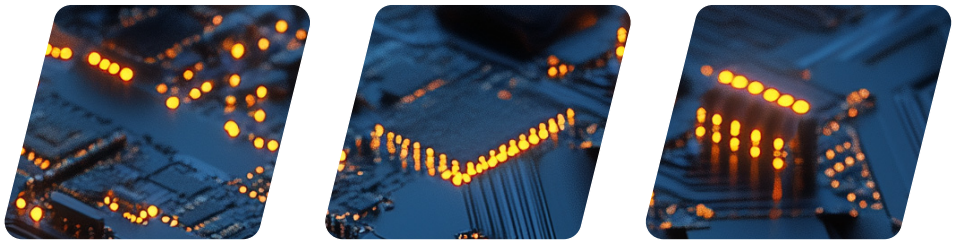
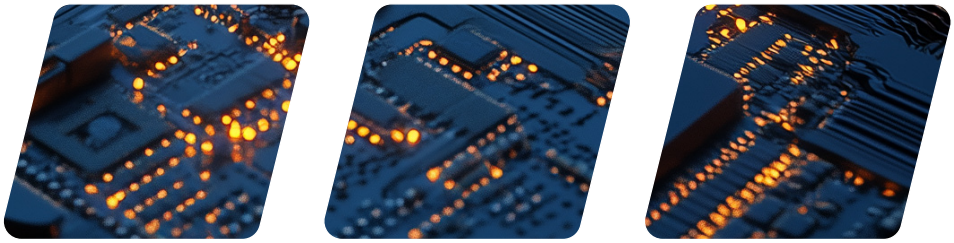


Future-Proof Trust: Securing Digital Systems with Lattice RoT FPGAs and Complete CNSA 2.0 Algorithm Coverage



White Paper

Author:
Ramya Chandrasekaran, Sr. Manager Product Marketing, Lattice Semiconductor
Temoc Chavez Corona, Security Architecture Engineer, 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.

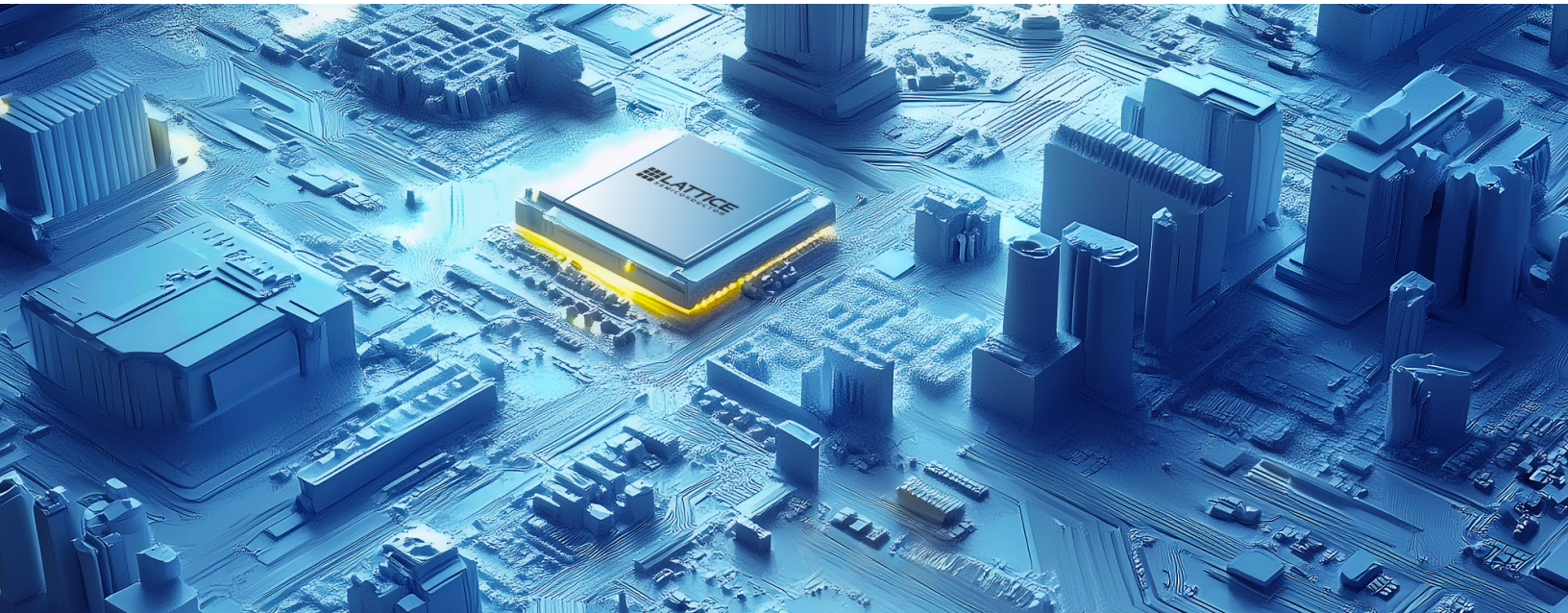


TABLE OF CONTENTS

Introduction

As data breaches surge and attackers grow more sophisticated, the rise of quantum computing adds a new layer of urgency—enabling adversaries to steal encrypted data today and decrypt it tomorrow, threatening the long-term trust in all digital systems. In response, governments and industries are accelerating regulations and adopting post-quantum cryptography (PQC) standards like CNSA 2.0 and NIST's FIPS 203/204 to safeguard critical infrastructure and ensure compliance. Trust in digital systems now depends on crypto-agility and hardware-based roots of trust that can adapt to evolving threats. This white paper explains why PQC matters now, how nations and industries are responding, and how Lattice Semiconductor's PQC enabled RoT FPGAs can equip organizations to secure their future in a quantum-enabled world.

Why Post-Quantum Cryptography Matters Now

The foundation of post-quantum security must begin with trusted hardware. Lattice's Root of Trust (RoT) FPGAs provide that secure anchor. They are uniquely designed to execute post-quantum algorithms with the broadest Commercial National Security Algorithm (CNSA) 2.0 coverage in the industry—supporting every mandated standard, including ML-KEM, ML-DSA, LMS, and XMSS. This ensures customers are not just future-proofed, but compliant with the regulatory deadlines already set by agencies like the National Security Agency (NSA).

Unlike traditional microcontrollers or generic hardware security modules, Lattice RoT FPGAs combine:

- Complete CNSA 2.0 compliance with all approved Post-Quantum Cryptography (PQC) algorithms
- Hardware-enforced Root of Trust, securing the boot chain, protecting firmware, and eliminating denial-of-service risks
- Crypto agility, enabling smooth migration between classical, hybrid, and PQC algorithms
- Efficiency with up to 10X faster secure boot and 50–75% lower power than competing devices

This makes Lattice RoT FPGAs the practical foundation on which PQC can be deployed today.

The Real Driver of Urgency

There is ongoing debate about when large-scale quantum computers will become a reality. But there is no debate about the immediate risk of "Harvest Now, Decrypt Later" (HNDL) attacks. Adversaries are already collecting encrypted communications, financial records, medical data, and classified information today—planning to decrypt them once quantum capabilities mature.

This is why governments are moving quickly. The NSA's CNSA 2.0 requires PQC adoption for software and firmware signing by 2025, with broader adoption mandated by 2027. The EU and other regions are setting similarly aggressive timelines. The runway is short, and organizations that delay migration risk exposing sensitive data to future compromise.

The message is clear: PQC is not a future concern—it is a present requirement. With Lattice RoT FPGAs as the secure foundation, organizations can begin deploying CNSA 2.0-compliant solutions now, protecting data created today from quantum threats of tomorrow.

Deep Dive in "Harvest Now, Decrypt Later" Attacks

While symmetric block encryption schemes are generally considered secure against quantum-based attacks, the protocols used to exchange or establish shared keys typically rely on asymmetric cryptography, which is vulnerable to quantum threats. The "Harvest Now, Decrypt Later" (HNDL) strategy involves adversaries—often nation-state actors or sophisticated cybercriminals—intercepting and storing encrypted data today with the intent to decrypt it in the future, once quantum computing capabilities mature.

This tactic is particularly dangerous because it targets long-lived sensitive data such as medical records, financial agreements, intellectual property, and classified communication information that retains strategic or personal value for decades. Unlike traditional attacks that seek immediate exploitation, HNDL is a long-term threat. The stolen data remains encrypted and seemingly secure, giving organizations a false sense of protection.

To mitigate this risk, organizations must begin planning for the transition to quantum-resistant key exchange mechanisms, such as ML-KEM (FIPS 203), especially for their most sensitive communications. Early adoption of post-quantum cryptographic standards is essential to ensure that data encrypted today remains secure tomorrow.

A Note About Progress on Quantum Computing World

In 2025, quantum computing made significant strides in both hardware and software. Google's 105-qubit Willow chip demonstrated exponential error reduction, completing a benchmark task in minutes that would take classical supercomputers trillions of years. Microsoft introduced Majorana 1, the first quantum processor based on topological qubits, offering a scalable path toward fault-tolerant quantum systems. While NVIDIA and Quantum Circuits advanced hybrid quantum-classical computing by integrating CUDA-Q into Aqumen, Amazon and NVIDIA also unveiled DGX Quantum, a platform combining AI superchips with quantum control systems to support real-time error correction and scalable quantum workloads.

Based on current progress, the first practical post-quantum computer—defined as one capable of breaking widely used cryptographic systems such as RSA-2048—is expected to emerge between 2030 and 2035, depending on technological advancements and implementation assumptions. At this point, all classical public key cryptographic schemes will be at risk, regardless of key size.

The Industry and Regulatory Response

The global cybersecurity industry is mobilizing in response to the looming threat posed by quantum computing. Governments and enterprises are increasingly adopting PQC to safeguard sensitive data against future quantum-enabled attacks. Some examples are the U.S. National Institute of Standards and Technology (NIST) that provides the NIST SP 800-208 recommendation for two stateful hash-based signature schemes: the eXtended Merkle Signature Scheme (XMSS) and the Leighton-Micali Signature system (LMS). And it has formalized the first set of PQC standards, including algorithms like the FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) and the FIPS 204 Module-Lattice-Based Digital Signature (ML-DSA) standards.

The European Union has launched a coordinated roadmap targeting 2030 for securing critical infrastructure with quantum-resistant encryption.

And the CNSA 2.0, released by the National Security Agency (NSA), is a comprehensive update to the cryptographic standards used in National Security Systems (NSS). It mandates the transition to quantum-resistant algorithms, replacing vulnerable schemes like RSA and ECC with lattice- and hash-based alternatives.

The transition timeline in the document is clear: software and firmware signing should begin using CNSA 2.0 algorithms by 2025, with broader adoption across NSS systems required by 2027. Full compliance across all NSS technologies is expected by 2035, making early planning and implementation critical for organizations handling sensitive or classified data.

What Does Lattice Offer?

Lattice RoT FPGAs deliver secure boot, low power operation, anti-tamper protection, bitstream and data security, real-time firmware protection, and end-to-end IP protection—all anchored in immutable hardware security functions. These foundational capabilities are available today, and PQC is built on top of this robust foundation to further strengthen resilience against emerging threats.

Lattice PQC-enabled FPGA devices are designed to meet the evolving demands of PQC by offering a broad suite of supported algorithms. Like lattice-based (ML-DSA and ML-KEM) and Hash Based Signing (LMS/XMSS), to accommodate diverse market requirements and application scenarios.

Recognizing the dynamic nature of cryptographic development, these devices are built with the crypto agility feature as main target, enabling rapid adaptation to emerging protocols and improvements.

To ease the transition to post-quantum standards, Lattice devices support hybrid cryptographic models, allowing classical and quantum-resistant algorithms to coexist for enhanced assurance.

Furthermore, they are engineered to pair seamlessly with emerging quantum technologies such as Quantum Random Number Generators (QRNGs), enabling stronger and more future-proof security solutions.

Classical + PQC Key Hierarchy

In public key signature schemes, the secrecy of the private key is the cornerstone of security. However, repeated incidents of key leakage over the years have demonstrated that key exfiltration is a real and persistent threat, making fallback mechanisms essential.

To address this, devices must support multiple valid public keys to enable secure key rotation and rapid revocation of compromised credentials.

Lattice PQC enabled devices implement this capability through a robust key hierarchy, allowing multiple valid public keys to coexist simultaneously.

The keys provisioned can be a mix of post quantum schemes like ML-DSA, XMSS or LMS alongside classical algorithms offering high flexibility to system designers.

Once provisioned, keys can be enabled, extended or revoked upon requests, supporting healthy rotation and robust lifecycle management.

This architecture ensures scalable, secure, and adaptable cryptographic operations in environments where resilience and agility are paramount.

Bitstream Authentication & User Data Signing Using PQC Schemes

The LMS and XMSS are hash-based digital signature algorithms proposed by IETF and the ML-DSA (FIPS 204) standardized by NIST are recognized as valid post-quantum cryptographic options under the CNSA 2.0 suite.

In Lattice PQC-Enabled family of devices, CNSA 2.0 algorithms are supported as available methods for bitstream authentication, a core security feature in these devices.

Customers can sign their Bitstream images with their LMS, XMSS or ML-DSA private key in their Hardware Security Module (HSM) ecosystem. This image will be authenticated when programmed in the device by the corresponding public key previously provisioned.

Customers can also use ML-DSA to sign their user data on Lattice FPGAs, ensuring that sensitive information benefits from post-quantum digital signature protection alongside bitstream authentication

Secure Channel using ML-KEM—Protection Against Harvest Now Decrypt Later

As mentioned before, one of the most critical threats posed by quantum computing is the “Harvest Now, Decrypt Later” strategy, where encrypted data is stolen and stored until quantum computers become powerful enough to break classical encryption schemes.

While traditional Nexus devices support secure channel creation using RSA or ECDH, these methods are vulnerable to HNDL attacks.

To address this, Lattice PQC enabled devices incorporate hardware-based ML-KEM for quantum-resistant key encapsulation.

These devices support the full ML-KEM suite, enabling secure communication either by encapsulating a shared secret using an external party’s public key or by initiating the exchange and decapsulating keys generated by other trusted agents.

Once established, the shared key can be immediately used with onboard AES engines to create a secure channel resistant to future quantum attacks.

Furthermore, Lattice PQC enabled devices support all ML-KEM security levels (as required in CNSA2.0), including ML-KEM-512, ML-KEM-768, and ML-KEM-1024, allowing users to tailor security and performance to their specific application needs.

SPDM with ML-DSA/ML-KEM

The Security Protocol and Data Model (SPDM) specification, developed by the Distributed Management Task Force (DMTF), is a standardized protocol designed to enable secure communication, device authentication, and attestation across a wide range of platforms and transport layers—ensuring a Zero Trust Security Environment.

SPDM facilitates encrypted and authenticated communication between components—similar in function to TLS 1.3—but is optimized for embedded and firmware-level environments.

It supports mutual authentication, key exchange, and session confidentiality, making it ideal for chip-to-chip and device-to-host interactions.

A key feature of SPDM is its ability to verify the identity and integrity of hardware components through mechanisms such as firmware attestation, where devices cryptographically prove their firmware state to a verifier.

With the release of SPDM 1.4, the protocol now includes support for post-quantum cryptographic algorithms like ML-KEM and ML-DSA, ensuring resilience against future quantum threats.

Lattice PQC enabled devices are fully equipped to support SPDM-compatible systems, offering the necessary cryptographic primitives—including ML-KEM, ML-DSA, AES-GCM—and transport support via MCTP, enabling secure integration of all platform components.

DICE in Lattice Devices

The Device Identifier Composition Engine (DICE) is a security specification developed by the Trusted Computing Group (TCG) to establish cryptographically strong, immutable identities for resource-constrained devices.

In Lattice devices, the loaded bitstream, its configuration, and a hardware-intrinsic secret are cryptographically combined to generate a unique identifier known as the Compound Device Identifier (CDI). This CDI reflects the device's current state and serves as the foundation for deriving a unique asymmetric key pair.

When this key pair is endorsed by the Lattice Certificate Authority during manufacturing, it results in a device-specific certificate. These DICE certificates can be used in conjunction with SPDM to establish secure communication between devices in a zero trust environment. Devices can share configuration data through signed evidence that can be traced back to an authentic Lattice device.

Additionally, system designers can leverage the capabilities of Lattice PQC-enabled devices to elevate their attestation infrastructure to a new level of security—one that is resilient against quantum attacks.

Platform Firmware Resiliency (PFR) in Lattice PQC-Enabled Devices

Platform Firmware Resiliency (PFR) is a security framework designed to protect, detect, and recover critical platform firmware—such as BIOS, bootloaders, and other low-level system components—from cyber threats, unauthorized modifications, and operational failures.

Lattice PQC-enabled devices are the first capable of implementing a PFR solution based on the guidelines outlined in NIST Special Publication 800-193, combined with the advanced cryptographic capabilities defined in CNSA 2.0.

As PQC algorithms continue to be developed across the industry, a hybrid approach—which combines classical and quantum-resistant methods—offers a practical and secure path forward. This model enables real-world testing of PQC while maintaining the reliability of well-established algorithms, thereby enhancing trust and easing adoption.

Lattice PQC-enabled devices are well-positioned to support this hybrid PFR model. They can combine classical algorithms like ECDSA with quantum-resistant options such as ML-DSA, LMS, and XMSS for firmware authentication. For attestation and secure channel services, combinations like ML-DSA/ML-KEM with ECDSA and AES-GCM can be employed.

This layered cryptographic approach ensures that if one algorithm is compromised—whether due to quantum advances or unforeseen vulnerabilities—the others continue to provide protection. This redundancy significantly strengthens overall system resilience.

Secure Manufacturing Using PQC Capabilities

Many of the security features described in this document rely on sensitive data provisioned into the device during manufacturing. This data may include cryptographic keys, configuration files, policy settings, or X.509 certificates used to endorse runtime keys.

However, manufacturing processes are often overlooked during security assessments, leaving this critical stage vulnerable to potential threats.

Lattice PQC-enabled devices, by contrast, begin their lifecycle with “Last Inch Secure” provisioning protocols in a protected test facility . Manufacturing HSMs fortified with post-quantum cryptographic technologies—such as the combination of ML-DSA and ML-KEM—ensure that sensitive provisioning data is delivered securely and remains protected against quantum-level attacks.

Closure

The threat posed by quantum computing is no longer theoretical—it is real and imminent, particularly due to “Harvest Now, Decrypt Later” attacks that exploit current cryptographic vulnerabilities.

In response, governments and organizations worldwide are actively driving the transition from classical to post-quantum public key cryptography to safeguard digital infrastructure.

Lattice’s PQC-enabled devices present a timely and robust solution to meet these evolving security requirements. With support for a broad spectrum of cryptographic algorithms and built-in crypto agility, these devices are well-positioned to adapt to future advancements in post-quantum cryptography.

Furthermore, the intrinsic flexibility of FPGAs enables the integration of advanced security services such as PFR and SPDM, leveraging existing primitives to build resilient architectures capable of withstanding quantum-era threats.

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.1 WP0047