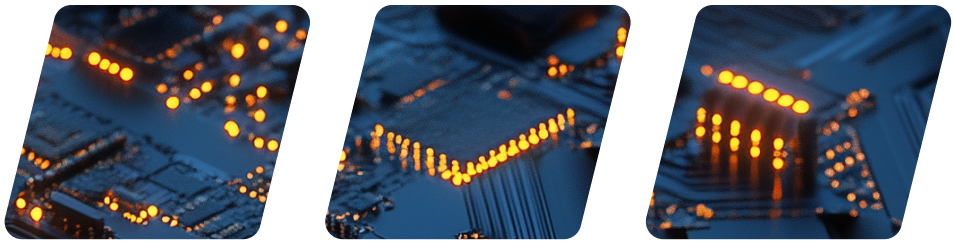
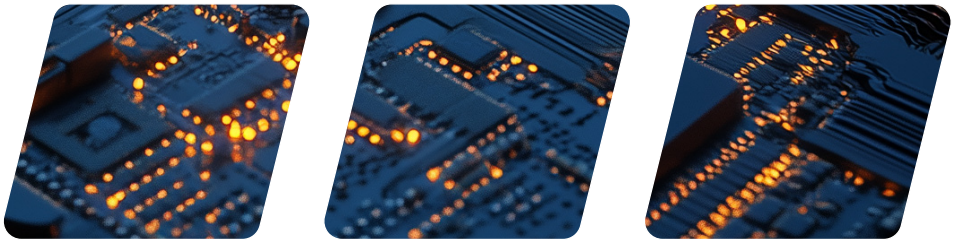


Post-Quantum Cryptography (PQC):

Securing the Future in the Quantum Age



White Paper

Authors:

Mamta Gupta, Sr. Director of Strategic Business Development, Security, Telecommunications, and Datacenters, Lattice Semiconductor

Jordan Anderson, Director of Security Solutions, Lattice Semiconductor

Temoc Chavez Corona, Product Security Architect, Lattice Semiconductor

Mehryar Rahmatian, Product Security Architect, Lattice Semiconductor

DISCLAIMERS

Lattice makes no warranty, representation, or guarantee regarding the accuracy of information contained in this document or the suitability of its products for any particular purpose. All information herein is provided AS IS, with all faults, and all associated risk is the responsibility entirely of the Buyer. The information provided herein is for informational purposes only and may contain technical inaccuracies or omissions, and may be otherwise rendered inaccurate for many reasons, and Lattice assumes no obligation to update or otherwise correct or revise this information. Products sold by Lattice have been subject to limited testing and it is the Buyer's responsibility to independently determine the suitability of any products and to test and verify the same. Lattice products and services are not designed, manufactured, or tested for use in life or safety critical systems, hazardous environments, or any other environments requiring fail-safe performance, including any application in which the failure of the product or service could lead to death, personal injury, severe property damage or environmental harm (collectively, "high-risk uses"). Further, buyer must take prudent steps to protect against product and service failures, including providing appropriate redundancies, fail-safe features, and/or shut-down mechanisms. Lattice expressly disclaims any express or implied warranty of fitness of the products or services for high-risk uses. The information provided in this document is proprietary to Lattice Semiconductor, and Lattice reserves the right to make any changes to the information in this document or to any products at any time without notice.

INCLUSIVE LANGUAGE

This document was created consistent with Lattice Semiconductor's inclusive language policy. In some cases, the language in underlying tools and other items may not yet have been updated. Please refer to Lattice's inclusive language FAQ 6878 for a cross reference of terms. Note in some cases such as register names and state names it has been necessary to continue to utilize older terminology for compatibility.

ABSTRACT

Rapid advancements in quantum computing pose a significant threat to traditional cryptographic systems.

In an era where quantum computing threatens to upend traditional cryptographic systems, the time to act is now. This white paper delves into the vulnerabilities of current encryption protocols, unveils newly standardized PQC algorithms, and provides a strategic roadmap for organizations adopting quantum-resistant practices. By aligning with Lattice Semiconductor's innovative solutions, you can safeguard your digital assets and stay ahead in the quantum age.

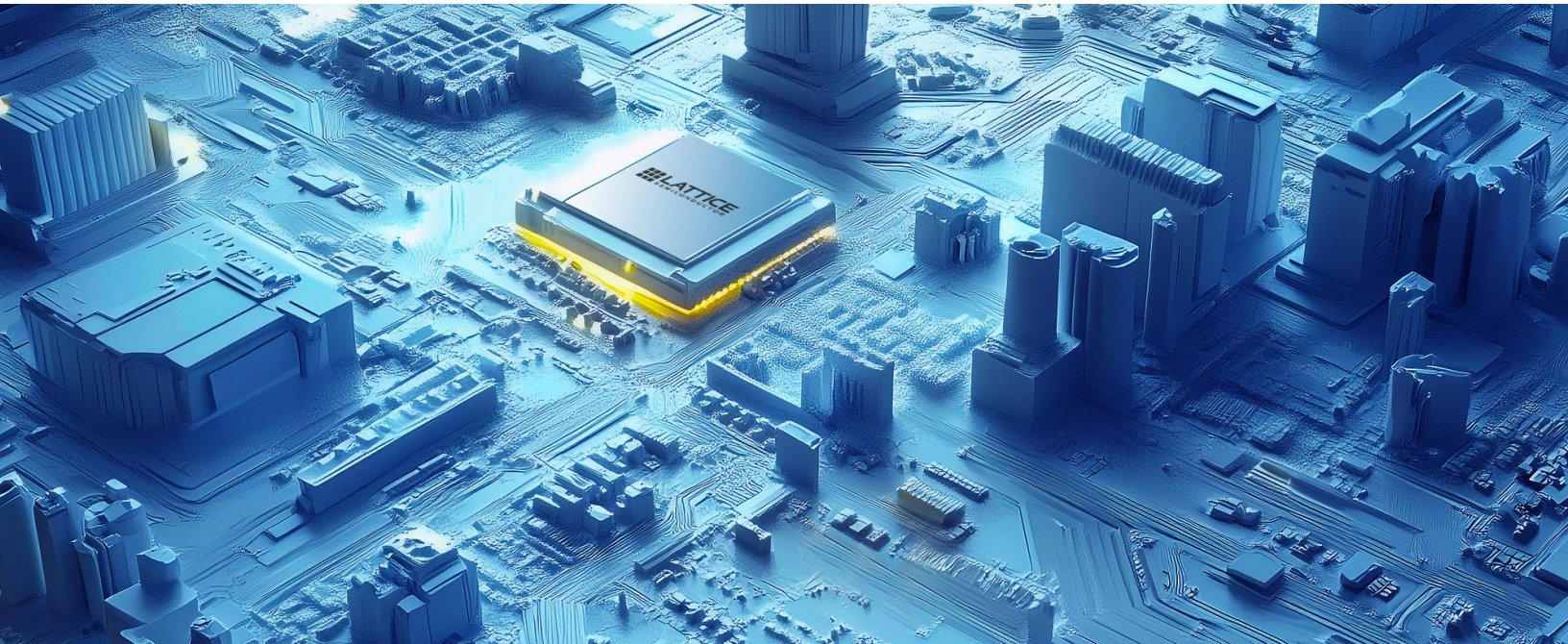


TABLE OF CONTENTS

1. Introduction

1.1. CURRENT CRYPTOGRAPHIC CHALLENGES

Quantum computing is not just a theoretical concept – it is rapidly approaching a reality that will compromise the very foundation of global digital security. Virtually all of today's security systems utilize RSA and ECC encryption algorithms, from securing financial transactions to safeguarding private communications. These traditional encryption methods are on the brink of obsolescence in the face of quantum algorithms capable of breaking them with ease[1]. The shift to quantum-resistance cryptography isn't just a recommendation; it is essential. Quantum computers are still being developed; however, the window to defend against their attacks is rapidly closing.

Now is the time to fortify your defenses and maintain the integrity of global digital security.

1.2. PQC ADOPTION AND CRYPTO AGILITY

Migration from RSA and ECC encryption to post-quantum algorithms requires updating the entire security infrastructure. This impacts everything from Public Key Infrastructure (PKI) systems and Hardware Security Modules (HSMs) to communication protocols and hardware crypto engines. PQC is a new technology and will continue to evolve. Cryptographic solutions must support "crypto agility" to adapt to new or updated standards.

In most cases, migration to PQC algorithms requires changes at the hardware level. Systems designed using field programmable gate arrays (FPGAs) have a significant advantage in adopting PQC algorithms. The inherent adaptability of FPGAs makes them ideal for PQC migration. As PQC algorithms continue to evolve, the ability of FPGAs to adapt through reconfigurability provides a significant advantage, ensuring that cryptographic implementations can stay current with the latest and most secure standards. This flexibility is crucial in maintaining the integrity of systems in the face of rapidly advancing quantum computing capabilities.

Lattice Semiconductor's FPGA products provide built-in support for NIST approved PQC algorithms and support crypto agility, making them an ideal choice for security critical operations and PQC migration efforts.

1.3. QUANTUM COMPUTING ADVANCES

Quantum computing has evolved from early theoretical discussions to practical implementations. Researchers have demonstrated quantum supremacy[2]. This section highlights the benefits of quantum computers as well as the threat they pose. Quantum algorithms, like Shor's algorithm for factoring and Grover's algorithm for searching, pose imminent threats to cryptographic algorithms and necessitate a shift to PQC. Due to their unique operational characteristics, quantum computers excel at solving certain types of problems that are exceptionally challenging for classical computers. Some areas where quantum computing shows promising potential include:

Optimization Problems: Optimizing the routing of delivery vehicles, scheduling flights, or managing supply chains by efficiently exploring multiple combinations.

Simulation of Quantum Systems: In fields such as material science and pharmacology, researchers can use quantum computers to understand complex molecules, leading to the discovery of new materials and drugs.

Machine Learning and Artificial Intelligence: Handling and processing large datasets more efficiently, leading to more powerful predictive models and faster processing times in areas like autonomous driving and personalized medicine.

Problem Solving in Theoretical Physics: Quantum computing can contribute significantly to theoretical physics by providing insights into quantum mechanics and other complex physical theories. This will facilitate advancements in understanding high-energy physics, gravitation, chemistry, and cosmology.

1.4. THE QUANTUM THREAT

Cryptography: Quantum computers can break many of the current cryptographic systems by efficiently solving problems foundational to Public Key cryptography, such as integer factorization and discrete logarithms. This capability will compromise data security systems.

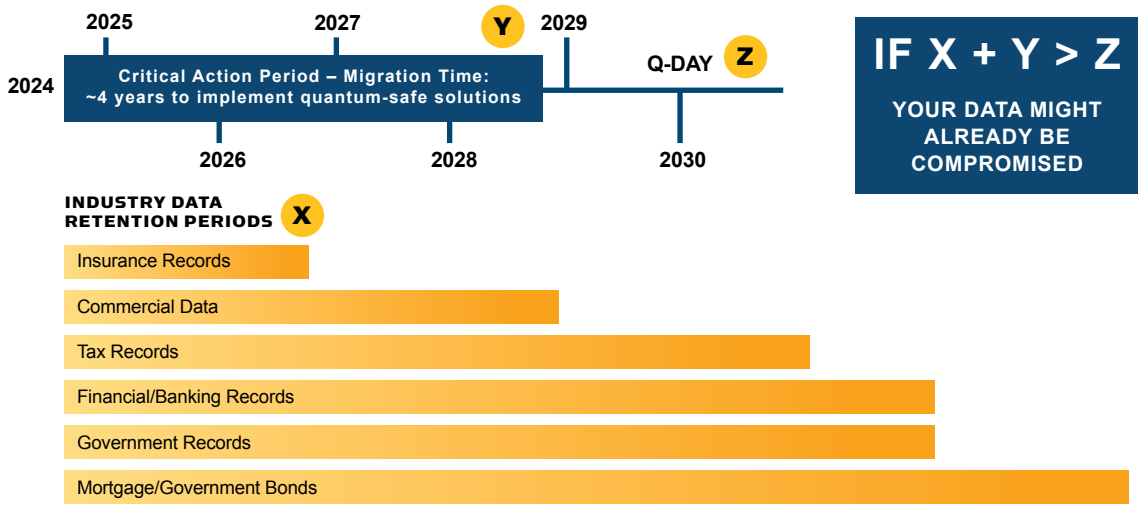
The development and scaling of quantum computing technology hold the promise of making significant breakthroughs in many areas, potentially leading to solutions currently unimaginable with classical computing technologies. However, the potential to solve such problems also highlights the need for quantum-safe encryption methods to protect sensitive information from future quantum threats.

2. Urgency To Adopt PQC

2.1. WHAT IS AT RISK

Without quantum-safe cryptography, all information transmitted on public channels, now or in the future, is vulnerable. Encrypted data stored today can be decrypted later once quantum computers become more advanced. The integrity and authenticity of transmitted information will be compromised, violating regulatory requirements for data privacy and security. This risk affects: government and military communications, financial and banking transactions, medical data and healthcare records, personal data stored in the cloud, and access to confidential corporate networks. See Figure 1.

Figure 1: Why Acting Now Matters



The time to act is now. What's your quantum readiness plan?

2.2. HARVEST NOW, DECRYPT LATER ATTACKS

Harvest now, decrypt later (HNDL) attacks, also called store now, decrypt later (SNDL) attacks, pose an immediate security concern. Attackers record encrypted data now, intending to decrypt it once quantum computing advances. For organizations that require long-term data security, this is a serious threat and demands immediate action. See Figure 2.

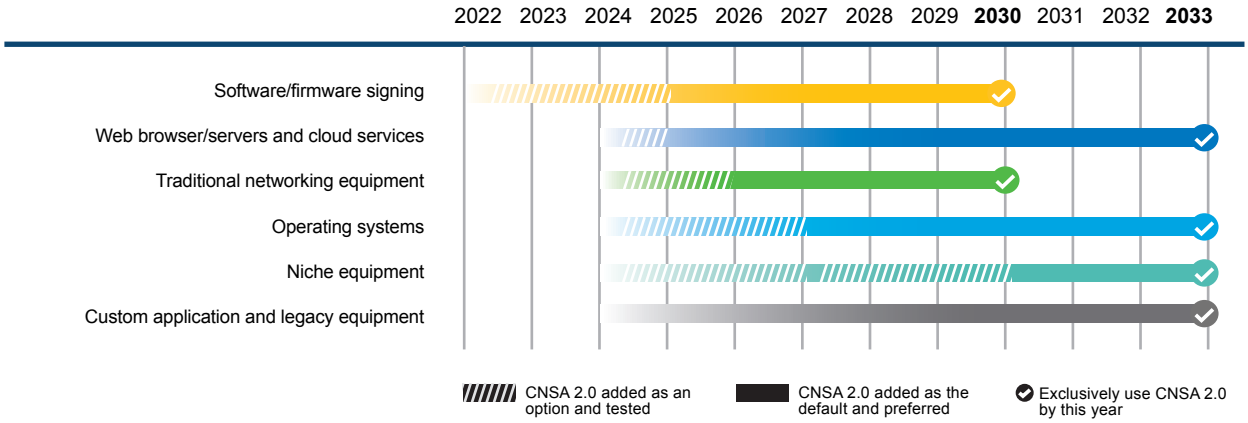
2.3. CNSA 2.0 TIMELINES

On September 7, 2022, the NSA released the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) requirements[3]. This document specifies the encryption algorithms to be used in systems related to national security. Non-compliance is not just risky; it is unacceptable. Aligning with these standards is crucial for any organization handling sensitive data in US infrastructure. See Figure 2.

CNSA 2.0 mandates the use of the following PQC algorithms, in some cases as soon as 2025:

- XMSS/LMS
- ML-DSA (CRYSTALS-Dilithium)
- ML-KEM (CYRSTALS-Kyber)
- XMSS and LMS are approved for code signing and code validation use cases

Figure 2: CNSA 2.0 Timeline

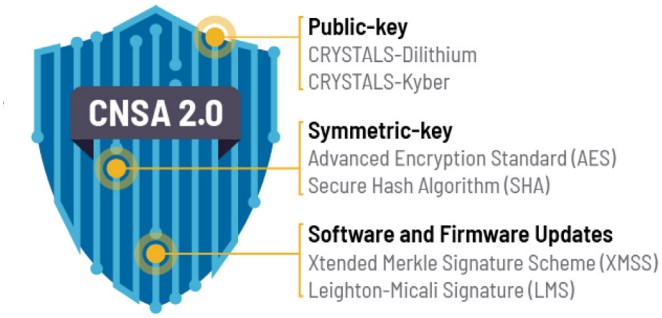


ML-DSA and ML-KEM are approved as the new Public Key encryption algorithms, replacing RSA, Diffie-Hellman Key Exchange, Elliptic Curve Diffie-Hellman (ECDH), and Elliptic Curve Digital Signature Algorithm (ECDSA). AES-256 remains the standard for symmetric encryption. Secure Hash Algorithm SHA-384 or SHA-512 remains the standard hashing algorithm.

See Figure 3 for the CNSA 2.0 algorithm suite. Critical dates in the CNSA 2.0 requirements include:

- **Software/Firmware Signing:** PQC algorithms must be used as the default and preferred algorithm by 2025
- **Web Browsers/Servers and Cloud Services:** PQC algorithms must be used as the default and preferred algorithm by 2026
- **Traditional Networking Equipment:** PQC algorithms must be used as the default and preferred algorithm by 2025
- **Operating Systems:** PQC algorithms must be used as the default and preferred algorithm by 2027

Figure 3: CNSA 2.0 Algorithm Suite



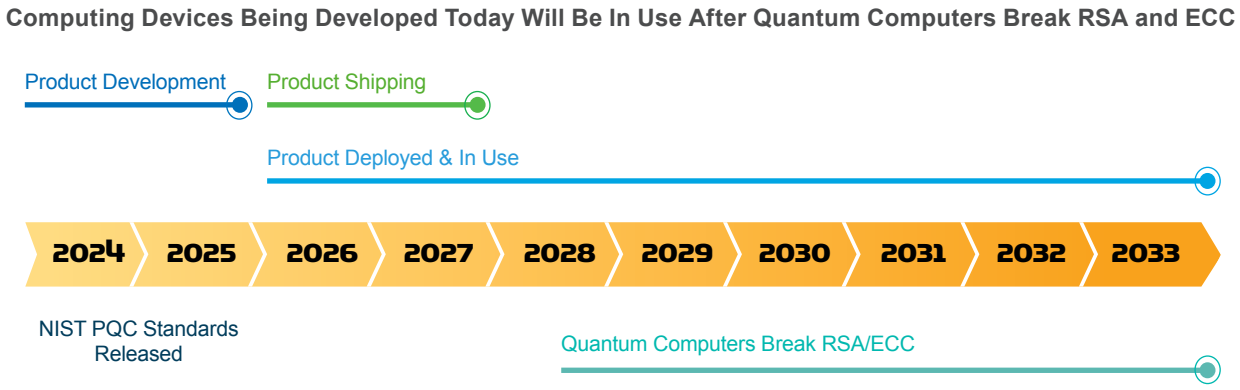
Source: NSA Cybersecurity Advisory, Announcing the Commercial National Security Algorithm Suite 2.0

2.4. DEVICE LIFE SPANS VS. QUANTUM COMPUTER DEVELOPMENT TIMELINES

Devices designed today may still be in use 15 to 20 years from now. The security implemented now must withstand future quantum threats. Quantum computers capable of breaking current encryption algorithms are expected to become operational within the next decade, posing an imminent threat to long-term data security.

Devices such as cars and those used in critical infrastructure like the electrical grid have operational lifespans extending 15 to 20 years into the future, meaning they will be in use well into the quantum era. This creates a critical security gap, as systems deployed now with traditional encryption will become vulnerable within their service life due to quantum attacks. Therefore, it's imperative to integrate quantum-resistant cryptography into these long-lived devices today to ensure their security throughout their operational lifespan. See Figure 4.

Figure 4: Device Life Spans vs. Quantum Computer Development



2.5. QUANTUM COMPUTER ROADMAP

Most experts believe a quantum computer will be able to break RSA and ECC encryption within the next decade. The US National Institute of Standards and Technology (NIST), one of the driving forces behind the development and adoption of new post-quantum cryptography encryption algorithms, predicts that it could be as early as 2030[4]. The Quantum Threat Timeline Report from the Global Risk Institute states that "there is no known fundamental barrier to realizing large-scale quantum computing. Thus, cyber risk managers should consider it more a matter of "when" than of "if"[5].

Researchers and leading technology companies are investing heavily in quantum computing technology, resulting in significant advances in quantum computing. For example, Google announced a 105-qubit version of its quantum computer in December of 2024, and they project to reach 1M qubits by 2030. IBM, D-Wave, Rigetti, and Fujitsu, among others, have developed commercially viable quantum computers and are also making rapid advancements in the capabilities of their systems.

3. PQC Initiatives Around The World

National governments and international standards bodies are working on guidance and regulations defining PQC algorithm requirements and adoption timelines. These standards define both the PQC algorithms to be used and the timelines for adopting PQC algorithms. The NIST PQC standards provide the foundation for the algorithms used throughout the world. Even those countries that are considering using algorithms other than those defined by NIST are still heavily influenced by the NIST algorithms. In some cases (France and Germany), they are adopting both the algorithms specified by NIST and some of the algorithms NIST considered but did not standardize. In other cases (China), they are considering country-specific algorithms. See Figure 5.

Figure 5: PQC Initiatives Around The World

COUNTRY/REGION	PQC ALGORITHMS UNDER CONSIDERATION	PUBLISHED GUIDANCE	TIMELINE FOR ADOPTION
Australia	NIST algorithms	CTPCO (2023)	Start implementation (2025/2026)
Canada	NIST algorithms	Cyber Centre (2021)	Start implementation (2025)
China	China specific	CACR (2020)	Start planning now (2025)
European Union	NIST algorithms	ENISA (2022), European Commission (2024)	Start planning & implementation now (2025)
France	NIST, FrodoKEM, LMS, XMSS	ANSSI (2023)	Start implementation now (2025)
Germany	NIST algorithms, LMS, XMSS, FrodoKEM, ClassicMcEliece-KEM	BSI (2022)	Start implementing now (2025)
Japan	Monitoring NIST	CRYPTREC (2022, 2024)	Start planning now (2025)
Netherlands	AES, NIST, SHA-DSA-256, XMSS	NCSC (2023)	Draft action plan now with defined timeframes (currently no mandate on timeframes)
New Zealand	NIST algorithms	NZISM (2022)	Start planning now (2025)
Singapore	Monitoring NIST	MCI (2022), Monetary Authority of Singapore (2024)	Start planning now (2025)
South Korea	KpqC	MSIT (2024)	Additional, South Korea specific algorithms to be selected in 2024
United Kingdom	NIST algorithms, LMS, XMSS	NCSC (2023)	Start implementing now (2025)
United States	NIST algorithms, LMS, XMSS	CISA (2021, 2022, 2023) NIST (2023) NSA (2022, 2024) White House (2022, 2024) Congress (2022)	Start implementing now (2025); implementation is required beginning in 2025

4. Which Algorithms Are Affected By Quantum Computers

Understanding which algorithms are vulnerable is the first step towards securing your system. Quantum computers will break existing asymmetric encryption algorithms like RSA and ECC. Increasing the key length of these algorithms will not provide any effective protection against a quantum attack. The algorithms must be replaced with quantum-resistant ones as defined by NIST and required by various regulating authorities. See Figure 6.

Symmetric encryption algorithms like AES are also affected, though to a lesser extent. Here upgrading all symmetric encryption to AES 256 will provide quantum attack resistance. The approved algorithms are categorized based on the underlying math used.

Lattice-based Algorithms: ML-KEM (Kyber), ML-DSA (Dilithium), and FN-DSA (Falcon) offer security based on complex lattice structures that are computationally challenging for quantum computers.

Hash-based Signatures: LMS (Leighton-Micali Signature), XMSS (eXtended Merkle Signature Scheme), and SLH-DSA (SPHINCS+) are hash-based signature schemes and are known for their security.

Figure 6: Algorithms Affected By Quantum Computers

CRYPTOGRAPHIC FUNCTION	CLASSICAL ALGORITHM	POST-QUANTUM STATUS	POST-QUANTUM REPLACEMENT
Random Number Generation	TRNGs	Quantum safe	No replacement needed
Symmetric Encryption	AES-128, AES-256	AES-256 is quantum safe AES-128 is vulnerable to quantum attacks	AES-256 required
Cryptographic Hashing	SHA2, SHA3	Larger output size needed	SHA2-384/512 or SHA3-384/512 required
Key Exchange	RSA, Diffie-Hellman, ECDH	Broken	ML-KEM (Kyber)
Digital Signature	RSA, ECDSA	Broken	ML-DSA (Dilithium) SLH-DSA (SPHINCS+) FN-DSA (Falcon) LMS, XMSS (code signing only)

5. PQC Algorithms and NIST Standards

On August 13, 2024, the U.S. National Institute of Standards and Technology (NIST) marked a significant milestone in cybersecurity by finalizing the first set of post-quantum cryptography standards.

The NIST standards provide the foundation for migration to PQC algorithms worldwide. These standards were created through the collaboration of security researchers and companies throughout the world, and they are being adopted by countries across the globe. Most countries are adopting NIST standards. A few countries are adopting their own country-specific algorithms, but these algorithms are derived from the NIST standards. In a few other cases, countries are adopting the NIST algorithms but also accepting a few additional algorithms. Those additional algorithms were finalists in the NIST process but not selected by NIST for standardization.

In the August 2024 release, NIST approved four algorithms designed to secure digital communications. These include:

- ML-KEM (CRYSTALS-Kyber)
- ML-DSA (CRYSTALS-Dilithium)
- SLH-DSA (SPHINCS+)
- FN-DSA (Falcon)

Implementation and Transition: These algorithms are intended for immediate integration into digital systems to enhance security against quantum attacks. NIST provides detailed guidelines on implementing these algorithms, aiming for a smooth transition without compromising current operational standards.

Future Considerations: NIST continues to evaluate additional algorithms for future standardization. Additional algorithms will be standardized to further enhance the robustness of cryptographic defenses and to provide algorithms optimized for a variety of use cases.

Conversion to new algorithms is a major undertaking, impacting PKI systems, TLS and VPN protocols, crypto libraries, HSMs, TPMs, and a host of other systems. Rolling out these new algorithms across the entire ecosystem and supply chain will take years. Companies must act now to begin migrating to PQC. Lattice Semiconductor provides the expertise and solutions to make this migration seamless and efficient.

6. Migration to PQC Algorithms

PQC algorithms have now been standardized, and developers can begin migrating to these new, NIST-approved algorithms. With Lattice's advanced FPGA technology, you can achieve a seamless and future-proof migration, ensuring your systems are always protected with the latest cryptographic standards. See Figure 7.

Figure 7. Migration to PQC Algorithms

ALGORITHM	CNSA 2.0 SUITE ALGORITHM	NIST STANDARD AVAILABLE	TYPE	PURPOSE	REPLACES
LMS	Yes	Yes	Stateful hash-based digital signature scheme	Code and firmware signing	ECDSA, RSA
XMSS	Yes	Yes	Stateful hash-based digital signature scheme	Code and firmware signing	ECDSA, RSA
ML-DSA (Dilithium)	Yes	Yes	Lattice-based	All digital signing use cases	ECDSA, RSA
ML-KEM (Kyber)	Yes	Yes	Lattice-based	Key exchange and encryption	ECDH, RSA, Diffie-Helman
SLH-DSA (SPHINCS+)	No	Yes	Stateless hash-based	All digital signing use cases	ECDSA, RSA
FN-DSA (Falcon)	No	No	Lattice-based	All digital signing use cases	ECDSA, RSA

LMS and XMSS are both stateful hash-based digital signature algorithms, meaning that the private key includes a state value that must be maintained. Each time a signature is generated, the state value must be updated. These algorithms are well suited for code signing use cases. The standards require signing operations and state management to be performed within an HSM to ensure security and proper state management. As a result, these algorithms are really only useful for code signing and are not well suited for use as general purpose digital signature algorithms.

ML-DSA (Dilithium) and ML-KEM (Kyber) are both lattice-based algorithms that have been fully standardized by NIST and are CNSA 2.0 approved. ML-DSA is a general-purpose digital signature algorithm that can be used for all use cases, including code signing. ML-KEM is a Key Exchange Mechanism and will be used by protocols such as TLS and IPSec to exchange AES keys.

SLH-DSA (SPHINCS+) is a stateless hash-based digital signature algorithm. This algorithm has also been fully standardized by NIST and can be used for all digital signing use cases. It is not, however, a CNSA 2.0 approved algorithm. SLH-DSA also suffers from poorer performance than the other post-quantum digital signature algorithms[6]. There are scenarios in which SLH-DSA will be used, but it is not well suited for performance critical applications.

FN-DSA (Falcon) has been selected by NIST for standardization, but the FN-DSA standard is not expected to be completed until 2025.

6.1. CHALLENGES IN IMPLEMENTING PQC ALGORITHMS

Implementing PQC algorithms is not without its challenges. Organizations face a learning curve on the adoption of new algorithms. The key sizes, signature sizes, and performance characteristics for PQC algorithms differ significantly from classical algorithms. They also differ significantly between PQC algorithms.

Organizations must familiarize themselves with these new algorithms to understand the tradeoffs between various algorithms. For example, signature verification times are very fast with both ML-DSA and LMS; and both have relatively large signature sizes. They differ significantly in other aspects. For example, LMS Public Key sizes are very small, whereas ML-DSA Public Keys are relatively large.

Organizations should choose a trusted partner, such as Lattice Semiconductor, that has experience and expertise with PQC algorithms and should begin implementing proof of concept (POC) solutions to gain the knowledge needed to begin migrating their devices and systems to PQC algorithms.

Lattice Semiconductor provides products with PQC algorithms already integrated into the on-device crypto engines. This enables customers to quickly and easily upgrade their solutions to support PQC. Development boards are available for customers who are implementing POCs to accelerate their migration to PQC.

7. Achieving Quantum Resistance in Major Use Cases

7.1. TRANSPORT LAYER SECURITY (TLS) & SECURE COMMUNICATIONS

TLS and other secure communication protocols utilize three separate encryption operations in securing data:

- **Authentication:** RSA/ECDSA replaced by ML-DSA, SLH-DSA, or FN-DSA
- **Key Exchange:** RSA, ECDH or Diffie-Helman replaced by ML-KEM
- **Bulk Data Encryption:** AES-128 or AES-256 ensure usage of AES-256

For use cases in which HNDL attacks are a concern, companies should prioritize the implementation of Kyber (ML-KEM) in their communication protocols. Use of ML-KEM will ensure that session keys cannot be recovered by quantum computers, rendering HNDL attacks ineffectual.

7.2. CODE SIGNING

LMS, XMSS, and ML-DSA can be used for code signing use cases.

7.3. ROOT OF TRUST

The RoT solution will perform signing on the device to allow verification of configuration data, as well as validation of other components of a broader system. ML-DSA is the best algorithm for RoT use cases, as it allows signing on the device.

7.4. NEED FOR CRYPTO AGILITY

The development of post-quantum cryptography is still in its nascent stages. As the field evolves, it's crucial that cryptographic solutions maintain a high degree of agility to adapt to new standards and discoveries. This need for 'crypto agility' is essential because it allows systems to swiftly integrate advancements in cryptography without extensive overhauls, ensuring ongoing security against emerging quantum threats.

8. Lattice Semiconductor: Your PQC Partner

FPGAs play a vital role in modern applications, and Lattice Semiconductor leads the way with security capabilities that protect against existing and emerging threats. Our Root of Trust solutions safeguard devices from power-up and throughout operation.

FPGAs are inherently flexible, enabling reprogramming to align with evolving standards. This adaptability ensures longevity and cost savings, making them ideal for secure, future-proof solutions. Lattice FPGAs serve as 'crypto agile' solutions, essential for transitioning to PQC standards. With Lattice, you can seamlessly upgrade hardware with PQC algorithms and patch vulnerabilities in existing systems.

Lattice Semiconductor has firmly established itself as a thought leader in the post-quantum cryptography arena, evidenced by successful proof-of-concept implementations on our advanced FPGA platforms. Leveraging a proven legacy of trusted Root of Trust solutions, we deliver robust security that is unbypassable when our secure devices are used for power sequencing. Our PQC solutions are built on hardened security algorithms in these secure control FPGAs and feature layered-on crypto agility, enabling seamless field upgrades of PQC algorithms as standards evolve. This ensures that your systems remain secure and adaptable, providing long-term protection against emerging quantum computing threats. Furthermore, Lattice Semiconductor is proactively rolling out solutions that incorporate all NIST-approved and CNSA 2.0-required PQC algorithms. These include:

- **ML-KEM (CRYSTALS-Kyber):** Replacing RSA, Diffie-Hellman, and ECDH
- **ML-DSA (CRYSTALS-Dilithium):** Replacing RSA and ECDSA
- **XMSS (eXtended Merkle Signature Scheme):** A stateful hash-based digital signature algorithm approved for code signing and verification
- **LMS (Leighton-Micali Signature):** Another stateful hash-based digital signature scheme for code signing and verification

Our development roadmap meticulously aligns with regulatory timelines, ensuring our customers can meet or exceed compliance requirements well before the mandated deadlines. By integrating these advanced, standardized algorithms into our FPGA solutions, we provide organizations with the essential tools to transition smoothly to quantum-resistant cryptography. With Lattice, you gain a trusted partner committed to delivering timely, compliant, and robust security technologies that safeguard your assets against current and future quantum threats.

8.1. MITIGATING TRANSITION RISKS: LATTICE'S SUPPORT FOR HYBRID CRYPTOGRAPHIC STRATEGIES

In addition to our advanced PQC offerings, Lattice Semiconductor continues to support all classical asymmetric algorithms, including ECC up to 512 bits and RSA up to 4096 bits, as well as AES-256 for symmetric encryption. We also provide comprehensive support for cryptographic hashing algorithms such as SHA-2 and SHA-3. This extensive algorithm support empowers our customers to implement hybrid cryptographic flows when necessary. Implementing a hybrid flow—combining both classical and quantum-resistant algorithms—can be a judicious approach during the transitional period to PQC standards. Such a strategy ensures backward compatibility and interoperability with existing systems and protocols while simultaneously adopting new quantum-safe algorithms. It provides an added layer of security, allowing organizations to mitigate risks associated with the immediate and complete overhaul of their cryptographic infrastructure.

By offering support for both classical and PQC algorithms, including essential hashing functions, Lattice enables customers to transition smoothly and securely to quantum-resistant cryptography, tailoring the migration to their specific operational needs and regulatory timelines.

At Lattice Semiconductor, we prioritize the robustness and reliability of our post-quantum cryptography and classical cryptographic algorithms. Our solutions incorporate hard and soft algorithms sourced from esteemed industry-leading IP vendors recognized for their excellence in cryptographic technologies. These algorithms have undergone validation adhering to stringent standards set by the National Institute of Standards and Technology. Additionally, they have been subjected to comprehensive penetration testing within customer system-level environments to ensure their security and resilience against potential threats in real world applications.

Our collaboration with these trusted IP vendors, who are actively pursuing additional certifications for their algorithms, enhances the credibility and integrity of our security offerings. This rigorous approach not only affirms the strength of Lattice's cryptographic solutions but also supports our customers in achieving their own compliance objectives. By integrating certified and thoroughly tested cryptographic algorithms, organizations can confidently secure their systems and may find it facilitates meeting advanced security certifications. This alignment can be particularly beneficial for customers aiming for certifications such as FIPS 140-3 Level 2 at the system level, providing a solid foundation for compliance with stringent regulatory standards.

9. Conclusion

The finalization of post-quantum cryptography standards by NIST marks a pivotal moment in digital security. Quantum computing advancements are no longer distant possibilities but imminent realities threating to render traditional cryptographic systems obsolete. Organizations worldwide must urgently upgrade their cryptographic infrastructures to align with these new standards. The time to act is now.

Migrating from classical encryption algorithms like RSA and ECC to quantum-resistant alternatives is a significant undertaking that will span several years. As companies plan for this transition, embracing crypto agility—the ability to adapt quickly to new algorithms as PQC continues to evolve—becomes essential. Field programmable gate arrays (FPGAs), with their inherent flexibility and reconfigurability, will play a crucial role.

Unlike fixed-function hardware, FPGAs allow for swift updates to implement the latest cryptographic standards, ensuring that security systems remain robust and future-proof against rapid advancements in quantum computing.

Lattice Semiconductor stands ready to support organizations during this transformative period. Leveraging proven expertise in PQC and a legacy of trusted security solutions, Lattice offers advanced FPGA technologies that enable seamless migration to quantum-resistant cryptography. By supporting both NIST-approved PQC algorithms and classical encryption methods, including ECC, RSA, AES- 256, and hashing algorithms like SHA-2 and SHA-3, Lattice empowers customers to implement hybrid cryptographic flows. This approach facilitates backward compatibility and interoperability with existing systems while adopting new quantum-safe algorithms, mitigating risks associated with a complete infrastructure overhaul. The proactive adoption of quantum-resistant standards, complemented by adaptable technologies like Lattice's FPGAs, is vital for maintaining the integrity and security of digital infrastructures in the post-quantum era. By integrating certified and thoroughly tested cryptography, organizations can confidently secure their systems and meet compliance objectives. Now is the moment to secure your digital future. The shift towards resilient cryptographic measures will safeguard sensitive information and systems against the burgeoning quantum and harvest now decrypt later threats, reinforcing trust and security in our increasingly digital world. Organizations should act promptly to adopt PQC solutions and partner with trusted leaders to ensure their critical data and infrastructure remain protected.

10. References:

1. Shor, W (1995) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. https://arxiv.org/abs/quant-ph/9508027
2. Quantum Supremacy is the ability to perform calculations that are too difficult for a classical computer to perform in a reasonable amount of time, for narrowly defined tasks. https://www.nature.com/articles/s41586-019-1666-5
3. Announcing the commercial national security algorithms ... National Security Agency. (2022). https://media.defense.gov/2022/ Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
4. Chen, L., Jordan, S., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., & Liu, Y.-K. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf
5. Mosca, Michele, Piani Marco (2024). Quantum Threat Timeline Report 2023, Global Risk Institute. https://globalriskinstitute.org/ publication/2023-quantum-threat-timeline-report/
6. Westerbaan, B., Meunier, T., Rubin, C. D., Faz-Hernández, A., Tholoniat, P., Kozlov, D., & Wang, M. (2024, July 29). NIST's Pleasant Post-quantum surprise. The Cloudflare Blog. https://blog.cloudflare.com/nist-post-quantum-surprise

11. Appendix:

XMSS, LMS, AND THE NIST PQC STANDARDS

August 13, 2024, the U.S. National Institute of Standards and Technology (NIST) finalizing the first set of post-quantum cryptography (PQC) standards. The algorithms that were standardized are:

- ML-KEM (CRYSTALS-Kyber)
- ML-DSA (CRYSTALS-Dilithum)
- SLH-DSA (SPHINCS+)
- FN-DSA (Falcon)

While it is true that these are the first general purpose PQC algorithms standardized by NIST, they were preceded by LMS and XMSS, two Stateful Hash-Based Signature Schemes whose standards were published by NIST on October 29, 2020.

NIST describes XMS and LMS algorithms as "…secure against the development of quantum computers, but they are not suitable for general use because their security depends on careful state management. They are most appropriate for applications in which the use of the private key may be carefully controlled…".

This makes XMS and LMS well suited for coding signing/code verification use cases such as Secure Boot and secure software updates, but not for most other use cases. For code signing, the private key and associated state management can be performed by an HSM capable of handling the state management requirements.

PQC ALGORITHM FAMILIES

Post-quantum cryptography utilizes different mathematical approaches than RSA and ECC to create algorithms that will run on traditional computers without being vulnerable to attacks from either quantum computers or traditional computers.

The NIST process considered algorithms utilizing several different mathematical approaches. The types of algorithms considered were:

- Code-Based (Classical McEliece)
- Lattice-Based (CRYSTALS-KYBER, NTRU, SABER, CRYSTALS-DILITHIUM, Falcon)
- Isogeny-Based (SIKE)
- Multivariate (Rainbow)
- Zero-Knowledge (Picnic)
- Hash-Based (SPHINCS+)
- Stateful Hash-Based (XMSS, LMS) (not part of the NIST process, but previously standardized by NIST)

Each algorithm type utilizes a different mathematical approach to achieve security that cannot be broken by classical or quantum computers within a reasonable time frame. NIST chose to standardize algorithms that are using Lattice-Based, Hash-Based, and Stateful Hash-Based approaches.

Lattice-based Algorithms: ML-KEM (Kyber), ML-DSA (Dilithium), and FN-DSA (Falcon) offer security based on complex lattice structures that are computationally challenging for quantum computers. Lattice-based cryptography is favored due to its presumed security against quantum and classical computers and its efficiency in operation. The Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) are Lattice-based mathematical problems which underpin the security of Lattice-based methods.

Stateful Hash-based Signatures: LMS (Leighton-Micali Signature) and XMSS (eXtended Merkle Signature Scheme) are stateful hash-based signature schemes and are known for their simplicity and security. As the name implies, these schemes rely on hash functions such as SHA2 or SHA3 for security. These algorithms are stateful, meaning that the private key includes a state value that must be maintained. Each time a signature is generated, the state value must be updated. These algorithms are well suited for code signing use cases. The standards require signing operations and state management to be performed within an HSM to ensure security and proper state management. As a result, these algorithms are really only useful for code signing and are not well suited for use as general purpose digital signature algorithms.

Hash-based Signatures: SLH-DSA (SPHINCS+) is a hash-based signature scheme. Like LMS and XMSS, it relies on hash functions such as SHA2 or SHA3 for security. Since it is not a stateful algorithm, the private key does not include a state value that must be maintained. This eliminates the requirement for updating and maintaining a state value, making this algorithm suitable for general purpose use.

HNDL ATTACKS EXPLAINED

HNDL attacks store all the packets for the entire communication session, including the key exchange operation. These attacks will then use a quantum computer to attempt to break the encryption used in the key exchange operation. If successful, the attack will recover the session key (AES key) which can then be used to decrypt the data transmitted during the communication session.

In other words, even though AES-256 is quantum safe, using it in TLS is not sufficient to ensure the protocol is quantum safe. The quantum computer will break the asymmetric encryption (RSA, ECDH, or Diffie-Helman) used to exchange the session key (AES key). Once the asymmetric encryption is broken, the AES key can be obtained and the data encrypted with AES can be decrypted.

To protect against HNDL attacks, communication protocols must utilize ML-KEM, which is currently the only standardized PQC algorithm for use in key exchange operations.

READY TO LEARN MORE?

To learn more about Lattice low power FPGA-based solutions for industrial, automotive, communications, computing, and consumer applications, visit **www.latticesemi.com** or contact us at **www.latticesemi.com/contact** or **www.latticesemi.com/buy**.

TECHNICAL SUPPORT ASSISTANCE

Submit a technical support case through **www.latticesemi.com/techsupport**.
For frequently asked questions, please refer to the Lattice Answer Database at **www.latticesemi.com/Support/AnswerDatabase.**

V.2 WP0041