



Lattice Launches Industry-First PQC-Ready FPGA Family: MachXO5-NX TDQ

October 13, 2025

– Sets new standard for secure control FPGAs with full CNSA 2.0-compliant post-quantum cryptography, crypto-agility, and hardware root of trust for next-generation infrastructure –

HILLSBORO, Ore.--(BUSINESS WIRE)--Oct. 13, 2025-- [Lattice Semiconductor](#) (NASDAQ: LSCC), the low power programmable leader, today introduced the Lattice MachXO5™-NX TDQ family, the industry's first secure control FPGAs with full [Commercial National Security Algorithm \(CNSA\) 2.0](#)-compliant post-quantum cryptography (PQC) support. Built on the award-winning Lattice Nexus™ platform, MachXO5-NX TDQ FPGAs deliver unmatched security, reliability, and flexibility for Computing, Communications, Industrial, and Automotive applications as the threat of quantum-enabled cyberattacks rises.

"Quantum computing advances increase the urgency to adopt quantum-resistant security across every industry," said Esam Elashmawi, Chief Strategy and Marketing officer, Lattice Semiconductor. "With MachXO5-NX TDQ, Lattice is first to market with a secure control FPGA family that not only meets today's security mandates but also delivers crypto-agility and hardware root of trust to future-proof our customers' infrastructure against evolving threats."

The Lattice MachXO5-NX TDQ FPGA family equips customers with:

- **Full Suite of CNSA 2.0 Compliant PQC**
 - First and only complete CNSA 2.0 and National Institute of Standards and Technology (NIST)-approved PQC algorithms (LMS, XMSS, ML-DSA, ML-KEM, AES256-GCM, SHA2, SHA3, SHAKE) for robust protection against quantum threats
 - Authenticated and/or encrypted bitstream ensuring data integrity and protection against unauthorized access with ML-DSA, LMS, XMSS, AES256
 - Unique, patent pending crypto-agility with in-field algorithm update capability and anti-rollback version protection to enable ongoing alignment with evolving standards
 - Secure bitstream key management with revokable root keys and sophisticated key hierarchy for both PQC and classical keys
- **Advanced Cryptography**
 - Full complement of advanced symmetric and classical asymmetric cryptographic algorithms (AES-CBC/GCM 256 bit, ECDSA-384/521, SHA-384/512, RSA 3072/4096 bit) for bitstream and user data protection
 - Device Identifier Composition Engine (DICE), Security Protocol and Data Model (SPDM), and Lattice SupplyGuard™ capable, providing attestation and secure lifecycle/supply chain management for future-proof, end-to-end security
- **Hardware Root of Trust (RoT)**
 - Trusted single-chip boot with integrated flash
 - Unique device secret (UDS) ensuring distinct device identity
 - Integrated non-volatile configuration memory and user flash memory (UFM) with flexible partitioning and secure locking
 - Comprehensive locking control of programming interface (SPI, JTAG), providing complete protection
 - Side Channel Attack (SCA) resiliency and [NIST Cryptographic Algorithm Validation Program \(CAVP\)](#) compliant algorithms

Lattice also expanded its RoT-enabled Lattice MachXO5-NX device family with new MachXO5-NX TD devices that offer new density and package options. These new Lattice MachXO5-NX TDQ and MachXO5-NX TD FPGA devices are available and have shipped to industry-leading Communications and Compute customers, and are supported by the latest release of Lattice Radiant™ design software.

Experience Lattice PQC-Ready Innovation at OCP Global Summit

Lattice will showcase live demonstrations of its latest FPGA solutions including the MachXO5-NX TDQ for secure, AI-optimized datacenter infrastructure at the OCP Global Summit, taking place Oct. 14–16, 2025 at the San Jose Convention Center, San Jose, Calif. Visit Lattice at Booth #A23 to experience future-ready security, including CNSA 2.0-compliant PQC, intelligent connectivity, and power-efficient AI acceleration.

Supporting Resources

- For more information about Lattice MachXO5-NX TDQ, visit [product webpage](#), read the [launch blog](#), or download the white paper [here](#).
- For more information about Lattice's OCP Global Summit participation, read the [event announcement](#).
- For more information about Lattice, please visit <https://www.latticesemi.com>

About Lattice Semiconductor

Lattice Semiconductor (NASDAQ: LSCC) is the low power programmable leader. We solve customer problems across the network, from the Edge to the Cloud, in the growing Communications, Computing, Industrial, Automotive, and Consumer markets. Our technology, long-standing relationships, and commitment to world-class support let our customers quickly and easily unleash their innovation to create a smart, secure, and connected world.

For more information about Lattice, please visit www.latticesemi.com. You can also follow us via [LinkedIn](#), [X](#), [Facebook](#), [YouTube](#), [WeChat](#), or [Weibo](#).

Lattice Semiconductor Corporation, Lattice Semiconductor (& design), and specific product designations are either registered trademarks or trademarks of Lattice Semiconductor Corporation or its subsidiaries in the United States and/or other countries. The use of the word "partner" does not imply a legal partnership between Lattice and any other entity.

GENERAL NOTICE: Other product names used in this publication are for identification purposes only and may be trademarks of their respective holders.

View source version on [businesswire.com](https://www.businesswire.com/news/home/20251013522544/en/): <https://www.businesswire.com/news/home/20251013522544/en/>

MEDIA CONTACT:

Sophia Hong
Lattice Semiconductor
503-268-8786
Sophia.Hong@latticesemi.com

INVESTOR CONTACT:

Rick Muscha
Lattice Semiconductor
408-826-6000
Rick.Muscha@latticesemi.com

Source: Lattice Semiconductor