Mach-N2 CNSA 2.0 PQC Demo

ML-DSA, ML-KEM and AES on Lattice Mach-N2

Problem:

- The transition to post-quantum cryptography (PQC) is driven by the risk that future quantum computers can compromise today's classic cryptography.
- CNSA 2.0 mandates migration to quantum-resistant algorithms, with firmware signing transitioning to PQC by 2030, creating an urgent need for PQC-enabled secure boot, attestation, and firmware update solutions.

Solution:

- **Hardware PQC suite:** The Lattice Mach-N2 ROT FPGA implements the CNSA 2.0 quantum-resistant suite in hardware, demonstrated with NIST test vectors.
- **Complete algorithm coverage:** It supports ML-DSA (FIPS 204) key generation, signing, and verification; ML-KEM (FIPS 203) key generation, encapsulation, and decapsulation; and AES-256-GCM encryption and decryption.
- **Future-proof and compliant:** It protects the root of trust against quantum attacks using NIST-standardized algorithms aligned with CNSA 2.0.
- **Integrated and efficient:** Signature, key establishment, and encryption are combined in one compact, low-power, crypto-agile device.

