宏太科技 AVANT TECHNOLOGY

Avant News Release

# EnSilica cuts post-quantum cryptography (PQC) silicon area with three-in-one IP block

**Oxford, UK, July 21st, 2025:**

EnSilica, a leading maker of mixed-signal ASICs (Application Specific Integrated Circuits), has developed a combined hardware IP block supporting the full CRYSTALS post-quantum cryptography (PQC) suite, saving silicon area, power and cost. The licensable eSi-CRYSTALS PQC accelerator runs Dilithium (FIPS-204), Kyber (FIPS-203) and SHA-3 (FIPS-202) algorithms, which previously required three separate IP blocks.

In August 2024, the US National Institute of Standards and Technology (NIST) released the first three finalised PQC standards, with additional algorithms announced or in draft stages. Dilithium, Kyber, and SHA-3 are advanced cryptographic algorithms designed to secure digital systems against both classical and quantum computing threats.

Dilithium is used for digital signatures, providing authentication and data integrity, while Kyber is a key encapsulation mechanism that enables secure key exchange. Integrated into the block is also a hardware-optimised implementation of the cryptographic SHA-3 hash function that creates a digital fingerprint of data allowing for robust integrity verification.

Together, these algorithms form the foundation for quantum-resistant security in modern systems, ensuring long-term protection of sensitive information.

## Industry Insight

> **Ian Lankshear, CEO of EnSilica**, commented:
>
> *“The emerging PQC threat is not just theoretical. Security analysts warn that adversaries can already capture encrypted data today, with the intention of decrypting it in the future when quantum capabilities become available, a tactic known as ‘harvest now, decrypt later’.”*

> “That’s why EnSilica’s PQC offering delivers future-proof hardware protection at the silicon level with minimal silicon area for mature and advanced technology nodes.”

EnSilica previously announced separate Dilithium, Kyber and SHA-3 algorithms licensed for use by a major semiconductor company for a 5 nm networking ASIC. The new IP offers a more compact implementation than separate cores.

EnSilica also has a full suite of classical cryptographic accelerators including ECC, ECDSA, RSA, AES, ChaCha20, and Poly1305. In addition, the company offers a NIST-compliant true random number generator (TRNG).

## About EnSilica

EnSilica is a leading fabless design house focused on custom ASIC design and supply for OEMs and system houses, as well as IC design services for companies with their own design teams.

The company has world-class expertise in supplying custom RF, mmWave, mixed-signal and digital ICs to its international customers in the automotive, industrial, healthcare and communications markets.

The company also offers a broad portfolio of core IP covering cryptography, radar, and communications systems. EnSilica has a track record in delivering high-quality solutions to demanding industry standards.

The company is headquartered near Oxford, UK and has design centres across the UK and in Bangalore, India, and Porto Alegre and Campinas, Brazil.

**More information:** www.ensilica.com

## About Avant Technology

Avant Technology Inc., founded in 1996 in Hsinchu, Taiwan, is a premier distributor of EDA tools and IP solutions across Asia. We connect clients with cutting-edge technology to fuel innovation and competitive advantage.

**Learn more:** http://www.avant-tek.com/
**Contact Us:** sales@avant-tek.com