Redefining Security by Enabling Post-Quantum Cryptography on Agilex 5 System on Module

The rapid development of quantum computing is revolutionizing the way we look at security. As quantum computers get more advanced, the encryption we rely on today, like RSA and ECC, will not be strong enough to keep the data safe. This shift is pushing the need for new, more secure methods. That's where Post-Quantum Cryptography (PQC) comes in, designed to protect sensitive information even against powerful quantum attacks.

With the belief that "systems designed today must support post-quantum cryptography tomorrow," iWave Global, a leader in embedded systems, has partnered with Xiphera, a Finland-based company known for its hardware-based security IP cores, to deliver quantum-resistant security on the Agilex™ 5 System on Module (SoM) powered by Altera.

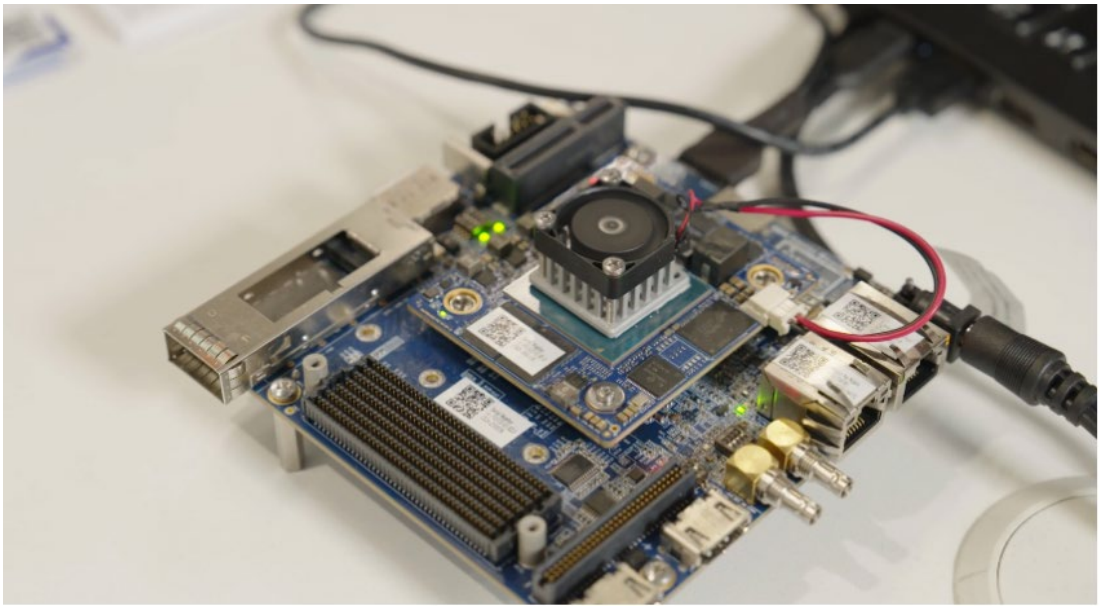
Xiphera's xQlave® product family offers quantum-secure cryptography, consisting of secure and efficient implementations of Post-Quantum Cryptography (PQC) – algorithms that are designed to withstand attacks made by quantum computers. The xQlave® product family includes a portfolio of quantum-secure key exchange (ML-KEM) and digital signatures (ML-DSA) that are based on the PQC algorithms standardized by the U.S. National Institute of Standards and Technology (NIST).

Implementation: Xiphera PQC on Agilex™ 5 System on Module

Post-Quantum Cryptography (PQC) has been successfully integrated into Agilex™ 5 System on Module, showcasing the platform's capability to handle next-generation cryptographic demands. Leveraging Xiphera's xQlave® IP cores for ML-KEM and ML-DSA, the Agilex 5 SoM demonstrates real-time, quantum-secure key exchange and digital signature operations directly in FPGA hardware. This integration highlights the SoM's ability to deliver low-latency, side-channel-resistant cryptography while remaining flexible for evolving PQC standards.

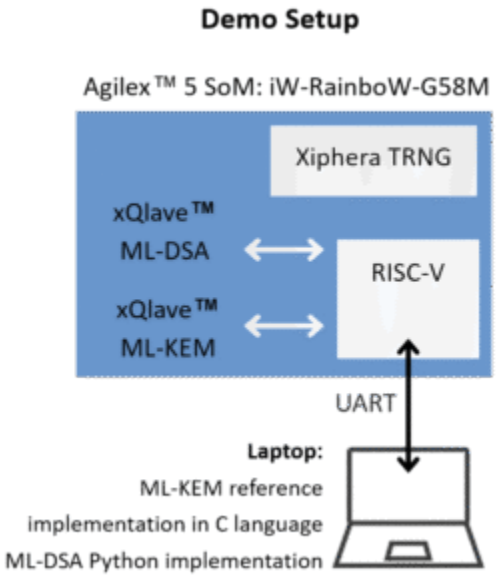
Xiphera ML-KEM (Kyber) & ML-DSA (Dilithium) IP core:

- Compliant with NIST specifications for ML-KEM
- Protected against timing-based side-channel attacks
- Computes thousands of operations per second in a typical FPGA implementation
- Seamless integration into embedded systems via standard interfaces



Demo Features:

- Demo includes a Linux laptop and an Altera Agilex™ 5 based iWave FPGA board.
- FPGA includes Xiphera ML-KEM, ML-DSA and TRNG IP cores, as well as a soft-core RISC-V processor to handle communications.
- Xiphera IP cores on an FPGA operate cryptographic calculations (KEM & DSA) against a laptop software application.
- FPGA part number: A5ED065BB32AE5SR0



Why Agilex™ 5 SoM (iW-RainboW-G58M) is the Ideal Platform for PQC?

- Agilex 5 E-Series family with B32A Package
- Bit 2GB LDDR4 for HPS and 2 x 32Bit 2GB LDDR4 for FPGA
- 16GB eMMC (Expandable) and 1Gb QSPI Configuration flash
- 24 x transceivers up to 28Gbps
- Up to 656,080 Logic cells
- 2.5G Ethernet PHY Transceiver
- Rich connectivity: PCIe Gen4, DDR4, Ethernet, and more
- Security features: Secure boot, hardware root of trust, and encrypted bitstreams

The System on Module (SoM) is built in a compact form factor of 60mm x 70mm and is compatible with the Intel Agilex™ 5 FPGA and SoC E-Series family and B32A package in two device variants:

- Group A: A5E 065A/052A/043A/028A/013A SoC FPGA
- Group B: A5E 065B/052B/043B/028B/013B/008B SoC FPGA

The Agilex™ 5 FPGA features an asymmetric applications processor system consisting of dual Arm Cortex-A76 cores and dual Cortex-A55 cores that optimise the performance and power efficiency of their workloads. Integrated with an enhanced DSP with AI Tensor block, the Agilex™ 5 offers advanced connectivity features, DisplayPort and HDMI Output.

Real-World Use Cases for PQC on Agilex™ 5 SoM

- Defence & Aerospace: Secure communication and control systems against future quantum threats.
- Industrial Automation: Protect edge devices and firmware updates in smart factories.
- Telecommunications: Future-proof 5G/6G networks and secure large-scale data transfers.
- Automotive: Enable secure V2X communication and OTA updates in connected vehicles.
- Healthcare: Safeguard patient data and medical devices with long-term encryption.
- Finance: Protect digital transactions and smart cards from future cyber risks.

The partnership between iWave and Xiphera brings to life a powerful demonstration of post-quantum security in action. By implementing Xiphera's xQlave™ ML-KEM and ML-DSA cores on the iWave Agilex™ 5 SoM, developers and OEMs gain access to hardware-accelerated, quantum-secure communication today.

With its powerful FPGA fabric, reconfigurable architecture, and robust security features, the Agilex 5 SoM enables seamless integration of post-quantum cryptography into real-world embedded systems. It stands as a versatile and scalable platform that not only meets today's security needs but is also engineered to withstand the evolving threats of the quantum era.

Related Part Numbers:

iG58D-E065B5-4L002G-E032G-CBA-ES
iG58M-E065B5-4L002G-E032G-EBA-ES