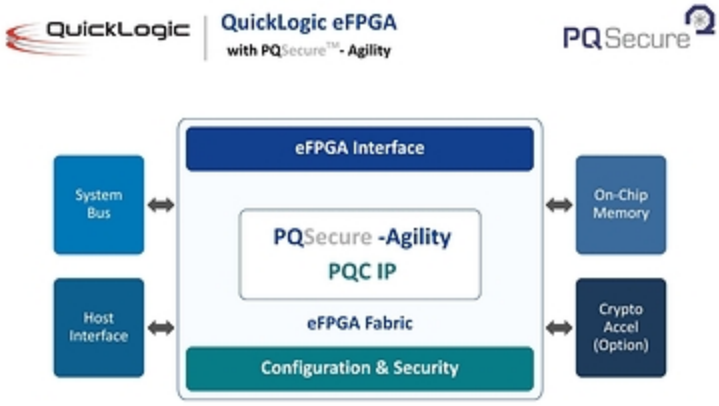
July 16, 2026

QuickLogic and PQSecure Enable Reprogrammable Post-Quantum Cryptography for SoCs

PQSecure IP efficiently maps into QuickLogic eFPGA fabric, delivering field-upgradeable security without costly silicon re-spins.

SAN JOSE, Calif., July 16, 2026 /PRNewswire/ -- QuickLogic® Corporation (NASDAQ: QUIK), a developer of embedded FPGA (eFPGA) Hard IP, Strategic Radiation Hardened and Antifuse FPGAs, and ruggedized programmable logic solutions, today announced results of a joint technical collaboration with PQSecure™ Technologies demonstrating that PQSecure's CRYSTAL-1000C post-quantum cryptographic IP core can be efficiently implemented as a reprogrammable function within SoCs using QuickLogic's eFPGA Hard IP fabric.



The trade study implemented CRYSTAL-1000C, targeting NIST-finalized standards FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA), on QuickLogic eFPGA Hard IP built for the Intel 18A process node. The PQSecure core was successfully placed and routed within eFPGA IP cores already used by QuickLogic customers in their ASICs, with sufficient performance for most applications and substantial capacity headroom.

PQSecure's CRYSTALS line is highly customizable to a broad range of use cases. SoC designers can use QuickLogic's Aurora programming tools to generate a project-specific resource report and determine the optimal eFPGA configuration for their crypto-agile security needs. SoC designers can right-size the eFPGA fabric for area and power efficiency or use the remaining resources to support higher-performance configurations and side-channel countermeasures such as masking and hiding.

The post-quantum migration is urgent: NIST's transition timeline deprecates classical algorithms by 2030 and mandates completion by 2035, while the "harvest-now, decrypt-

later" threat requires action today. Fixed-silicon cryptographic engines cannot adapt without costly re-spins. A recent study by Markets and Markets Research indicates that the global post-quantum cryptography (PQC) market is projected to grow from $420M in 2025 to over $2.8B in 2030.

With QuickLogic's eFPGA Hard IP, ASICs/SoCs can update their cryptographic engine in the field by loading a new bitstream – swapping algorithm parameter sets, running hybrid classical and post-quantum modes during transition, or patching side-channel vulnerabilities without new silicon. QuickLogic's Australis IP Generator produces customer-specific eFPGA Hard IP at leading process nodes as silicon-proven, GDSII-level blocks, delivering superior PPA versus soft eFPGA IP alternatives.

"This collaboration demonstrates the perfect use case for eFPGA Hard IP," said Trey Peterson, Field Applications Engineer at QuickLogic. "The post-quantum cryptography transition is an evolving process, not a single event. SoC designers who hard-wire their security engines today face costly, avoidable re-spins. We've proven that a reprogrammable solution works seamlessly today while leaving the flexibility to adapt tomorrow."

"PQSecure's CRYSTAL-1000C-SCA delivers hardware-speed and side-channel protected post-quantum security for resource-constrained platforms," said Luke Beckwith, Senior Hardware Engineer at PQSecure Technologies. "Our customers need to know their devices will remain secure a decade from now. Pairing our IP with QuickLogic's reconfigurable fabric future-proofs their hardware without requiring a new tape-out every time the threat landscape evolves."

A summary of the trade study, including target configuration specifications and architectural analysis, is available at www.quicklogic.com/pqsecure-partnership and www.pqsecurity.com.

Detailed performance and resource-utilization data is available to qualified customers under NDA. Engineers and SoC designers evaluating eFPGA-based post-quantum security solutions are encouraged to contact QuickLogic's technical sales team.

About QuickLogic

QuickLogic is a fabless semiconductor company specializing in embedded FPGA (eFPGA) Hard IP, Strategic Radiation Hardened and Antifuse FPGAs, and ruggedized programmable logic solutions. QuickLogic's unique approach combines cutting-edge technology with open-source tools to deliver highly customizable low-power solutions for aerospace and defense, industrial, computing, and consumer markets. For more information, visit www.quicklogic.com.

About PQSecure Technologies

PQSecure Technologies is a quantum-safe cryptography company focused on delivering production-grade, low-resource post-quantum cryptographic IP for SoC, ASIC, and embedded platforms. Its PQSecure-CRYSTALS product line implements ML-KEM (FIPS 203) and ML-DSA (FIPS 204) with optional side-channel and fault-attack countermeasures, in profiles from ultra-compact to high-performance. For more information, visit www.pqsecurity.com.

QuickLogic and logo are registered trademarks of QuickLogic. All other trademarks are the property of their respective holders and should be treated as such.

View original content to download multimedia:https://www.prnewswire.com/news-releases/quicklogic-and-pqsecure-enable-reprogrammable-post-quantum-cryptography-for-socs-302827173.html

SOURCE QuickLogic Corporation