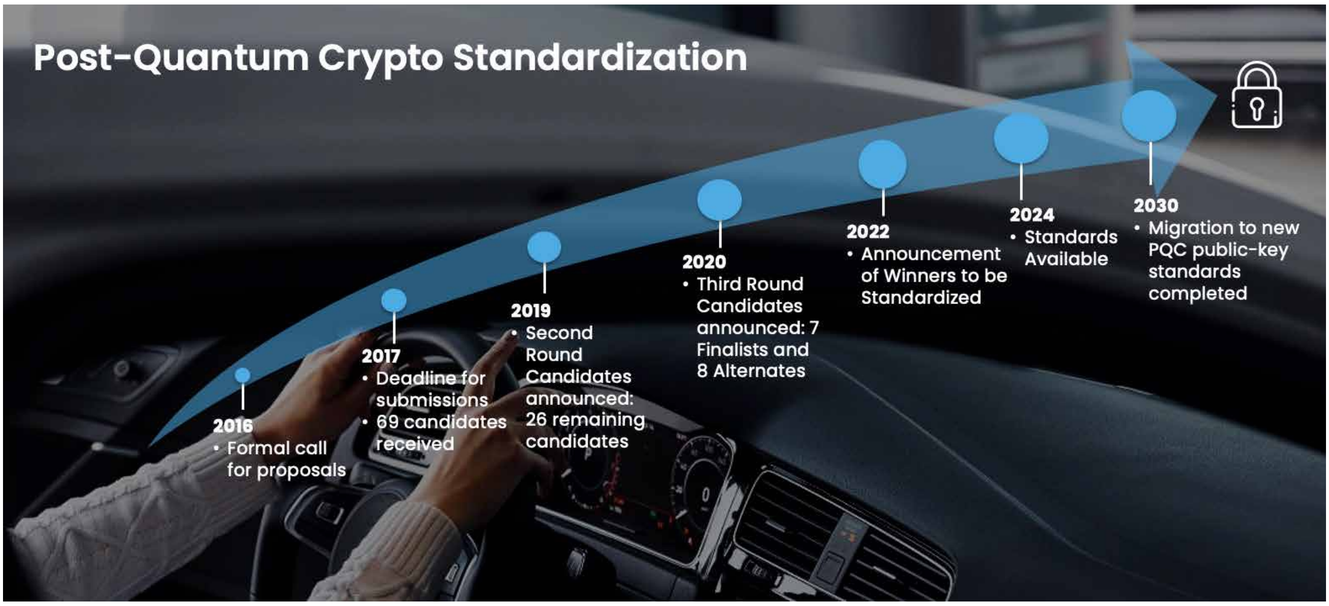
The First PQC Standards

In 2016, to prepare for a potential “crypto-apocalypse” and encourage the brightest minds around the world to develop standards for secure and efficient PQC solutions, the National Institute of Standards and Technology (NIST) in the United States issued a formal call for proposals. About a year later, 69 “complete and proper” submissions were received for the cryptographic functionalities of Key Encapsulation Mechanisms (KEMs), which enable key exchange, and digital signatures. Among the submitted schemes, six of the KEM proposals included an NXP security expert as a co-author.

Quantum Key Distribution (QKD)

One of the most prominent examples of a protocol using components of quantum mechanics is Quantum Key Distribution (QKD). With QKD, a provably secure link between two parties is established by an exchange of quantum particles such as photons over a fiberoptic link. This kind of “quantum cryptography” has the potential to offer an additional layer of defence to existing methods. As concluded by various government agencies in the European Union, “Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective.”[9]

Over the course of three rounds, the 69 schemes were pruned in 2020 to only 15. Five of six submissions that included NXP involvement were included in the final 15. At the end of a nearly six-year process, NIST announced the first selection of winners of their post-quantum cryptography standardization effort in July 2022. The NXP co-authored CRYSTALS-Kyber submission was the sole winner of the KEMs portion of the competition and will be standardized under the name ML-KEM. ML-KEM is a lattice-based proposal and was selected due to its high performance, manageable key sizes and the confidence NIST has in its lasting security capabilities[10]. Three PQC signature algorithms will be standardized as part of this outcome, as summarized in the table below. The third PQC signature algorithm FALCON (to be standardized as FN-DSA) is not included in the table because NIST will release it at a later point.


Post-Quantum Crypto Standardization
2016
• Formal call for proposals
2017
• Deadline for submissions
• 69 candidates received
2019
• Second Round Candidates announced: 26 remaining candidates
2020
• Third Round Candidates announced: 7 Finalists and 8 Alternates
2022
• Announcement of Winners to be Standardized
2024
• Standards Available
2030
• Migration to new PQC public-key standards completed

Type	Submission name	Standard name	Standard document
Key Encapsulation Mechanism (KEM)	CRYSTALS-Kyber	ML-KEM	FIPS-203: Module-Lattice-Based Key-Encapsulation Mechanism Standard[10]
Digital signature	CRYSTALS-Dilithium	ML-DSA	FIPS-204: Module-Lattice-Based Digital Signature Standard[11]
Digital signature	SPHINCS+	SLH-DSA	FIPS-205: Stateless Hash-Based Digital Signature Standard[112]

With NIST's introduction of the first PQC standards in 2024, we've reached the end of the beginning and are entering a new phase of expansion. The International Organization for Standardization (ISO) is evaluating extensions to the list of algorithms, and Korea will standardize their own PQC algorithms[13]. It is expected that other nations, including China, will follow suit.

To diversify their PQC signature portfolio, NIST recently issued an additional call for proposals. The announcement of second-round candidates is expected later in 2024[14]. These efforts are all at the algorithm level, but that's by no means the end of the story. Protocol standards for various use cases will need to be updated. These various efforts are the start of a major migration to a world that offers protection against quantum threats.

The upcoming FIPS standards are not the first PQC algorithms to be standardized. NIST SP 800-208[15] defines parameter sets for two stateful, hash-based signature schemes, Leighton-Micali Signatures (LMS) and Extended Merkle Signature Scheme (XMSS). Because LMS and XMSS are stateful, the entity creating the signature needs to maintain and synchronize a state. This makes them more suitable for firmware/software signing use cases.

Migration to Post-Quantum Cryptography

Migrating devices and systems to PQC implies a significant effort in applied research, engineering and standardization. In view of the recent advancements in the quantum-computing field and the time that such large-scale migrations can take, it is paramount to start preparing for the migration to PQC now.

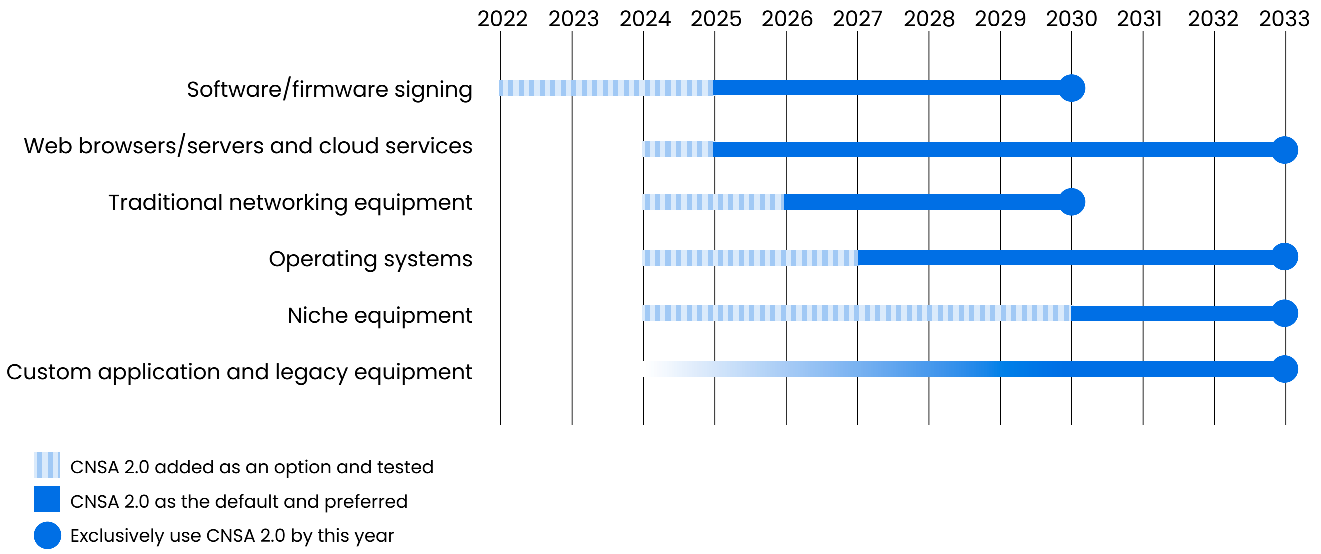
There are two main challenges to address. First, there is the need to protect confidentiality, meaning data transmitted now needs to be protected with a quantum-resistant algorithm to prevent future decryption, or what is called a "store now, decrypt later" attack. Second, there is the need to use quantum-resistant authentication, so a future adversary can't gain unauthorized access to a system and modify or replace firmware. Without these two kinds of quantum-resistant security mechanisms in place, data and devices are at risk of a quantum attack launched in the future, using a cryptographically relevant quantum computer (CRQC).

In the embedded world, we also need to consider devices that hold, process and exchange data, since many present-day devices have long lifetimes in the field. Device manufacturers need to ensure that such devices are reliable and secure throughout their lifetime, in compliance with legislation such as the upcoming Cyber Resilience Act (CRA)[16]. The firmware devices run needs to be trustworthy, as do updates to firmware or software. Digital signatures are typically used to check that firmware is genuine, as part of secure-boot operations, and that secure updates are received from a trusted source. These signatures also protect integrity, by confirming that software was not modified by a malicious party. If a future attacker with a CRQC can forge traditional digital signatures, then they can load their own software onto deployed devices and take control, with comprised security and safety issues as the result. For this reason, focusing on secure implementations of digital signatures will be as important, or even more important for some stakeholders, than key establishment and the "store now, decrypt later" threat.

Migration also needs to be done in a way that reflects the risk to ecosystem actors, with priority given to migrating the cryptography that secures the most valuable assets or underpins device security. National and international bodies are developing strategies and timelines for mandated migration, and this may lead to conflicting requirements for stakeholders that operate in multiple markets. For U.S. National Security Systems and related assets, the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) has set strict limits on the cutoff point for migration of products and devices certified to Federal Information Processing Standards (FIPS)[17].

Other agencies have similar timelines but slightly different algorithm preferences. For example, ANSSI (France) and the BSI (Germany) have emphasized their support for the NIST PQC standards but have also expressed interest in extending the list of standardized PQC algorithms.

CNSA 2.0 Timeline for USA National Security System (NSS) Requirements



Migration Challenges for Embedded Devices

Updating any system or application in a secure manner is challenging. This holds for software solutions but is even more difficult for systems which rely on specific hardware acceleration. Performance might be impacted, migration might affect interoperability, and service can experience discontinuity. For resource-constrained embedded devices, the impact is even greater. Unlike servers, which can often be assigned additional memory, constrained devices have a restricted amount of memory available. Similarly, where highly secure cloud applications often run on isolated remote machines, embedded devices have no guarantee that timing and other side-channel information is protected from misuse by malicious entities. We expand on some of these challenges in this section.

Hardware Constraints for Post-Quantum Cryptography

Hardware acceleration for cryptographic functions is a core part of present-day chip design.

Not only is hardware acceleration used for symmetric functions, like AES, and for hash functions, like SHA-2/SHA-3, it's also used for public-key cryptography, such as ECC and RSA. Hardware acceleration ensures that running cryptographic functions and protocols is not prohibitively slow, so devices stay secure while fulfilling their performance requirements.

Hardware acceleration for post-quantum cryptography is still in its infancy. Cryptographic hardware that accelerates hash computations can be re-used for schemes like ML-DSA, ML-KEM and SLH-DSA. ML-DSA and ML-KEM benefit from additional, dedicated acceleration. Designing, developing and producing dedicated PQC hardware is a process that can easily span multiple years. The NXP PQC team has led the effort to re-purpose existing ECC/RSA acceleration for PQC[18]. However, the ideal situation is to deploy dedicated PQC hardware co-processors whenever feasible.

Another hardware concern is memory. For non-volatile memory, the increased storage requirements for cryptographic keys need to be taken into account. With ECC, for instance, only 32 bytes are needed to represent a key, but with PQC the amount of memory can be orders of magnitude larger.

Scheme	Quantum-Safe?	Public Key (bytes)	Secret Key (bytes)
ECC-256	X	~32	~32
RSA-3072	X	~384	~768
ML-KEM-768	√	1184	*1216
ML-DSA-65	√	1952	4000

* The secret key for ML-KEM contains 1216 bytes required to decrypt the ciphertext and additionally the 1184-byte encapsulation key. If the public encapsulation key is not stored with the 1216 bytes for decryption then the full secret key length is 2400 bytes.

A larger challenge for embedded devices, however, is that post-quantum cryptography can, in some cases, require more working memory (RAM) and long-term storage compared to contemporary cryptography. Whereas an ECC implementation might require only a few KiB of memory[19], fast implementations of ML-DSA can easily take 50 KiB[20]. For larger devices like laptops or servers this isn't a problem, because they often have gigabytes of RAM at their disposal. For embedded devices, though, it's a different story. The secure microcontrollers used in access cards, passports and sensing can have as little as 16 KiB or even 8 KiB of RAM.

NXP is leading the effort on solutions that enable PQC on embedded devices. One of the most promising approaches involves research into low-footprint implementations of PQC schemes[21] [22]. These efforts aim to reduce memory usage to the lowest possible impact on performance. Another line of inquiry is performing feasibility studies on existing hardware for common PQC use-cases[23] to show where migration is already possible.

A Plethora of Standards

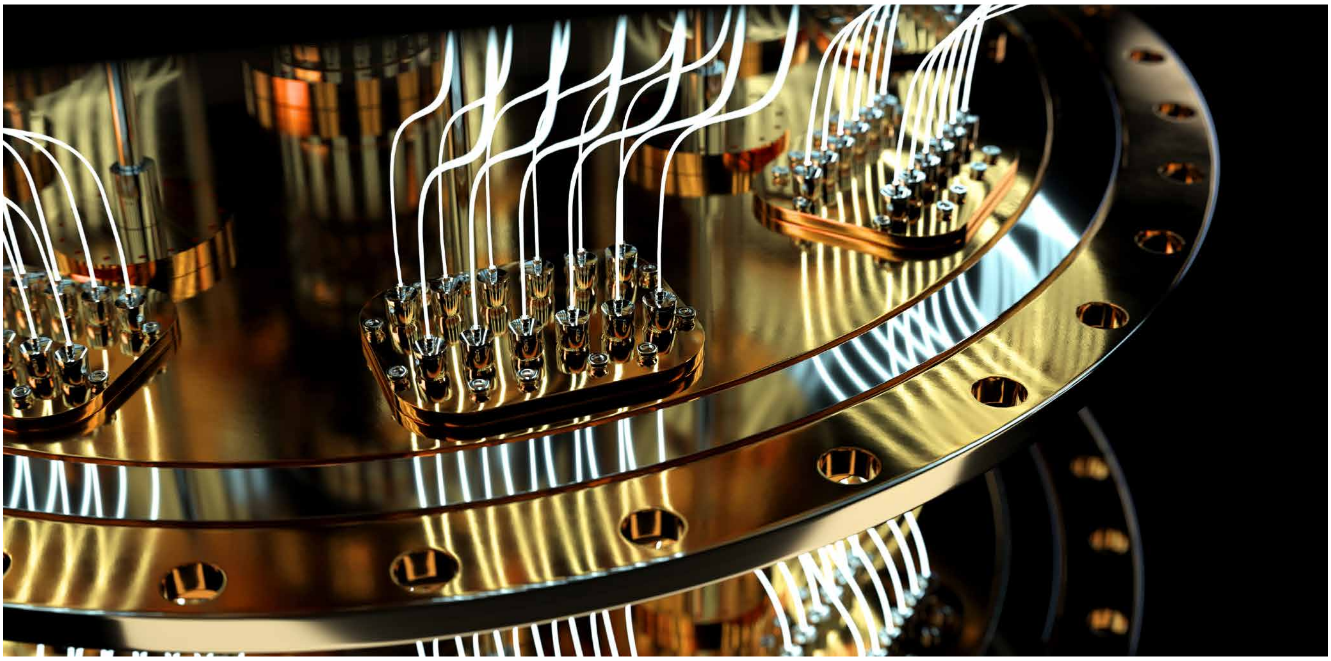
Updating contemporary cryptography to a single PQC scheme has significant consequences for the (hardware) requirements of an embedded device. But the reality is that devices will probably need to support multiple PQC standards, because there are likely to be multiple PQC standards for key establishment and digital signatures.

It does not stop there. Embedded devices are generally used for many different use cases and scenarios. Some will have use cases where ML-DSA is more suitable, others where SLH-DSA or stateful hash-based schemes such as XMSS / LMS as defined in NIST SP 800-208 are preferred. Additionally, these devices might be sold in countries that use guidelines and standards that are different from those issued by NIST. As mentioned in the introduction, different schemes are expected to be standardized in Europe and in Asia. A single chip, designed to serve different markets and regulations will need more storage space for the keys and increased code size to support multiple cryptographic algorithms. Some re-use might, of course, be possible, but compared to contemporary cryptography it's a large increase in the number of algorithms.

This challenge is made bigger by the existence of higher-level standards. Use cases often don't use cryptographic primitives directly, but instead utilize them through cryptographic protocols. For example, communication with other devices happens with Transport Layer Security (TLS) while internal chip communication is typically secured with another protocol, such as Secure Channel Protocol (SCP). Higher-level protocols are standardized by various standardization bodies to ensure interoperability between vendors.

To maintain interoperability in a PQC world, these standards need to be updated. Not only is this a process that can take many years, there's no guarantee that different standardization bodies will select the same algorithms. If embedded devices have to support multiple higher-level protocols, there might not be sufficient allocatable space for all globally supported KEMs and signatures. Developers will have to prioritize.

NXP is helping to address this challenge by actively contributing to the standards and consortia that



are standardizing the protocols that secure the world's digital and embedded infrastructure, such as the Connectivity Standards Alliance (CSA), Global Platform, the GSM Association (GSMA), the Internet Engineering Task Force (IETF) and more. By advocating for as much cross-standard uniformity as possible and making embedded-friendly choices in protocol updates, we help ensure that the protocols remain as feasible and as easy to enable on as many embedded devices as possible.

Lastly, as we will also see in the following section, chips that are developed now need to have the right tradeoffs between hardware and software support. The balance of security, performance, and flexibility needs to be designed in from the start. This makes it significantly easier to implement protocol updates in the future.

Protection Against Physical Attacks

In most applications, users of the security system can submit inputs and observe the outputs, but they can't get information about internal values, such as the secret key used by the cryptographic algorithm.

However, when we implement and deploy cryptography in a physical system, such as an embedded device, this is no longer a valid assumption(24) because secret information can be deduced by measuring the system's physical properties, such as cryptographic implementation's execution time. If the execution time of an algorithm depends on the value of the secret key, the execution time might vary, and this timing difference can reveal information about the secret key. This concept of measuring the physical characteristics of the device while it is processing secret information has been formalized under the term side-channel analysis. For this kind of analysis, other sources of information besides the timing behavior, such as the power consumption or electro-magnetic emanation, can be used as well. It is also possible to actively disturb a cryptographic computation to successfully recover sensitive information, in what's known as a fault-injection attack.

Physical threats are a serious reality. Any implementation of cryptographic schemes in an at-risk system requires dedicated countermeasures. Such measures typically impose significant overhead on memory requirements and performance, but this is outweighed by the cost and impact of a potential successful attack. With the standardized public-key cryptography of today, we know how to efficiently achieve protection against increasingly potent physical attacks. For PQC, such dedicated protections are still a topic of active research.

As a leader in high-assurance implementations of classical public-key cryptography, NXP is also contributing to the development and optimization of countermeasures for the to-be-standardized cryptographic schemes(25) (26). NXP has many cryptography and security experts who work together with leading academic researchers in this area. This effort includes investigating new side-channel and fault attacks to ensure the coverage of our countermeasures(27) (28), so we can stay ahead in this game of cat and mouse.

Updateability of Embedded Devices

Another limitation of embedded devices compared to their larger-scale counterparts is their ability to be updated. Due to their limited resources or connectivity, not all embedded devices can be updated in the field. This is especially true for the class of constrained devices such as access tokens. Additionally, even if a device has an update mechanism in place, it is still limited to the hardware acceleration, flash memory and RAM it was given in production. The update mechanism itself might also not be PQ-secure. PQC updates may not be feasible. To avoid this, we need to enable devices with PQC now, but the challenges mentioned in the previous section can make this difficult to do.

There are many inputs into the decision process for planning PQC migration or updating a device's existing implementation of asymmetric cryptography, and the process has many potential outcomes. In some cases, the data being transmitted will be relatively short-lived and of low value, meaning that even when in possession of a CRQC it would not be worth the cost to mount an attack to obtain the data. Such use cases will be regarded as low priority in a migration plan, with a higher priority given to more exposed assets, such as root certificates, which could give a successful attacker signing capabilities. The higher the risk associated with exposure, the higher the priority in the migration plan.

In other cases, the entities involved in the system will be limited in number. In this case, deploying pre-shared symmetric keys[29] (which are PQ-secure) may be a viable path to post-quantum security.

Cryptographic agility, as described below, and long-term thinking regarding security and risk, can be effective in mitigating threats before they appear.

Practical Migration Solutions

In this section we describe some of the approaches to PQC migration that span many usages of public-key cryptography. It is important to think about these approaches on a system level. Algorithms and protocols will be standardized and integrated into products and devices that will then interact with wider solutions. All links or endpoints should be assessed based on how they provide security properties to the system, rather than as individual components.

Hybrid Post-Quantum Cryptography

Hybrid PQC combines the security of a traditional scheme along with a PQC scheme. The rationale behind this approach is that, if the traditional scheme is compromised due to a CRQC, the PQC scheme can still be relied on for security. Contrarily, if the PQC scheme is compromised due to an unforeseen standard attack while no CRQC has yet been realized, the traditional scheme can be relied on for security. Many national agencies, including the German BSI[30] and the French ANSSI[31] are recommending hybrid approaches. The overhead of executing a traditional algorithm is relatively small compared to the overhead of executing a PQC algorithm. Therefore, hybrid PQC has been identified as a pragmatic solution to hedge one's bets.

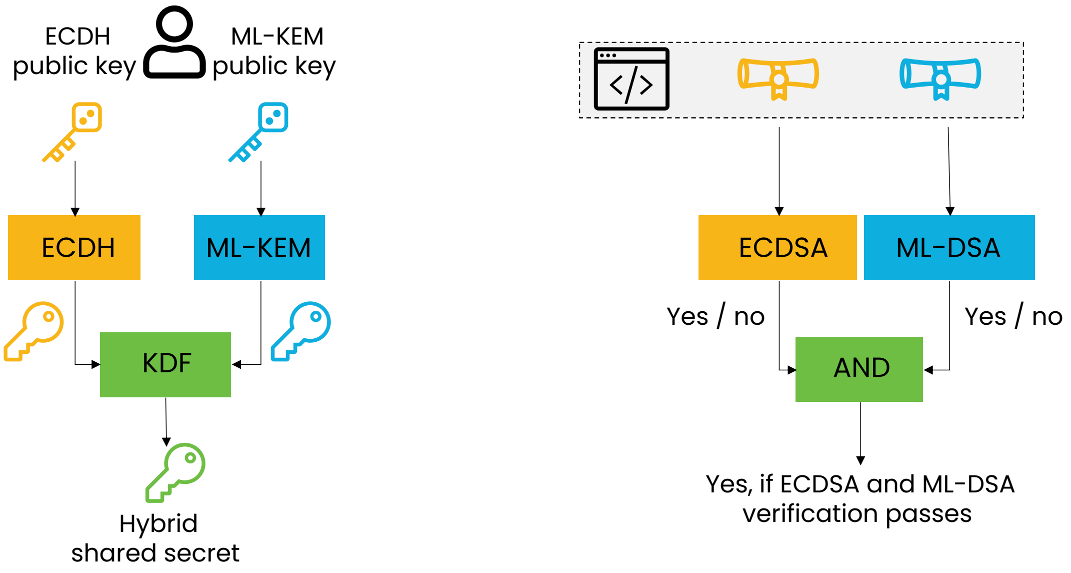
In practice, Hybrid PQC would be realized as follows:

- Combining ML-KEM (or another PQC KEM) with a traditional scheme for key exchange, such as Elliptic-curve Diffie-Hellman (ECDH) is achieved by combining the shared secrets derived from the ML-KEM exchange and the ECDH exchange using a key derivation function (KDF). This results in a shared secret which combines the security of both schemes.
- Combining ML-DSA (or another PQC signature scheme) with a traditional signature scheme, such as Elliptic Curve Digital Signature (ECDSA) or RSA signature, is simpler than combining ML-KEM with a traditional key-exchange system. All that's needed is to sign the message with both schemes and transmit both signatures to the verifier. The crucial step is for the verifier to verify both signatures and only accept the message if both signatures are valid.

Interoperability

While migration to PQC is required for many devices and use cases, maintaining security and performance is also necessary. However, one important aspect of migration is maintaining interoperability. Interoperability helps our digital world function and makes it possible for many devices and applications to communicate and share information seamlessly. Interoperability is currently supported by many cryptographic schemes, communication protocols and digital certificates. A main example is the work done in the IETF, which includes internet drafts of algorithm identifiers for ML-KEM[32] and ML-DSA[33] and a proposal for hybrid key exchange in TLS 1.3[34].

Hybrid post-quantum cryptography



Migration to Post-Quantum Cryptography Consortium

NXP is a member of the Migration to Post-Quantum Cryptography Project Consortium established by the NIST National Cybersecurity Center of Excellence (NCCoE). The Consortium aims to bring awareness to the issues involved in migrating to post-quantum algorithms and to develop best practices for vendors and integrators, with a focus on cryptographic discovery, interoperability and cryptographic agility[34].

Cryptographic Agility

Cryptographic agility refers to all mechanisms or implementation techniques that provide a simple way to easily, reliably and securely update the cryptographic security of a system. Ideally, this is done without the user even noticing such a change or upgrade has taken place. Updates can help mitigate any future attacks on both traditional and PQC schemes. Cryptographic agility goes beyond migrating from one scheme to another. It also involves flexibility, in terms of parameter sets, and can even go as far as updating implementations or countermeasures against side-channel or fault injection attacks.

While cryptographic agility sounds like a must, it remains expensive to realize in practice, particularly for resource-constrained devices. In addition, adding a level of flexibility and allowing for more frequent and possibly radical updates to a system or device can introduce vulnerabilities. It is imperative that any update is prompted by a trusted source and does not allow for a security downgrade. This process can be protected by a hardware root of trust.

Conclusions and Outlook

While the migration to post-quantum cryptography presents significant challenges for resource-constrained embedded devices, it is imperative that we take proactive measures to ensure the security and resilience of our digital infrastructure. NXP ensures that cryptographic agility is considered from the beginning, at the design stage. This is a crucial step in overcoming the challenges of post-quantum cryptography in the embedded space and helps usher in a new era of quantum-safe cryptographic solutions. By addressing issues such as hardware constraints, side-channel protection and updatability, NXP leads the way for an efficient and secure digital future for embedded devices in the post-quantum era.

References

[1] NIST; FIPS 197, Advanced Encryption Standard (AES) https://csrc.nist.gov/pubs/fips/197/final

[2] NIST; FIPS 186-5 Digital Signature Standard (DSS) https://csrc.nist.gov/pubs/fips/186-5/final

[3] Chuang, Gershenfeld, Kubinec; Experimental Implementation of Fast Quantum Searching. In: Phys. Rev. Lett. 80, 3408, 1998 https://doi.org/10.1103%2FPhysRevLett.80.3408

[4] https://www.ibm.com/quantum/blog/quantum-roadmap-2033

[5] https://www.ibm.com/roadmaps/quantum/2029/

[6] BSI; BT-Drucksache 19/26340 https://dserver.bundestag.de/btd/19/263/1926340.pdf

[7] Shor; Algorithms for quantum computation: discrete logarithms and factoring. In: FOCS 1994 https://doi.org/10.1137%2FS0097539795293172

[8] Grover; A fast quantum mechanical algorithm for database search. In: STOC 1996 https://doi.org/10.1145%2F237814.237866

[9] Position Paper on Quantum Key Distribution by French Cybersecurity Agency (ANSSI), German Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces. Jan. 2024 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

[10] NIST; FIPS-203, Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/ipd

[11] NIST; FIPS-204, Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/ipd

[12] NIST; FIPS-205, Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/ipd

[13] https://www.kpqc.or.kr/

[14] https://csrc.nist.gov/Projects/pqc-dig-sig/standardization

[15] NIST; SP800-208, Recommendation for Stateful Hash-Based Signature Schemes https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

[16] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[17] NSA; CNSA 2.0 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[18] Bos, Renes, van Vredendaal; Post-Quantum Cryptography with Contemporary: Co-Processors Beyond Kronecker, Schönhage-Strassen & Nussbaumer. In: USENIX 2022 https://www.usenix.org/conference/usenixsecurity22/presentation/bos

[19] Fujii, Aranha; Curve25519 for the Cortex-M4 and beyond. In: LatinCrypt 2017 https://doi.org/10.1007/978-3-030-25283-0_6

[20] Abdulrahman, Hwang, Kannwischer, Sprenkels; Faster Kyber and Dilithium on the Cortex-M4. In: ACNS 2022 https://doi.org/10.1007/978-3-031-09234-3_42

[21] Bos, Renes, Sprenkels; Dilithium for Memory Constrained Devices. In: AFRICACRYPT 2022 https://doi.org/10.1007/978-3-031-17433-9_10

[22] Bos, Bronchain, Custers, Renes, Verbakel, van Vredendaal; Enabling FrodoKEM on embedded devices. In: CHES 2023 https://doi.org/10.46586/tches.v2023.i3.74-96

[23] Bos, Carlson, Renes, Rotaru, Sprenkels, Waters; Post-Quantum Secure Boot on Vehicle Network Processors. In: escar 2022 https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/year/2022/docId/9372

[24] Kocher; Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: CRYPTO 1996 https://doi.org/10.1007/3-540-68697-5_9

[25] Bos, Gourjon, Renes, Schneider, van Vredendaal; Masking Kyber: First- and Higher-Order Implementations. In: TCHES 2021 https://doi.org/10.46586/tches.v2021.i4.173-214

[26] Azouaoui, Bronchain, Cassiers, Hoffmann, Kuzovkova, Renes, Schneider, Schönauer, Standaert, van Vredendaal; Protecting Dilithium against Leakage: Revisited Sensitivity Analysis and Improved Implementations. In: TCHES 2023 https://doi.org/10.46586/tches.v2023.i4.58-79

[27] ElGhamrawy, Azouaoui, Bronchain, Renes, Schneider, Schönauer, Seker, van Vredendaal; From MLWE to RLWE: A Differential Fault Attack on Randomized & Deterministic Dilithium. In: TCHES 2023 https://doi.org/10.46586/tches.v2023.i4.262-286

[28] Bronchain, Azouaoui, ElGhamrawy, Renes, Schneider; Exploiting Small-Norm Polynomial Multiplication with Physical Attacks Application to CRYSTALS-Dilithium. In: TCHES 2024 https://doi.org/10.46586/tches.v2024.i2.359-383

[29] NSA; Symmetric Key Management Requirements Annex v2.1 https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/Symmetric%20Key%20Management%20Requirements%20v2_1.pdf

[30] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626

[31] https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition

[32] https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/

[33] https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/

[34] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[35] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

How to reach us

Website:
www.nxp.com/pqc

Whitepaper:
The Emergence of Post-Quantum Cryptography

Blogs:

A Brief Outlook on the Migration to Post-Quantum Cryptography

Conservative Post-Quantum Security with FrodoKEM

Protecting Post-Quantum Cryptography Against Side-Channel Attacks

Standardization of Post-Quantum Cryptography

NXP Stands at the Forefront of Post-Quantum Cryptography

Post-Quantum Cryptography: Physical Attacks and Countermeasures

Prepare for the Quantum Breakthrough with Post-Quantum Cryptography

The Emergence of Post-Quantum Cryptography

Joppe Bos

Joppe W. Bos is a Technical Director and cryptographer at the Competence Center Crypto & Security (CCC&S) in the CTO organization at NXP Semiconductors. Based in Belgium, he is the technical lead of the Post-Quantum Cryptography team, and has authored over 20 patents and 50 academic papers. He is the co-editor of the IACR Cryptology ePrint Archive.

Christine Cloostermans

Christine Cloostermans is a principal cryptographer at the Competence Center for Cryptography and Security (CCC&S) in the CTO organization at NXP Semiconductors. She acquired her doctorate from TU Eindhoven on topics related to lattice-based cryptography. Christine is a co-author on 10+ scientific publications, and has given many public presentations in the area of post-quantum cryptography. Beyond PQC, she is active in multiple standardization efforts, including IEC 62443 for the Industrial domain, ISO 18013 for the mobile driver's license, and the Access Control Working Group of the Connectivity Standards Alliance.

Melissa Azouaoui

Melissa Azouaoui is a senior cryptographer at the Competence Center for Cryptography and Security (CCC&S) in the CTO organization at NXP Semiconductors. She completed her PhD in 2021 at UCLouvain in Belgium, and NXP in Germany with a focus on side-channel countermeasures and evaluations for symmetric and asymmetric cryptography. Melissa is a member of the Post-Quantum Cryptography team and her work at NXP includes side-channel and fault injection attacks and countermeasures, with a particular focus on lattice and hash-based cryptography.

Gareth Thomas Davies

Gareth T. Davies is a senior cryptographer at the Competence Center for Cryptography and Security (CCC&S) in the CTO organization at NXP Semiconductors. Gareth is a member of the Post-Quantum Cryptography team and works on various topics including protocol analysis, authentication schemes and standardization.

Visit nxp.com/pqc