Solution Brief

SECURING MODERN COMPLEX SYSTEMS WITH LATTICE FPGA-BASED ROOT OF TRUST SOLUTIONS

Achieve Cyber Resilience and Enable Compliance with Key CNSA, NIST and EU Regulations for Enhanced Security and Trust

Overview

Lattice FPGA solutions with advanced security features enable Hardware Root of Trust (HRoT) capabilities. These solutions come in a variety of form factors, supporting a wide range of use cases.

Lattice enables system level security with its hardware-based Root of Trust solutions, providing secure boot and ensuring security of FPGA bitstreams, firmware, software, and device configuration. This solution provides virtually instant detection against multiple types of attacks and compliance with multiple security standards including NIST 800-193 (Platform Firmware Resiliency) and the Trusted Computing Group's Device Identifier Composite Engine (DICE) Specification.

KEY CHALLENGES

- Modern systems cannot be secured with point solutions or by adding a single layer of security
- Organizations need a holistic approach to protect modern systems against cyber threats
- Security solutions must be updatable to stay ahead of evolving attacks
- Strong locking and tamper detection is needed to prevent malicious malware installations or code modifications

LATTICE SOLUTION

- Secure boot
- Platform Firmware Resilience (PFR)
- Device Identifier Composition Engine (DICE)
- Secure Enclave
- Cyber Resilience Act (CRA) compliance
- Regulatory compliance
- Identity, encryption, and authentication
- Agile Post-quantum cryptography
- Denial of Service attack resistance
- CNSA 1.0 and CNSA 2.0 compliance

Lattice Security Capabilities

Cybersecurity for modern devices cannot be achieved with point solutions or by adding a single layer of security. Security must be considered holistically, and Lattice supports a broad range of security features needed to protect devices against the latest cyber threats.

- HRoT, PFR, DICE
- Secure the Wire™: Mutually authenticated ORAN PCIe® & IEEE 1588, Crypto Bridge across protocols (AES-256)
- Hardware enabled security: crypto acceleration, flexible port lock control, secure key storage, PUF
- Anti-tamper capabilities
- Supply chain security
- Key provisioning
- On chip flash enabling recovery to known good image

These security features provide the foundation needed to achieve cyber resilience through an integrated, end-to-end approach to security.

Hardware Root of Trust

Cybersecurity starts at the device level with a Hardware Root of Trust. Lattice FPGAs provide market-leading HRoT capabilities with critical security features including:

- Unique hardware based device identity
- Secure storage of cryptographic keys
- Hardened cryptography
- Support for Post-quantum cryptography (PQC) algorithms
  - XMSS and LMS
  - ML-DSA (Dilithium) and ML-KEM (Kyber)
- Compliant with CNSA 2.0 requirements
- Secure dual boot with lockable onboard Flash
- Secure programming, authentication and encryption
- Anti-tamper protections and side-channel attack resistance (SCA) to protect against physical attacks
- Flexible lock control to ensure tightly controlled access to debug ports and other interfaces

Lattice Hardware Root of Trust Security Engine

BITSTREAM/IMAGE PROTECTIONS

- Confidentiality (AES256-GCM)
- Authentication (up to ECC 512/RSA4096)
- Strong side-channel attack (SCA) protections
- Algorithms validated against NIST CAVP
- SHA2/SHA3
- HMAC

KEY PROTECTIONS & UNIQUE IDENTIFIERS

- Physically Unclonable Function (PUF)
- Device root key protection via PUF
- Device + user key storage (w/ zeroize)
- Key Derivation Function (KDF) & Key Exchange
- Secure Unique ID for RoT/Attestation (e.g, DICE)
- Public Unique ID (Trace ID)

ANTI-TAMPER (AT) PROTECTIONS

- Voltage monitor & alarms
- Temperature monitor & alarms
- Fault Injection Attack (FIA) prevent & detect
- Test Port (e.g., JTAG) activity detect & block
- Penalties (zeroizations, secure lockdown, etc.)

USER ACCESS TO SECURITY FUNCTIONS

- Available post-configuration / post-boot via fabric
- Comprehensive API (modes, key lengths, etc.)
- Functions pre-qualified to reduce TTM
- Frees up fabric resources for user applications

+

RISC-V SOFT CPU SUBSYSTEM FEATURES:

- Secure FPGA config via Security Engine RoT
- Comprehen-sive API calls for user mode security

RANDOM NUMBER GENERATION (RNG)

- True random entropy source (TRNG)
- Determistic Random Bit Generator (DRBG)
- TRNG +DRBG Construction + Health Checker
- NIST SP 800-90A/B/C qualified

CRYPTO ALGORITHMS NIST CAVP VALIDATED

- RNG NIST SP 800-90A/B/C Qualification
- FIPS 140-3 Level 2 Certification Ready

Platform Root of Trust

Lattice provides market leading platform Root of Trust solutions with its Lattice Mach™ Advanced Secure Control FPGA families. The FPGA operates as the “first on, last off” component in a system and serves as the platform Root of Trust hardware within a complex system. With Lattice FPGAs, you can implement a Platform Firmware Resiliency (PFR) solution, as specified in NIST Special Publication 800-193, providing protection, detection, and recovery. See Figure 1.

Figure 1: Platform Firmware Resiliency (PFR) Solution with Lattice FPGAs

Protection
Ensure the integrity of platform firmware and critical data, ensuring the authenticity and integrity of firmware updates.

Detection
Detect when platform firmware and critical data have been corrupted or changed unexpectedly

Recovery
Restore platform firmware and critical data to their proper state when an unauthorized change is detected.

Cyber Resilience

Achieving cyber resilience requires security at the device, system, and supply chain level. This requires multiple layers of protection, which can only be achieved by implementing multiple security features to protect against sophisticated, multi-stage attacks.

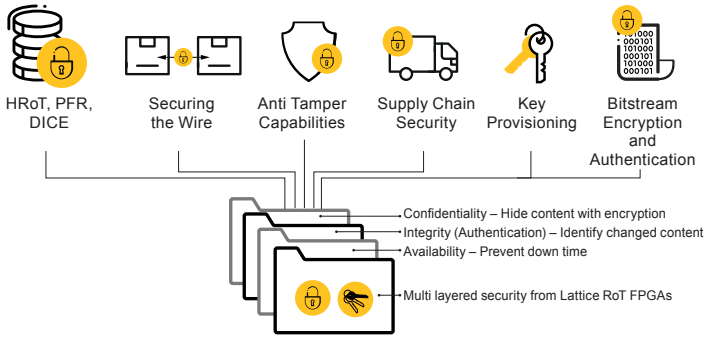
To achieve cyber resilience, security must be a driving factor in the design of the system from the earliest stages of the design cycle. Security is not a single feature or an afterthought, but a fundamental consideration in all aspects of the system and the product’s design.

Lattice’s family of security solutions enables OEMs to achieve high levels of security in their designs and to develop products meeting stringent regulatory requirements like the Cyber Resilience Act (CRA).

Flexible Security with FPGAs

FPGAs provide an ideal platform for addressing modern security concerns. Security standards and requirements continue to evolve. Hackers are constantly developing new attacks and searching for new vulnerabilities. To maintain pace with new standards and stay ahead of evolving attacks, security solutions must be updateable. Lattice FPGAs provide the flexibility required to develop cutting edge products and maintain the ability to adapt to new security threats. While these FPGAs can be updated to add security features or patch vulnerabilities, they can also be locked down to prevent malicious third parties from installing malware or making malicious code modifications. Thus providing a robust and cyber resilient solution for the whole life cycle of the product. Secure update process ensures all updates are validated and authenticated before they are accepted. See Figure 2.

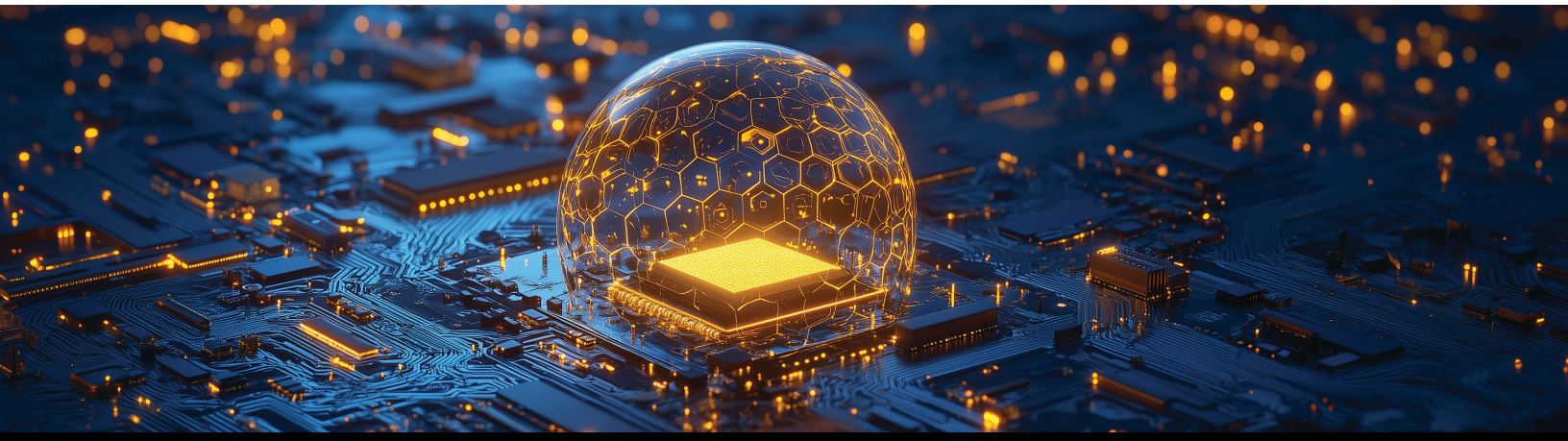
Figure 2: Lattice’s End-to-End Approach to Post-Quantum Cryptography



Lattice FPGA platforms enable trusted programmable security including the following capabilities:

- Trusted data for AI/ML applications
- Soft Baseboard Management Controller (BMC)
- FPGA based Trusted Platform Module (TPM)
- Caliptra

Lattice is continuing to invest in new security capabilities to meet emerging industry trends and cybersecurity regulations such as CRA and CNSA 2.0.



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 **sales@latticesemi.com**.