WHITEPAPER

Security in the era of quantum computing

Relevant standards and local transition guidelines for Secure Elements

www.infineon.com

Table of contents

1 Executive summary

Rapid advancements in quantum computing present both opportunities and significant threats to existing cryptographic systems. While quantum technology offers transformative prospects in areas such as the simulation of financial services, chemical science, and artificial intelligence, it also endangers the security of traditional cryptographic algorithms. This applies in particular to algorithms using asymmetric methods that rely on the hardness of prime factorization and the discrete logarithm, such as systems based on RSA and elliptic curve cryptography (ECC).

Post-quantum cryptography (PQC) has emerged as a potential solution to this threat, focusing on the development of cryptographic algorithms that remain secured even in the presence of powerful quantum computers or cryptographically relevant quantum computers (CRQC). Secure Elements, such as hardware security modules and trusted platform modules, play an important role in the deployment of PQC due to their ability to deliver reliable and tamper-resistant environments for executing cryptographic functions. The integration of quantum-safe algorithms into Secure Elements gives critical applications, such as identification, authentication, secured communication, and digital signatures, the ability to remain robust against attacks using quantum computers.

As the transition to PQC and quantum-safe infrastructure accelerates, organizations must prioritize support for new cryptographic standards. This entails updating Secure Element hardware, software, and security infrastructures to facilitate a seamless evolution toward quantum resilience.

This article highlights not only the necessity of PQC in the quantum era but also the critical role of Secure Elements in defending digital ecosystems against emerging computational threats.

2 Basics of quantum computers

2.1 The difference between conventional and quantum computers

Conventional computers process information using bits that can exist only in one of two states at any given moment – 1 or 0. While the transistors that drive conventional computers do rely on quantum effects at microscopic level, the overall computation process adheres strictly to conventional mechanisms.

Quantum computers, however, function in a fundamentally different way. Through the principle of superposition, quantum bits (qubits) can exist in a combination of states, representing both 0 and 1 simultaneously (see Figure 1). This unique property is not limited to individual qubits – the entire quantum processor operates with this capability, enabling new computational paradigms. As a result, quantum computers can, in certain cases, provide tremendous computational speedups.

Quantum computers can process vast amounts of information at once, potentially far surpassing what conventional computers can achieve [8] .

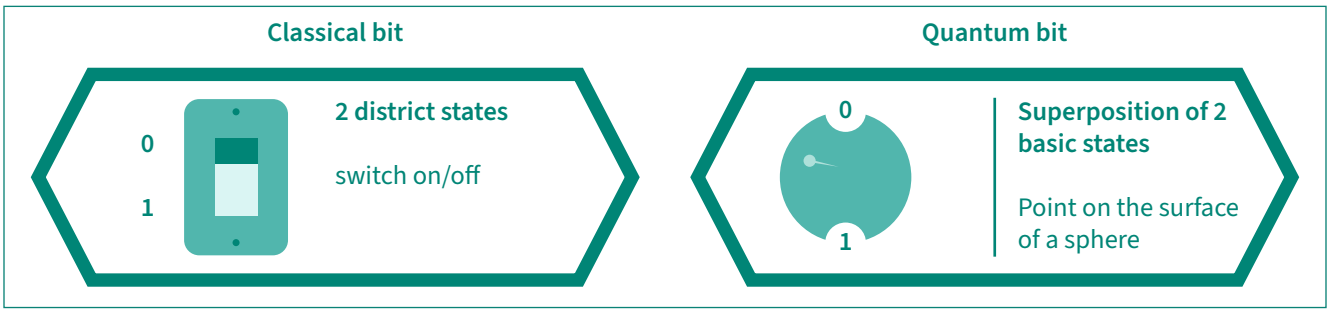

Figure 1 Conventional bit versus quantum bit

While conventional systems continue to improve and are highly effective at solving many computational problems, specific challenges lie beyond their reach. Quantum computers can tackle some of these problems much more efficiently, opening the door to solutions that conventional computers may never achieve.

However, quantum computers will not replace conventional computers. Instead, they will most likely run in parallel. Quantum computers will manage specific, highly complex tasks, while traditional computers handle general processing and user-interface operations. As quantum computers become more powerful, they will be able to host an increasing number of tasks.

The potential of current quantum processors is severely limited by noise and error rates. Present-day quantum computers are considered “noisy intermediate-scale quantum” (NISQ) devices, which means their performance is limited by environmental interference and imperfect qubit control. Even the tiniest disturbances, such as interactions with stray particles of light or changes in temperature, can cause computational errors. To overcome these obstacles, quantum computers require robust error correction mechanisms capable of protecting qubits from external disturbances. The development of effective error-correcting methods is essential for achieving usable “logical qubits” that are reliable enough for practical applications [10].

In summary, while conventional and quantum computers are rooted in fundamentally different principles, they are complementary in their purpose. Conventional computers excel at a wide range of tasks, while quantum computers, though still in development, promise to revolutionize certain fields by solving problems once thought impossible.

2.1.1 Simulating a quantum computer with a conventional computer

What would it mean if a conventional computer had to simulate a quantum computer? This is demonstrated in Table 1 and Figure 2.

Table 1 Conventional computer power versus quantum computer power [23]

Memory of quantum computers in qubits	Memory of conventional computers	Computing time on device
10	16 KB	Microseconds on watch
20	16 MB	Milliseconds on smartphone
30	16 GB	Seconds on laptop
40	16 TB	Seconds on supercomputer
50	16 PB	Seconds on top supercomputer
60	16 EB	Minutes on future supercomputer
70	16 ZB	Hours on potential supercomputer?
…	…	…
250	More bytes than atoms in the universe	Longer than the age of the universe

16 PB

50 qubits [11]

Figure 2 Comparison of top supercomputer with quantum computer

2.2 Outlook and challenges for quantum computers

The key challenge with quantum computing lies in detecting and correcting errors. The two key performance indicators involved in this are the number of qubits and the error rate.

The current generation of quantum computers is described as NISQ devices. The size of logical qubits (or even physical qubits) is limited in these NISQ devices. The next challenge is qubit fidelity. Two-qubit fidelity is a crucial metric in quantum computing. It refers to the accuracy or performance of quantum gates – a fundamental building block in quantum circuits – involving two qubits. In essence, this metric quantifies how closely the operation performed by a two-qubit gate matches the ideal, theoretical gate operation. High fidelity is a key requirement for building practical quantum computers because errors in quantum operations degrade the quality of quantum computations.

It is anticipated that quantum computing will continue to advance rapidly over the coming years with the development of new quantum devices featuring an increasing number of logical qubits. However, the limitations of today's NISQ devices – particularly their susceptibility to noise and errors – means that they are unlikely to solve large-scale, real-world problems effectively in their current form. As a result, the long-term future of quantum computing will likely depend on the creation of error-corrected qubits. These advanced systems will have the ability to tackle significantly larger and more complex problems than today's devices.

Quantum usefulness begins to emerge once a critical threshold of qubits has been achieved, enabling quantum computers to solve certain problems more efficiently than conventional systems. Figure 3 shows the number of two-qubit gates over the error rate. It demonstrates the relationship between the number of qubits, error correction, and the respective capabilities of conventional and quantum computers. This illustration highlights the transition point where quantum technology surpasses conventional computing in specific applications, paving the way for practical and impactful quantum advantage.

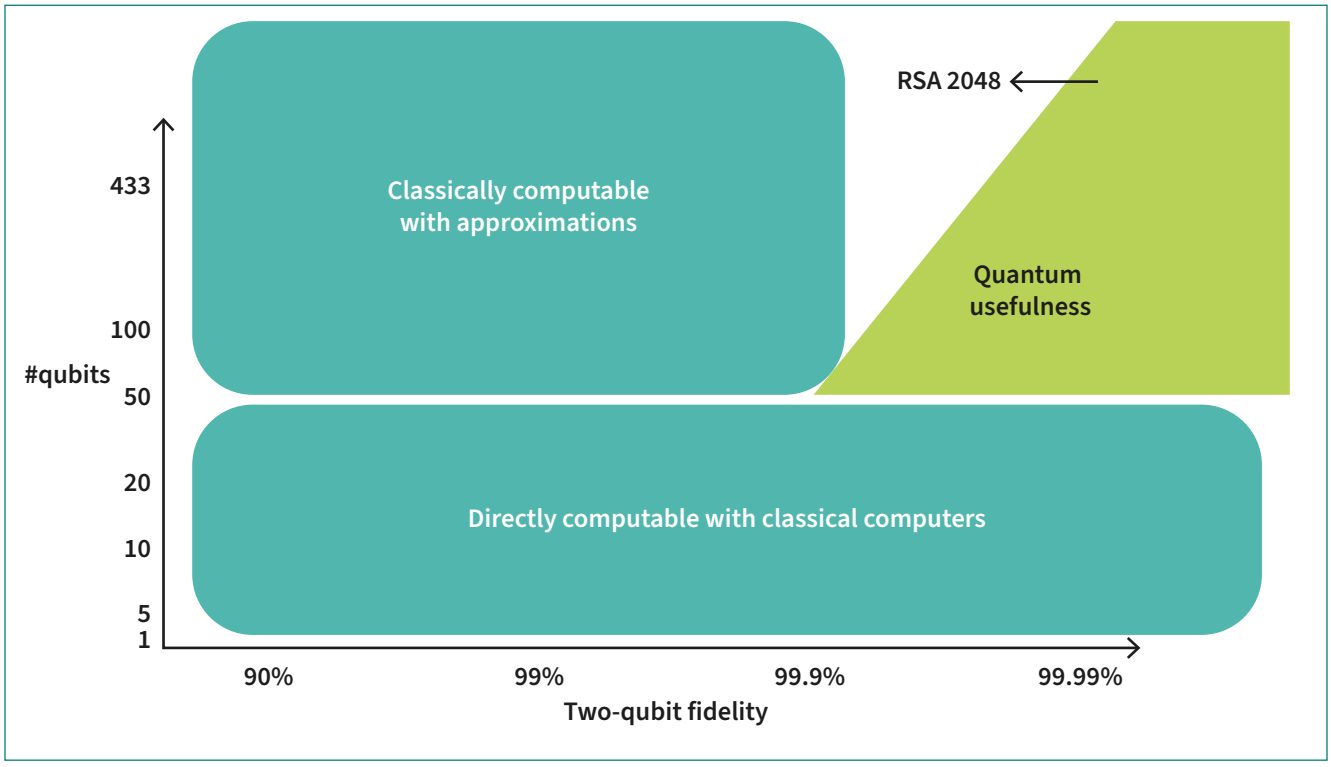

Figure 3 Illustration of quantum usefulness (Infineon, 2025)

As shown in Figure 3, breaking the RSA encryption algorithm with a 2048-bit key would require more than 4,000 logical qubits. Infineon's experts predict that such a feat will become feasible by approximately 2035 or even before, as ongoing advancements in quantum error correction and the scaling up of logical qubits continue to push the boundaries of what quantum computers can achieve.

Building on its expertise in chip design, materials technology, and semiconductor fabrication, Infineon is taking quantum computing beyond basic research so it can be scaled and commercialized to support concrete applications running on quantum computers. Infineon has state-of-the-art know-how in process development, fabrication, and quantum processing unit (QPU) technology. This includes laboratories for quantum electronics as well as dedicated quantum labs next to chip production.

In the quantum space, Infineon embraces a multi-level approach that includes silicon-based qubits and ion-trap technology. Each of these approaches offers different advantages and challenges. In ion-trap technology, a previous landmark record with two-qubit gate fidelity of 99.99 % was achieved in 2025 [22].

3 Opportunities and threats presented by quantum computers

3.1 Opportunities presented by quantum computers

Quantum computing is poised to revolutionize several industries, offering transformative use cases that could redefine how problems are solved. Four key applications have been highlighted as particularly game-changing [9].

Optimization of financial services

One of the most promising applications lies in financial services. A collaboration between IBM, Quantinuum, Banca D'Italia, and multiple universities successfully used quantum computing to address highly complex optimization tasks. By minimizing delays in processes like setting payments on the TARGET2-Securities[1] platform, this technology could save financial institutions millions of dollars. Quantum computers excel at solving such problems by identifying optimal combinations across a vast number of interconnected variables.

Drug discovery

Quantum computers are particularly well-suited to drug discovery because of their ability to simulate molecules which closely reflect the real world governed by the laws of quantum physics. They can accurately model and predict interactions between medical particles and biological targets, aiding in the development of new treatments. Currently, 70 % of these interactions are too complex for conventional computers to simulate, but quantum technology has the potential to bridge this gap, drastically accelerating breakthroughs in medicine.

Battery innovations

Better batteries could also become a reality with the help of quantum computers. By enabling researchers to model and simulate complex battery chemistries more precisely, quantum computers will pave the way for the design of batteries with longer lifespans, faster charging capabilities, and enhanced energy efficiency. This could have far-reaching impacts on industries like renewable energy and electric vehicles.

Materials discovery [12]

Quantum technology is transforming materials science by allowing researchers to simulate, design, and analyze new materials at the atomic level. This speeds up the development of stronger, lighter, and more efficient materials for industries ranging from aerospace and energy to consumer electronics and healthcare.

Looking ahead, Google predicts that commercial quantum computing will be available to a broad range of businesses and organizations within the next five years. This accessibility will likely drive further innovations across industries, accelerating the real-world adoption and impact of quantum technologies [10].

As a semiconductor leader, Infineon is in a unique position to leverage the potential performance gains of quantum computing while protecting against the associated threats. Powering the pioneers, Infineon is a trusted partner for powerful quantum processing units as well as for PQC solutions.

1 TARGET2-Securities (T2S) is a European post-trade platform for the simultaneous settlement of securities and cash transactions using central bank money. T2S is a common platform on which securities and cash can be transferred between investors across Europe, using harmonized rules and practices. Currently 23 European countries use T2S [7].

3.2 Threats posed by quantum computers

One of the biggest threats posed by quantum computers relates to cryptography. NIST describes this threat as follow:

"If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secured against both quantum and classical computers, and can interoperate with existing communications protocols and networks [19]."

To address this critical issue, PQC has emerged as a vital area of research. The objective is to create cryptographic systems that are resilient to both quantum and conventional computing attacks while maintaining compatibility with existing communication protocols and networks. By preparing these robust systems, industry can safeguard more effectively against the cryptographic vulnerabilities posed by advancements in quantum computing.

The timeline for the arrival of large-scale quantum computers (also called cryptographic-relevant quantum computers) remains uncertain. While earlier doubts focused on their physical feasibility, today many scientists agree that they represent a significant, yet ultimately solvable, engineering challenge. Some experts predict that such computers could be operational within the next two decades, with the power to break nearly all existing public-key cryptosystems. This projection is particularly alarming because the current public key cryptography infrastructure took almost two decades to deploy.

Given this historical precedent, we cannot afford to wait until the first large-scale quantum computer is brought to market. Regardless of the exact timeline, the urgency of the situation demands immediate action. We must start transitioning our information security frameworks now to prepare for the era of quantum computing, and make them robust enough to withstand the potential risks posed by this transformative technology. Such proactive preparation is essential to maintaining the security of digital communication and data integrity in a post-quantum world.

BSI, the German Federal Office of Information Security, has stipulated that crypto migration for high-risk use cases involving sensitive data (harvest now, decrypt later[2]) must be finalized by the end of 2030 at the latest [3].

4 Post-quantum cryptography (PQC)

As outlined in Chapter 3.2, one of the most critical threats posed by quantum computers is their potential to compromise cryptographic algorithms.

Quantum computing's impact on cryptographic algorithms is most relevant in the context of Shor's algorithm, which can factor large integers and compute discrete logarithms in polynomial time. This would break widely used asymmetric cryptographic schemes such as RSA and ECC. However, AES is a symmetric-key algorithm, and quantum computing does not have a direct equivalent to Shor's algorithm for symmetric-key encryption.

For symmetric schemes like AES, quantum computing poses a different challenge: Grover's algorithm. Grover's algorithm allows for a quadratic speedup in searching unsorted databases, and when applied to AES, could reduce the effective security of the algorithm.

As an example, quantum computers might break AES-128 (AES with 128-bit keys) in $\sqrt{2128} = 264$ Grover steps, with each Grover step containing a (quantum) evaluation of the AES. Some years ago, the general view was that this means that symmetric key sizes need to be doubled – calling for AES-256 instead of AES-128.

However, today this is considered a misconception. For instance, NIST now states that AES-128 will likely remain secured for decades to come, despite Grover's algorithm. In fact, the NIST PQC security levels are defined based on AES, including AES-128 (see Table 2).

2 "Harvest now, decrypt later" refers to a process where highly sensitive encrypted data could be copied by hackers now and decrypted once quantum computers have sufficient performance.

4.1 What is post-quantum cryptography?

Post-quantum cryptography, also referred to as quantum-safe cryptography, involves the design and implementation of algorithms and protocols that are considered secured against the enhanced computational power of quantum computers.

4.2 Post-quantum algorithms

Several PQC algorithm standards have been developed in different countries. This document does not list all these standards, but only the most important ones that are defined by international standardization organizations.

4.2.1 National Institute of Standards and Technology (NIST)

The cryptography standards established by NIST offer detailed guidance on a wide range of cryptographic techniques vital for protecting sensitive data across federal and nonfederal systems. These standards encompass core topics critical to maintaining data confidentiality, integrity, and authenticity, including encryption methods, digital signatures, hashing algorithms, key establishment protocols, and random number generation. Furthermore, NIST provides specifications for effective key management, outlining best practices for the secured generation, storage, distribution, and eventually destruction of cryptographic keys [20].

Over the past eight years, NIST has been hosting a competition with worldwide crypto experts to identify and standardize new PQC schemes, similar to the earlier AES and SHA3 competition. Researchers were invited to submit their proposals for key encapsulation mechanisms (KEMs) and digital signature algorithms (DSAs), which underwent rigorous public evaluation across multiple rounds. After each round, the candidate pool was gradually narrowed down to focus on the most promising algorithms.

By 2022, on conclusion of the third round, four cryptographic schemes had been selected for standardization. Subsequently, an additional scheme was chosen in 2025. While the first standards have already been released, the standardization process for the remaining selected algorithms was still ongoing at the time of publication (2026).

Recognizing the need to further diversify its selection of signature schemes, NIST aimed to reach beyond its earlier approaches by incorporating advancements made after the original 2017 submission deadline. Specifically, NIST sought alternatives to structured lattice-based algorithms, as two such schemes had already been standardized. At the time of publication, this “signature on-ramp” initiative had progressed to its second round of evaluations, where 14 candidates remained under scrutiny. These efforts reflect NIST’s commitment to building a robust and forward-looking cryptographic ecosystem to address the challenges of the quantum era.

To date, NIST has successfully standardized the majority of PQC algorithms. In their 2024 guideline draft [21], NIST defines five distinct security categories for PQC algorithms to represent varying levels of security strength (or protection), which are based on the key sizes used in symmetric encryption schemes. These same security benchmarks, derived from the strength of AES, are also applied to assess the security of asymmetric PQC algorithms (see Table 2).

Table 2 Summary of security categories as defined by NIST

Security category	Attack type	Example
I	**Key search on a block cipher with a 128-bit key**	**AES-128**
II	Collision search on a 256-bit hash function	SHA-256
III	**Key search on a block cipher with a 192-bit key**	**AES-192**
IV	Collision search on a 384-bit hash function	SHA3-384
V	**Key search on a block cipher with a 256-bit key**	**AES-256**

Table 3 NIST Schemes with different Security Categories

NIST scheme	Parameter sets (security category)	Type of algorithm	Suitable for use with Secure Elements[3]
Key encapsulation			
ML-KEM (Kyber) FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard https://doi.org/10.6028/NIST.FIPS.203	ML-KEM-512 (I) ML-KEM-768 (III) ML-KEM-1024 (V)	Key encap-sulation	**Yes**
HQC FIPS xxx: (upcoming)	HQC-128 (I) HQC-192 (III) HQC-256 (V)	Key encap-sulation	No
Signatures			
ML-DSA (Dilithium) FIPS 204: Module-Lattice-Based Digital Signature Standard https://doi.org/10.6028/NIST.FIPS.204	ML-DSA-44 (I) ML-DSA-65 (III) ML-DSA-87 (V)	Signature	**Yes**
SLH-DSA (SPHINCS+) FIPS 205: Stateless Hash-Based Digital Signature Standard https://doi.org/10.6028/NIST.FIPS.205	SPHINCS-128 (I) SPHINCS-192 (III) SPHINCS-256 (V)	Signature	No
FN-DSA (Falcon) FIPS 206: (upcoming)	Falcon-512 (I) Falcon-1024 (V)	Signature	Not ideal due to low signature performance but small signature size
XMSS / LMS FIPS SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes https://doi.org/10.6028/NIST.SP.800-208		Signature	**Yes**, for verification

3 Refer to chapter 7 showing the challenges associated with the implementation of PQC in restricted devices.

4.2.2 ISO/IEC

Table 4 ISO-defined PQC algorithms

ISO/IEC scheme	Parameter sets (security category)	Type of algorithm	Suitable for use with Secure Elements
Classic McEliece ISO (upcoming)	Culparcimus	Key encapsulation	No
FrodoKEM ISO (upcoming)	FrodoKEM-640 (I) FrodoKEM-976 (III) FrodoKEM-1344 (V)	Key encapsulation	No

Additionally, NIST defined algorithms such as ML-KEM, ML-DSA, and SLH-DSA, which were discussed in the previous chapter, are will be included in the ISO/IEC standards.

5 The optimal algorithms for Secure Elements

Secure Elements have limited resources in terms of memory, communication bandwidth, and CPU performance. At the same time, they need to fulfill strong security requirements like side-channel resistance against security attacks.

Due to these constraints, not all PQC algorithms are suitable for implementation in Secure Element environments. Some algorithms are challenging to deploy because of their large key sizes (e.g. the ML-KEM key size is larger than the ECC key size by a factor of up to 50), while others require excessive computation time, making them inefficient for resource-constrained platforms. Please refer to Table 3 and Table 4 above for the different PQC algorithms.

5.1 Key encapsulation mechanisms (KEMs)

5.1.1 ML-KEM

The performance[4] of ML-KEM (module-lattice-based key-encapsulation mechanism) [18] is comparable to that of conventional ECC [13]. However, the key size of ML-KEM is significantly larger – up to 50 times greater than that of ECC. This makes ML-KEM less efficient in scenarios where storage and communication bandwidth are limited. However, ML-KEM is the optimum quantum-safe KEM algorithm for restricted devices like Secure Elements.

5.1.2 HQC

HQC (hamming quasi-cyclic) has a key size that is approximately 2 times larger than that of ML-KEM or about 100 times larger than that of ECC, which makes it impractical for use in Secure Elements. Furthermore, HQC's performance is up to 400 times slower than ML-KEM (see Annex I – Comparison of key sizes and performance of different PQC algorithms for more information). This substantial difference in both key size and computation time means HQC is not a viable option for Secure Elements.

5.1.3 Classic McEliece

Classic McEliece has a small ciphertext but a large public key of more than 250 KB, which is not suitable for use with Secure Elements.

5.1.4 FrodoKEM

Frodo has large ciphertexts and keys (bigger than ML-KEM by a factor of at least 10), which is not suitable for use with Secure Elements.

5.2 Digital signature algorithms (DSAs)

5.2.1 ML-DSA

The performance of the conventional ECDSA (elliptic curve digital signature algorithm) is significantly better than that of the ML-DSA (module-LWE-based digital signature algorithm). Specifically, ECDSA computes approximately 16 times faster than ML-DSA. ML-DSA signature generation time is not deterministic and therefore varies.

4 Performance values are based on implementations without protection against security breaches.

5.2.2 FN-DSA

The FN-DSA (falcon-based digital signature algorithm) has a distinct advantage over ML-DSA with its much smaller signature sizes. This could make it appealing for space-constrained applications. However, its signing performance is slower than ML-DSA by a factor of between 6 and 8. It is very complex to secure this algorithm against side-channel attacks. A standard for this algorithm has not yet been released.

5.2.3 SLH-DSA

SLH-DSA (SPHINCS+ digital signature algorithm) has substantial downsides in terms of both signature size and computational speed. Its signature size is larger than ML-DSA by a factor of up to 6, while its signing performance can be up to 10 times slower.

For further information about key sizes and performance, refer to Annex I – Comparison of key sizes and performance of different PQC algorithms.

5.2.4 XMSS and LMS

XMSS (extended Merkle signature scheme) and LMS (Leighton-Micali signature) public keys are notably small, making them advantageous in certain scenarios. However, a significant drawback is that the signature sizes are very large, rendering them less than ideal for use in space-constrained devices. Despite this, the algorithm's small public key size makes it well-suited to signature verification on such devices. On the other hand, generating signatures is not suitable for space-constrained devices due to the large signature size.

The stateful nature of the XMSS and LMS algorithm limits its applicability to specific use cases, such as secure boot and OS update verification, where on-device signing is not required.

Summary

In environments with resource constraints, such as Secure Elements, conventional cryptographic algorithms like ECC and ECDSA maintain significant performance and efficiency advantages over many post-quantum algorithms. Among the PQC candidates, a relatively small signature, small key size, and fast computation time are key success factors for algorithms to be feasible alternatives in embedded systems.

At the moment, the most efficient algorithms for Secure Elements are ML-KEM for key encapsulation and ML-DSA for signature[5]. For verification operations, XMSS / LMS and FN-DSA are also suitable for restricted devices.

5.2.5 Hybrid cryptography

Hybrid systems that combine conventional cryptography with PQC can provide an intermediate solution pending full maturity of quantum computing.

5 In addition, most applications require hybrid cryptography (see also chapter 7.4) that combines conventional cryptography (RSA or ECC) with PQC as an intermediate solution.

6 Recommendations for migration from national bodies and authorities

6.1 USA

6.1.1 NSA

The US National Security Agency (NSA) describes the requirements for National Security Systems (NSS) [21].

Timeline

The transition timeline is defined as follows:

- CNSSP 15 (Committee on National Security Systems Policy 15) states that by 1 January 2027, all new acquisitions for NSS will be required to be compliant with CNSA 2.0 (Commercial National Security Algorithm Suite 2.0) unless otherwise noted.
- By 31 December 2030, all equipment and services that cannot support CNSA 2.0 must be phased out unless otherwise noted.
- By 31 December 2031, CNSA 2.0 algorithms are mandatory unless otherwise noted.

CNSSP 15 specifies commercial cryptographic algorithms for protecting NSS, in conjunction with other CNSS- and NSA-documented processes.

Table 5 CSNA timeline for different applications [5]

	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
Software / firmware signing									✓			
Web browsers / servers and cloud services												✓
Traditional networking equipment									✓			
Operating systems												✓
Niche equipment												✓
Custom application and legacy equipment												✓

- - - CNSA 2.0 added as an option and tested
—— CNSA 2.0 as the default and preferred
✓ Exclusively use CNSA 2.0 by this year

Algorithms

CNSA 2.0 is the suite of quantum-resilient algorithms approved for NSS use.

- KEM: ML-KEM (security category V)
- Signatures: ML-DSA (security category V)
- Hash-based signatures: LMS, XMMS
- Symmetric algorithms: AES 256
- Hash algorithms: SHA-384, SHA-512NIST

Hybrid cryptography (see chapter 7.1) is generally not required.

6.1.2 NIST [17]

Timeline

The terms “acceptable,” “deprecated”, “disallowed,” and “legacy use” are used throughout the NIST document for PQC migration to indicate the approval status of an algorithm [20].

The classification of algorithms and their key lengths or strengths is divided into four categories. “Acceptable” refers to algorithms and key strengths approved for use under relevant guidelines. “Deprecated” indicates that such algorithms may still be used despite presenting some security risks, which must be evaluated by the data owner. “Disallowed” identifies algorithms, key strengths, or schemes that are no longer permitted for their intended purpose. Lastly, “Legacy use” applies to algorithms or schemes that can only be used to process already protected data, such as decrypting ciphertext or verifying digital signatures.

Transition of digital signatures

- Deprecated after 2030: ECDSA 112-bit security strength[6], RSA 112-bit security strength
- Disallowed after 2035: ECDSA 112-bit and ≥ 128-bit security strength, RSA 112-bit and ≥ 128-bit security strength, and ECDSA ≥ 128-bit security strength

ML-DSA

ML-DSA (security category I, III, V)

SLH-DSA

- SLH-DSA (security category I,III, V)

LMS and HSS

- LMS and HSS (security category III and V)

XMSS, XMSSMT (multi-tree XMSS)

- XMSS, XMSSMT(security category III and V)

Transition of key establishment

- Deprecated after 2030
  - Finite field DH (Diffie-Hellman key agreement) and MQV (Menezes-Qu-Vanstone key agreement) (112-bit security strength)
  - Elliptic curve DH and MQV (112-bit security strength)
  - RSA (112-bit security strength)

- Disallowed after 2035
  - Finite field DH and MQV (112-bit and ≥ 128-bit security strength)
  - Elliptic curve DH and MQC (112-bit and ≥ 128-bit security strength)
  - RSA (112-bit and ≥ 128-bit security strength)

KEM

ML-KEM

- ML-KEM (security category I, III, V)

Symmetric cryptography

- AES-128, AES-192, AES-256

6 Historically, the security strength that an algorithm could provide was defined in terms of the amount of work (i.e., the number of operations) required to break the algorithm (i.e. an algorithm has s bits of security strength if breaking the algorithm requires 2s operations of some kind, where s = 112, 128, 192, or 256). However, there are significant uncertainties in estimating the security strengths of post-quantum cryptosystems given the difficulty of accurately predicting the performance characteristics of future quantum computers, such as their cost, speed, and memory size” [20].

Hash functions and XOFs[7]
- SHA-1 (security category I, for non-digital signature applications only)
- SHA-2: SHA-224, SHA-512/224 (security level III), SHA-256, SHA-512/256 (security level V), SHA-384, SHA-512 (security level V)
- SHA-3: SHA-224 (security level III), SHA 256 (security level V), SHAKE-128 (security level II), SHA-384, SHA-512, SHAKE 256 (security level V)

NIST allows each specific application to determine whether it can accommodate the implementation cost, performance overhead, and engineering complexity – such as conducting proper and independent security reviews – associated with employing a hybrid key establishment mode or utilizing dual signatures [20].

6.2 EU, European Commission

The NIS Cooperation Group has provided recommendations to guide EU member states on how to achieve a synchronized transition to PQC. These recommendations outline a structured timeline and critical steps that member states need to implement to be prepared for the quantum era [16].

The document establishes a risk-based classification system to cluster use cases into four defined risk levels. Level 1 represents "low-risk" scenarios, level 2 encompasses "medium-risk", while levels 3 and 4 are categorized as "high-risk" cases.

Use cases with high-risk classification involve situations where compromises to the confidentiality of data – even 10 years after its capture – could still lead to significant damage, especially if attackers exhibit strong motivation to store and potentially exploit encrypted information over time.

Timeline

As a "first step", all EU member states are advised to initiate their transition strategies by the end of 2026. This initial phase involves several foundational activities, including identifying and involving relevant stakeholders, supporting mature cryptographic asset management practices, and creating dependency maps for applications, products, platforms, and operations. Additionally, the first step entails quantum risk analyses to evaluate potential vulnerabilities and transition preparations by defining an actionable timeline and initiating supporting activities.

A clear timeline for the PQC transition is defined in the NIS Cooperation Group document [16]:
- By 31 December 2026, all EU member states are expected to have completed the initial phase.
- By 31 December 2030, steps to address "high-risk" use cases should have been fully implemented; transition planning and pilot projects for "medium-risk" use cases should be completed.
- The process should be completed by 31 December 2035, by which time the transition for "medium-risk" use cases should be finalized, along with the subsequent completion of PQC transitions for "low-risk" use cases.

By implementing these recommendations on a coordinated timeline, EU member states aim to collectively mitigate the risks posed by quantum computing advancements, enabling a harmonized transition to quantum-safe cryptographic systems and PQC-enabled products.

6.2.1 Algorithms – Germany, Federal Office of Information Security (BSI)

Timeline:

The use of only classical asymmetric algorithms used for key generation, signature and encryption are recommended to be used only until 2031. After 2031 only hybrid implementations are recommended to be used. Signatures based on RSA with a key length of at least 3000 bit are recommended to be used until 2035 [3].

7 An extendable-output function (XOF) is a type of cryptographic hash function that can produce an output of arbitrary length, unlike traditional hash functions which produce a fixed-size output.

BSI defines the following quantum-safe algorithms for use in Germany [3]:
- KEM: FrodoKEM-976 and FrodoKEM-1344, McEliece (460896, 6688128, 8192128, 460896f, 6688128f and 8192128f)
- NIST recently selected HQC (Hamming Quasi-Cyclic) as the fifth algorithm for Post-Quantum Encryption which could be a backup of ML-KEM [4]. BSI intends to include HQC after the publication of the standard with security categories III and V [3].
- Signatures: ML-DSA, SLH-DSA (security category III and V)
- Hash-based signatures: LMS, XMSS
- Symmetric algorithms: AES-128, AES-192, AES-256
- Hash algorithms: SHA-256, SHA-512/256, SHA-384 und SHA-512; SHA3-256, SHA3-384, SHA3-512

Hybrid cryptography is recommended.

6.2.2 Algorithms – France, French Cybersecurity Agency (ANSSI)

ANSSI defines the following quantum-safe algorithms for use in France [2]:
- KEM: FrodoKEM, ML-KEM (security category III and V)
- Signatures: ML-DSA (security category III and V), FN-DSA (not yet published) (security category III and V)
- Hash-based signature: LMS/XMSS, SLH-DSA (security category III and V)
- Symmetric algorithms: AES-256
- Hash algorithms: SHA-384, SHA2-512, SHA3-256, SHA3-384 and SHA3-512

Hybrid cryptography is recommended.

6.3 UK, National Cyber Security Center [15]

NCSC as defined the following timeline and key milestones for the UK [14]:
- Define key milestones by 2028
- Carry out the highest priority PQC migration activities by 2031
- Complete migration to PQC across all systems, services, and products by 2035

NCSC recommends the following crypto algorithms:
- KEM: ML-KEM
- Signature: ML-DSA, SLH-DSA
- Hash-based signatures: LMS, XMMS

Hybrid cryptography is recommended as an interim solution only.

7 Challenges in adopting PQC for Secure Elements and solutions for different applications

This chapter focuses on Secure Elements tailored to high-security applications. These include use cases such as electronic documents, payment systems, embedded Secure Elements, and embedded subscriber identity modules (eSIMs) commonly used in mobile devices.

7.1 Security

The security performance of Secure Elements can be adapted to different application requirements and certified to various schemes such as EMVCo or EUCC (Common Criteria). To achieve a high level of security, robust counter-measures must be implemented to prevent side-channel attacks and fault attacks.

The recently standardized post-quantum algorithms differ fundamentally from traditional cryptography. Thus, the attack landscape needs to be re-evaluated from the ground up. In fact, research has shown that entirely new exploit paths are emerging, while some techniques that threatened traditional cryptography have become less relevant in the post-quantum world. The same applies on the defense side, as new approaches have emerged to provide effective hardening against side-channel attacks. However, these approaches need to be improved and combined to achieve holistic protection that can withstand potential attack advancements over the coming years. Infineon is actively driving PQC and achieved the world's first CC certificate for a PQ-equipped Secure Element in 2024.

7.2 Performance

Increasing cryptographic key lengths and signature sizes has a direct impact on processing and communication times. To address this performance challenge, hardware accelerators with the ability to maintain application performance or at least deliver an acceptable level are becoming essential.

As the certificates are much larger (compared with ECC), a much larger volume of data has to be transferred. This must be factored into design choices when selecting the communication interface. In particular, a higher NFC bit rate (0.85 / 1.7 / 3.4 Mbit/s) must be chosen for contactless devices in order to keep the data transfer time acceptable. For this reason, in PQC applications, Infineon recommends utilizing the very high bit rates (VHBR) of up to 6.8 Mbit/s available with some of its solutions.

7.3 Crypto agility

Transitioning global infrastructures to PQC calls for systems that are cryptographically agile – capable of supporting and seamlessly switching between different algorithms without requiring extensive redesigns. This will allow stakeholders to swiftly adapt to new advancements and unforeseen developments in the field [1].

Achieving true cryptographic agility means that PQC algorithms must be implemented in updateable software running on hardware designed to accommodate most of the PQC algorithms that may emerge in the future. This approach enables scalability and adaptability, laying the foundation for systems to remain secured in an ever-evolving cryptographic landscape.

To achieve crypto agility, governments and enterprises are advised to migrate to Secure Elements – such as those offered by Infineon – that are capable of supporting PQC.

7.4 Memory

PQC algorithms, larger key sizes, hybrid cryptography, and the need for crypto agility significantly increase the data volume and footprint of the operating system. This also impacts the size of RAM and NVM required. In addition, it triggers a disproportionate leap in the resources needed to support the additional cryptographic processes.

8 Migration of applications to PQC

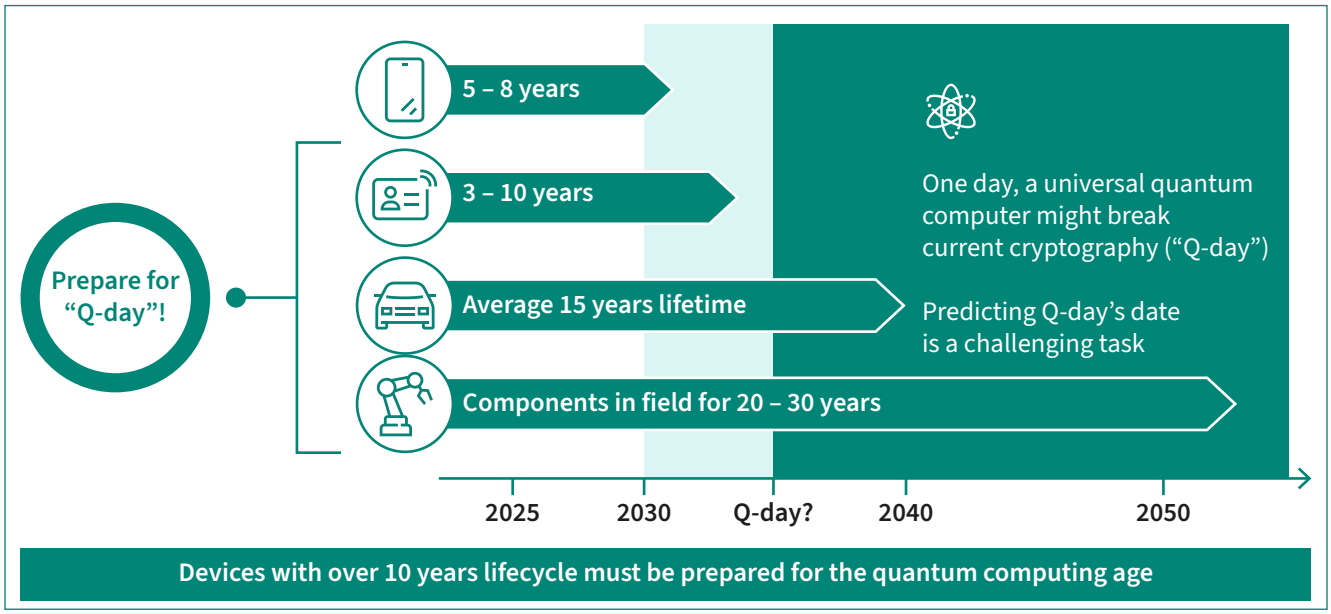

Figure 4 Impact of PQC on different industry sectors

Figure 4 illustrates how the expected lifetimes of different devices vary depending on their specific use cases. For instance, consumer products typically have shorter lifetimes, which translates into a lower urgency for cryptographic migration. In contrast, the need to transition cryptography in applications such as cars or industrial machinery is much more critical due to their longer service lives. Many national regulations stipulate that cars and industrial machinery in particular need to be migrated now.

In the case of smartcard-based applications, there is a clear distinction between different types of cards. Payment cards, for example, generally remain in use for only about 5 years, whereas ID-related documents, such as passports, have a significantly longer field deployment spanning approximately 10 years. Consequently, cards used for ID applications need to migrate now.

Initiating migration now is crucial, as the process of redefining, redeveloping, and recertifying products will be time-consuming.

8.1 Applications for Secure Elements

The standards for PQC algorithms have been established to a large extent. However, the development of standards tailored to specific applications remains ongoing. Currently, there is still uncertainty around the PQC algorithm best suited to each application, and critical details, such as the definition of protocols – whether they should adopt a hybrid approach or not – are yet to be finalized.

Infineon is actively involved in standardization activities for PQC. In Table 6 below, you can see Infineon's perspective on the status and urgency of PQC standardization for applications. This will change over time and represents the current view.

Table 6 Some applications that rely on Secure Elements

Application	Perceived urgency of migration	Standards	Status of PQC migration
Automotive security	High	Vehicle to everything (V2X), Car Connectivity Consortium (CCC), vendor proprietary	Complex ecosystem, many players, CCC has low progress
Brand protection	High	Customer specific	Depends on customer requirements
Subscriber identity modules (SIM)	High	Global System for Mobile Communications Association (GSMA), European Telecommunications Standards Institute (ETSI), Global Platform (GP), 3rd Generation Partnership Project (3GPP)	PQC is part of the GSMA standard used for the remote SIM provisioning (RSP) use case
Platform integrity (TPM)	High	Trusted Computing Group (TCG)	Draft standard available
Electronic passports	High	International Civil Aviation Organization (ICAO) (ISO/IEC JTC 1/SC 17/WG 3)	Integrity proof of attributes using PQC – draft standard available
Logical and physical access (PIV)	High	Federal Information Processing Standards (FIPS)	NIST will develop / update application-specific guidance throughout the transition [6]
Medical	Medium	Food and Drug Administration (FDA)	Low demand for PQC at the moment
Logical access (FIDO)	Medium	Fast Identity Online (FIDO®) Alliance	PQC algorithms selected by study group (ML-DSA, ML-KEM) – start of standardization
Payment cards and connected wearables	Low	EMVCo global payment standard	Migration planned by EMVCo approx. in 2038
Physical access	Low	Aliro® standard for physical access	PQC not mentioned in standard up to now
Smart home – Matter standard	Low	Matter v1.5 smart home connectivity standard	New version 1.5 will include PQC with device attestation certificate.

The above table highlights several key Secure Element applications, accompanied by a status indicator reflecting the current estimated progress of standardization activities for PQC migration. A closer look shows that the pace of standardization does not always align with the urgency of the respective applications.

This misalignment is particularly critical in automotive applications, where accelerated standardization efforts are imperative. Automotive products often have prolonged lifecycles and involve a wide array of stakeholders, who must collaborate to effectively harmonize the underlying standards. Without swift progress, this lag poses a challenge to long-term security and interoperability in the field.

9 The role of Infineon Technologies in PQC

Infineon has been at the forefront of advancing PQC for many years, actively contributing to the development and definition of PQC algorithms. With deep expertise in PQC and a strong foothold in this new field, Infineon is committed to delivering products designed to support agile migration strategies for post-quantum readiness.

In 2017, Infineon demonstrated its pioneering spirit by implementing a post-quantum key exchange method based on the “New Hope” algorithm on commercially available contactless smart card chips. This marked a groundbreaking milestone in the practical application of PQC in secured hardware. Building on this foundation, Infineon has participated in numerous funding projects since 2018, leveraging its expertise to drive innovation and publishing several trailblazing research papers set to shape the future of quantum-resistant technologies.

A significant advancement came in 2022, when Infineon introduced a quantum-resistant firmware upgrade path for its OPTIGA™ TPM (Trusted Platform Module), providing a secured approach for post-quantum migration in trusted computing environments. Furthermore, Infineon played an instrumental role in the development of the SPHINCS+ stateless hash-based signature scheme. This signature scheme was recently standardized by NIST as SLH-DSA, making it one of the core schemes selected to counteract the potential threats posed by quantum computing.

Most notably, in December 2024, Infineon achieved another industry-first milestone by obtaining the world’s first Common Criteria certification for PQC (ML-KEM) on a security controller. This historic accomplishment underscores Infineon’s leadership and unwavering commitment to ensuring secured, future-proof solutions in the era of quantum computing.

In 2025, Infineon was awarded Common Criteria certification for a Secure Element for PQC using ML-KEM and ML-DSA.

10 Conclusion

PQC represents a critical focus area in the evolution of secured systems, especially in the era of advancing quantum computing technologies.

As described in this whitepaper, the overarching goal of PQC is to enable robust cryptographic mechanisms that remain resilient even against quantum-based computational attacks. To achieve this aim, the market needs quantum-safe algorithms, which are generally standardized. The PQC migration currently underway has the overarching aim of protecting today's and tomorrow's digital ecosystems. Consequently, organizations must begin proactive preparations now, including the assessment of infrastructures and related security assets (keys, certificates, readers, servers, protocols, etc.). In some cases, this may include the adoption of hybrid cryptography.

For Secure Elements, it is essential that designers carefully balance resource constraints with the implementation of appropriate measures as described in chapter 7. This is the key to achieving optimal performance while maintaining strong protection against PQC attacks by delivering a robust security level.

11 Annex I – Comparison of key sizes and performance of different PQC algorithms

11.1 KEMs needed to establish secured channel

The following table shows key sizes and performance figures of different KEMs needed to establish a secured channel.

Table 7 Algorithms needed to establish secured channels

	Public key size in bytes	Private key size in bytes	Ciphertext in bytes	Encryption performance in MCycles	Decryption performance in MCycles (decapsulation)
ML-KEM 512 (L1[8])	800	1,632	768	0.7	0.9
ML-KEM 768 (L3)	1,184	2,400	1,088	1.1	1.4
ML-KEM 1024 (L5)	1,568	3,168	1,568	1.7	2.0
HQC-128 (L1)	2,249	2,305	4,433	105.6	159.6
HQC-192 (L3)	4,522	4,586	8,978	323.1	486.2
HQC-256 (L5)	7,245	7,317	14,421	591.9	891.2
ECC 256	64	32	64	Refer to Additional information below	
ECC 384	96	48	96		
ECC 521	132	66	132		

Additional information

The performance of the ECC algorithm is comparable to that of ML-KEM. For further information about ECC, refer to Curve25519 for the Cortex-M4 and Beyond.

The ML-KEM private key size is larger than that of ECC by a factor of up to 50.

HQC (refer to HQC for details) is not really viable for embedded controllers as the key size is around 5 times bigger than that of ML-KEM and the performance is up to 400 times slower than ML-KEM.

Performance values are based on implementations without protection against security and therefore are ballpark numbers to give a general idea about the performance differences between different algorithms.

8 L1, L3, and L5 stand for the NIST security categories 1, 3, and 5 respectively.

11.2 Digital signatures

The following table shows key and signature sizes, as well as performance figures for different digital signature schemes.

Table 8 Algorithms needed to establish secured channels

	Public key size in bytes	Private key size in bytes	Signature size in bytes	Signature performance in MCycles	Verify performance in MCycles
ML-DSA-44 (L1)	1,312	2,560	2,420	7.9	2.1
ML-DSA-65 (L3)	1,952	4,032	3,309	12.4	3.4
ML-DSA-87 (L5)	2,592	4,896	4,627	15.6	5.6
FN-DSA-512 (L1)	897	1281	666	49.5	0.7
FN-DSA-1024 (L5)	1,793	2305	1,280	107.5	1.5
SLH-DSA-SHA2-128s/f (L1)	32	64	7 856 17 088	7 657.6 368.6	7.5 21.9
SLH-DSA-SHA2-192s/f (L3)	48	96	16 224 35 664	15 452.1 666.4	13.5 35.5
SLH-DSA-SHA2-256s/f (L5)	64	128	29 792 49 856	14 326.2 1 377.8	19.6 37.3

The performance of ECDSA is about 16 times faster than ML-DSA (refer to Curve25519 for the Cortex-M4 and Beyond).

FN-DSA has a much smaller signature size than ML-DSA and might therefore be of interest for some applications; the performance of the signing is 6-8 times slower than that of ML-DSA.

SLH-DSA has a signature size that is over 6 times bigger than ML-DSA although the performance is slower by a factor of up to 10. Both variants are provided in the table. Note that the performance values apply to SHA2 variants only; SHAKE variants fare much worse in this software benchmark as SHAKE is optimized for hardware implementations.

Source for PQC algorithm performance: pqm4/benchmarks.md

The pqm4 library with its benchmarking and testing framework were instigated under the PQCRYPTO project funded by the European Commission in the H2020 program. It currently contains implementations of post-quantum key-encapsulation mechanisms and post-quantum signature schemes targeting the Arm® Cortex®-M4 family of microcontrollers.

References

[1] AIVD | CWI | TNO. (2024). The PQC Migration Handbook.

[2] ANSSI. (2023, 12 21). Avis de l'ANSSI sur la migration vers la cryptographie post-quantique (suivi 2023). Retrieved from Cyber gouv: https://messervices.cyber.gouv.fr/documents-guides/Avis%20de%20l'ANSSI%20sur%20la%20migration%20vers%20la%20cryptographie.pdf

[3] BSI. (2026, 01 23). bsi.bund. Retrieved from TR02102: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html

[4] NIST. (2025, 03 11). NIST. Retrieved from NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[5] CNSA. (2022). Announcing the Commercial National Security Algorithm Suite 2.0. National Security Agency.

[6] CTG, D. M. (2025, 03). NIST GOV. Retrieved from The Road Ahead: https://csrc.nist.gov/presentations/2025/nist-pqc-the-road-ahead

[7] European Central Bank. (2025, 10 09). What is TARGET2-Securities (T2S)? Retrieved from European Central Bank: https://www.ecb.europa.eu/paym/target/t2s/html/index.en.html

[8] Federal Office for Information Security, Germany. (2024). Status of quantum computer development. Berlin: BSI.

[9] Forbes. (2025, 04 16). 5 Game-Changing Quantum Computing Use Cases You Should Know About. Retrieved from Forbes: https://www.forbes.com/sites/bernardmarr/2025/04/16/5-game-changing-quantum-computing-use-cases-you-should-know-about/

[10] Swayne, M. (2025, 03 26). The Quantum Insider. Retrieved from Google Executive Says Quantum Applications Could Arrive in Five Years: https://thequantuminsider.com/2025/03/26/google-executive-says-quantum-applications-could-arrive-in-five-years/

[11] Google. (2026, 01 22). Quantumai.google. Retrieved from Building scalable quantum systems: https://quantumai.google/quantumcomputer

[12] Infleqtion. (2025). Infleqtion. Retrieved from Quantum for Materials Science: https://infleqtion.com/materials-science/

[13] Kannwischer, M. J. (2026, 01 22). github.com. Retrieved from Speed Evaluation: https://github.com/mupq/pqm4/blob/master/benchmarks.md

[14] National Cyber Security Centre. (2024, 08 14). Next steps in preparing for post-quantum cryptography. Retrieved from gov uk: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

[15] NCSC . (2025). NCSC. Retrieved from NCSC Annual Review 2025: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025

[16] NIS Cooperation Group. (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. NIS Cooperation Group.

[17] NIST - National Institute of Standards and Technology. (2025, 07 25). Post-Quantum Cryptography PQC. Retrieved from Computer Security Resource Center: https://csrc.nist.gov/projects/post-quantum-cryptography

[18] NIST. (2024, 08 13). Module-Lattice-Based Key-Encapsulation Mechanism Standard. Retrieved from NIST: https://csrc.nist.gov/pubs/fips/203/final

[19] NIST. (2025, 02 11). NIST. Retrieved from Post-Quantum Cryptography: https://csrc.nist.rip/Projects/Post-Quantum-Cryptography

[20] NIST, Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). Transition to Post-Quantum Cryptography Standards - NIST IR 8547 Initial Public Draft. NIST. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[21] NSA. (2024). The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ. National Security Agency.

[22] Swayne, M. (2025, 10 21). The Quantum Insider. Retrieved from IonQ Achieves 99.99% Two-Qubit Gate Performance: https://thequantuminsider.com/2025/10/21/ionq-achieves-99-99-two-qubit-gate-performance/

[23] Troyer, M. (2021, 01 21). Simulating Quantum Computers on Classical Computers. Retrieved from youtube: https://www.youtube.com/watch?v=6dTrPQaJLz0

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

© 2026 Infineon Technologies AG.
All rights reserved.

Public

Version: V1.0_EN
Date: 04/2026

Stay connected!

Scan QR code and explore offering
www.infineon.com

Important notice
Products are sold or provided and delivered by Infineon Technologies AG and its affiliates ("Infineon") subject to the terms and conditions of the frame supply contract or other written agreement(s) executed by a customer and Infineon or, in the absence of the foregoing, the applicable Sales Conditions of Infineon. General terms and conditions of a customer or deviations from applicable Sales Conditions of Infineon shall only be binding for Infineon if and to the extent Infineon has given its express written consent.

To the fullest extent permissible pursuant to applicable law, with respect to any information given in this document or in any associated documentation, Infineon disclaims all warranties and liabilities of any kind, whether express or implied, including but not limited to any warranties of merchantability, suitability of the products for the intended application or the specific use, or non-infringement of third-party rights.

Subject to the development and release of the products for series supply by Infineon, the technical specifications of the products are set forth in the relevant final datasheet provided by Infineon and, if any, agreed and signed specifications. Infineon's customers are required to evaluate the suitability of the products for the intended application or specific use.

The information given in this document is subject to change by Infineon at any time without notice.