Lattice Sentry™ 5.0 PFR with PQC

Platform Firmware Resiliency Using Classical Cryptography and PQC

Problem:

Industry and the federal government are mandating a transition from classical cryptography to post-quantum cryptography (PQC) by 2030. PQC Platform Firmware Resiliency (PFR) requires image authentication, protection, and recovery that support CNSA 2.0-defined algorithms.

Solution:

The Lattice Sentry 5.0 PFR PQC solution is built using the MachXO5™ 55TDQ device. Sentry 5.0 supports self-authentication and external image authentication for BMC and Host CPU using either classical cryptography or PQC.

The solution executes the three pillars of PFR: detection, protection, and recovery functionality. External communication with BMC, CPU, SCM-CPLD, and HPM-CPLD devices is enabled via SMBus mailbox, I2C, I3C, LTPI, and SGPIO interfaces.

Features:

- **Detect:** Authenticate internal and external images using PQC-signed images with XMSS, LMS, or ML-DSA algorithms
- **Protect**: QSPI monitoring and filtering, and SMBus/I2C filtering
- **Recover**: Primary and backup image boot capability
- Two-layer key hierarchy with key revocation and up to 2,048 keys

