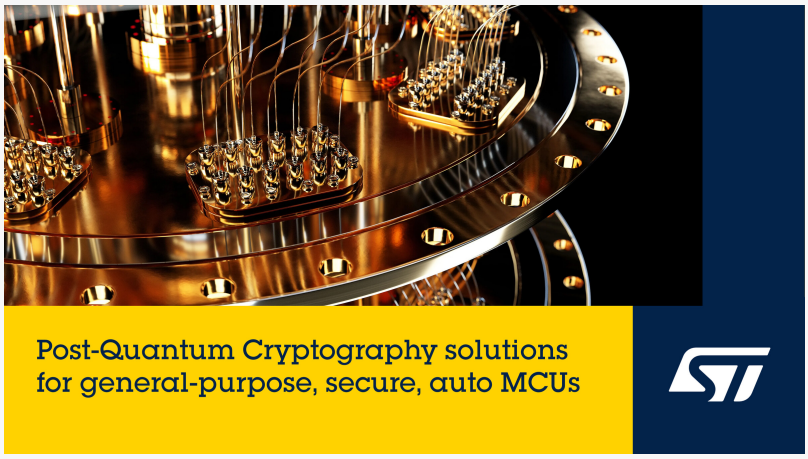
STMicroelectronics reveals solutions for post-quantum cryptography, bringing quantum resistance to embedded systems

New post-quantum cryptographic algorithms integrated in general-purpose MCUs, secure microcontrollers, and automotive microcontrollers



ST solutions for PQC

GENEVA, SWITZERLAND, March 10, 2025 /EINPresswire.com/ -- STMicroelectronics has introduced hardware cryptographic accelerators and associated software libraries for general-purpose and secure microcontrollers, ready for future generations of embedded systems to resist quantum attacks.

As quantum computers are beginning to outperform classical computers in research trials, industries are starting to prepare now for their use to become mainstream. New government specifications are emerging to standardize Post-Quantum Cryptography (PQC), leveraging new techniques based on mathematical problems that are difficult for quantum computers to solve. The PQC standards published to-date use the award-winning Keccak algorithm -- a highly resistant hash algorithm which has been invented by ST experts.

Solutions compliant with these standards are needed now, so that product developers can build-in protection according to current best practice and continue to strengthen resistance as the state of the art evolves. ST's new solutions are available for STM32 developers in the X-CUBE-PQC software library, and for Stellar automotive microcontrollers that contain the SHA-3 hardware accelerator. There are also new software libraries and hardware IPs for secure microcontrollers, targeting Common Criteria and FIPS 140-3 and supporting ML-KEM, ML-DSA and XMSS/LMS PQC algorithms.

"Quantum computers are expected to bring advantages to activities such as finance, scientific research, earth observation, and many more. On the other hand, they could overpower some current types of cryptography in equipment used on a daily basis," said Jacques Fournier,

Director of Security Platform at STMicroelectronics. “ST is the first to provide quantum resistant features across all its product ranges, for all customers, for all required levels of security.”

The post-quantum cryptographic assets ST is announcing today are ready to use, empowering customers to bring quantum resistance to critical security features of their products like firmware update, secure boot, and authentication mechanisms.

ST’s Jacques Fournier will address the embedded world Exhibitor Forum in Nuremberg on March 12, 2025. Visitors can discuss the latest quantum-resistant algorithms with the company’s security experts and see related demonstrations at the ST booth, 4A-148, during the event.

For more information on ST’s efforts in PQC, please click here.

For more information on ST’s presence at embedded world 2025, click here.

Alexander Jurman
STMicroelectronics
Alexander.Jurman@st.com
