Lattice + Quside Verified Entropy Module

Post-Quantum-Safe Root of Trust on Lattice MachXO5™-NX — A Complete FPGA

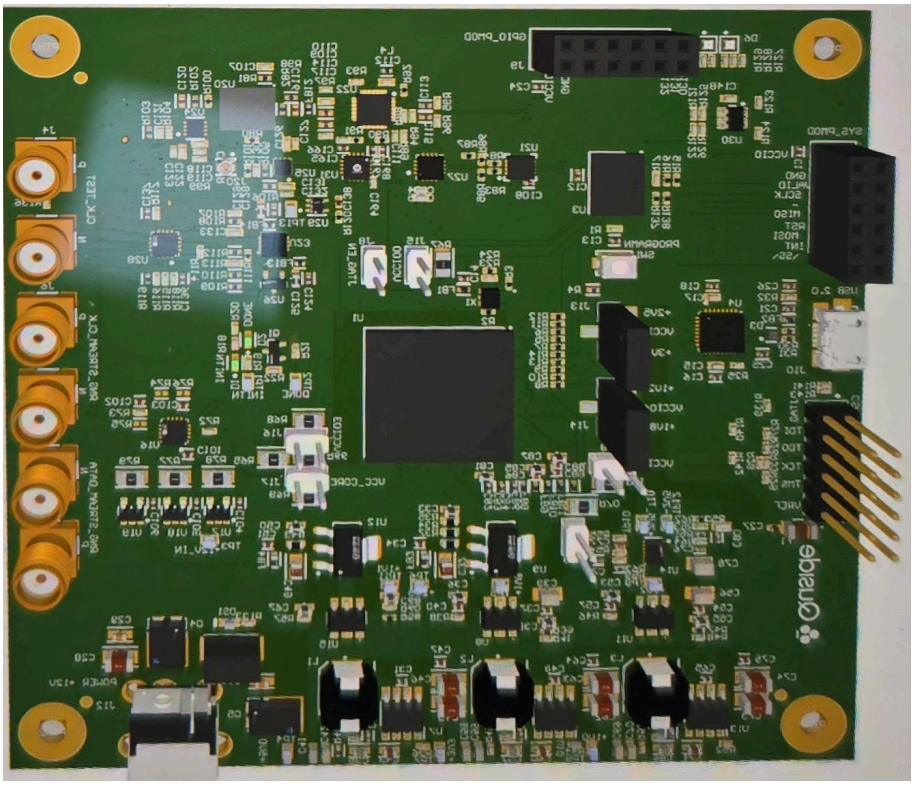
Solution:

Lattice and Quside deliver a verified entropy module — a post-quantum-safe root of trust inside a single Lattice MachXO5-NX (LFMXO5-55TDQ) FPGA, shipped as a complete development kit. The solution is designed to demonstrate entropy quality, which is verified at runtime.

- A root of trust inside the FPGA: entropy source, conditioning, and health tests, with no dedicated security chip on the BOM
- Post-quantum-safe, built against the NIST SP 800-90B and BSI AIS-31 frameworks
- Entropy quality measured continuously at runtime and reported to the host, so the platform can act on a degraded root of trust

Features:

- Complete development kit: Onyx PQC Evaluation Board, Lattice MachXO5-NX, and verified entropy IP
- Quantum entropy source, conditioning, and health tests in FPGA fabric, up to 50 Mbps
- SPI host interface for BMC and platform-controller integration



latticesemi.com