# Lattice Introduces New Secure Control FPGA Family with Advanced Crypto-Agility and Hardware Root of Trust

June 26, 2024

*—New Nexus-based MachXO5D-NX FPGAs and Sentry solution stack optimized for evolving security landscape with industry-standard compliant, crypto-agile, and class-leading RoT features —*

HILLSBORO, Ore.--(BUSINESS WIRE)--Jun. 26, 2024-- Lattice Semiconductor (NASDAQ: LSCC), the low power programmable leader, today expanded its leadership in security-focused hardware and software with the launch of two new solutions to address customer challenges around increasing threats to system security. The company announced the Lattice MachXO5D™-NX family of advanced secure control FPGAs, offering crypto-agile algorithms, hardware root of trust features with integrated flash, and fail-safe remote field updates for reliable and secure product lifecycle management. In addition, Lattice launched the latest version of the Lattice Sentry™ solution stack, featuring new capabilities to equip customers with customizable FPGA-based platform firmware resiliency (PFR) solutions supporting the new MachXO5D-NX family.

“At Lattice, we’re focused on addressing our customers’ evolving security needs and helping them stay ahead of accelerating cyberthreats to system data and infrastructure,” said Dan Mansur, Corporate Vice President of Product Marketing at Lattice Semiconductor. “Crypto-agile security based on hardware root of trust devices is increasingly fundamental in this digital age, and we’re excited to further expand our product portfolio with the MachXO5D-NX FPGA family and the latest Sentry solution stack release.”

Key features and performance highlights of the new low power Lattice MachXO5D-NX FPGAs based on the Lattice Nexus™ FPGA platform include:

- **Advanced Cryptographic Agility**
  - Security algorithms specified by the Commercial National Security Algorithm (CNSA) Suite for bitstream and user data protection, including AES-256, ECDSA-384/521, SHA2-256,384/512, and RSA 3072/4096
- **Hardware Root of Trust**
  - Immutable boot ROM, enabling secure-dual boot with integrated flash for fail safe updates
  - Unique Device Secret (UDS) protecting device identity
  - Side channel attack (SCA) resiliency
  - Integrated non-volatile configuration memory and up to 57 Mb of configurable user flash memory (UFM) for user data storage and management
  - Fully configurable programming interface (SPI, JTAG) locking control preventing advanced external attacks
- **Reliable and Secure Product Lifecycle**
  - Secure on-chip multi-boot with bitstream encryption and authentication, enabling fail-safe remote field updates
  - Anti-rollback version protection and revocable root keys, protecting against malicious bitstream attacks and ensuring design integrity
  - DICE and Lattice SupplyGuard™ capability for secure product lifecycle and supply chain management

Enabling NIST SP800-193 compliant PFR solution development for Communications, Computing, Industrial, and Automotive applications, the Lattice Sentry (v 4.0) solution stack now includes:

- Multiple QSPI/SPI monitoring with I2C peripheral attack protection demonstration
- SPDM and MCTP support for efficient platform management and secure and seamless server operations
- A new design workspace template reference design that enables PFR 4.0 solution with I3C support, newer crypto algorithms (ECC384/512), and full DC-SCM compatibility
- Expanded plug-and-play design tools and reference designs with workspace template, and policy, provisioning, and manifest generator

The new MachXO5D-NX FPGA family and the latest Sentry solution stack are supported by the latest releases of award-winning Lattice Radiant™ and Lattice Propel™ design software.

For more information about the technologies mentioned above, please visit:

- Lattice MachXO5D-NX
- Lattice Sentry Solution Stack

- Lattice Nexus FPGA platform
- Lattice Radiant Design Software
- Lattice Propel Design Environment
- Lattice SupplyGuard

**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, Twitter, Facebook, YouTube, WeChat, or Weibo.



View source version on businesswire.com: https://www.businesswire.com/news/home/20240626638418/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