September 19, 2023

Securing the Future: QuickLogic and Xiphera Partner to Pioneer Post-Quantum Cryptography on eFPGAs

SAN JOSE, Calif., Sept. 19, 2023 /PRNewswire/ -- QuickLogic Corporation (NASDAQ: QUIK), a developer of embedded FPGA (eFPGA) IP, ruggedized FPGAs and Endpoint AI/ML solutions, today announced a partnership with Xiphera, a provider of hardware-based cryptographic security solutions, including Post-Quantum Cryptography (PQC), to implement Xiphera's xQlave™ quantum-secure cryptographic IP cores on QuickLogic's eFPGA architecture. This partnership provides architects with a path towards securing their assets against the quantum threat, enabling them to stay one step ahead in the evolving landscape of cyber threats.

With the rapid development of quantum computers and the increasing threat they pose to information and network security, the need for robust cybersecurity measures has become more crucial than ever. Xiphera answers the quantum-threat with its xQlave™ family of PQC IP cores. The family includes ML-KEM (Kyber) and ML-DSA(Dilithium) – primary PQC algorithms in the PQC standard draft of the National Institute of Standards and Technology (NIST) – with logic-only implementations. Together, these IP cores provide quantum-secure key exchange, digital signature and authentication.

eFPGA technology offers two key benefits to implementing hardware security – distributed on-chip programmability, and the ability to parallelize intensive algorithmic computation requirements. This enables the eFPGA IP cores to offload heavy cryptographic operations from processor/software implementations, resulting in superior boot up and key calculation times. Furthermore, keys and secrets can be isolated from the rest of the system providing secure access only to trusted components. eFPGA technology also enables so-called crypto agility, which is the ability to update underlaying cryptographic algorithms and protocols, even after an SoC/ASIC has already been deployed into the field.

QuickLogic's eFPGA IP is generated using the Australis™ IP generator, which supports any foundry and any process geometry while at the same time having the ability to create customized eFPGA IP that meets customers' PPA requirements and provides the ideal hardware platform for post-quantum cryptographic algorithms. Combining Xiphera's xQlave™ PQC solutions with traditional cryptographic algorithms (ECC or RSA) into a hybrid scheme enables a future-proof secure system on new and already existing eFPGA platforms.

Benefits of the Joint Solution:

- **Data Protection:** Implementing xQlave™ ML-KEM (Kyber) on QuickLogic's eFPGA architecture reinforces product security architecture, ensuring data protection against future threats.
- **Enhanced Performance**: Hardware acceleration through QuickLogic's eFPGA architecture significantly optimizes the performance of Xiphera's xQlave™ family's ML-KEM (Kyber) and ML-DSA (Dilithium) IP cores.
- **Secure Storage:** The secluded block RAMs of the QuickLogic eFPGA architecture enable secure storage of secrets, without allowing privileged upper system components to access them.
- **Future Compatibility:** The implementation allows for easy upgrades to support the final NIST PQC standards when available, ensuring mission-critical systems remain secure against quantum threats.

"This partnership allows us to leverage the power of hardware acceleration and quantum-secure algorithms to deliver enhanced data protection and performance for our customers," said Mao Wang, senior director of product marketing at QuickLogic.

"With the rise of quantum computing, and government mandates to protect critical infrastructures against the threat posed by it, the time to address post-quantum cryptography in hardware security design is now. Xiphera's standards-based PQC IP combined with the design flexibility of QuickLogic's eFPGA platform enables solution designers to cost-effectively meet the rapidly evolving market demands for quantum-resilience," said Tommi Lampila, director of business development at Xiphera.

Availability
The QuickLogic and Xiphera solution for post-quantum cryptography is available now. Customers can contact QuickLogic at info@quicklogic.com or Xiphera at info@xiphera.com for more information.

Webinar – September 20 at 10 AM PT

Join us to learn more about the future of data protection with Xiphera's groundbreaking Post-Quantum Cryptography and QuickLogic's cutting-edge eFPGA technology. Register at https://us02web.zoom.us/webinar/register/9316950788331/WN_N8vkBfVxQ5qRhDkxVsDeWC

About Xiphera
Xiphera Ltd. is a Finnish company designing hardware-based security solutions using standardised cryptographic algorithms. We have strong cryptographic expertise, extensive experience in system design, and deep knowledge on reprogrammable logic, enabling us to protect our customers' critical information and assets. Xiphera's product portfolio consists of

secure and efficient cryptographic Intellectual Property (IP) cores, designed for Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). Our widely applicable solutions for various end markets offer our customers peace of mind in a dangerous world.

About QuickLogic

QuickLogic Corporation (NASDAQ: QUIK) is a fabless semiconductor company that develops low power, multi-core semiconductor platforms and Intellectual Property (IP) for Artificial Intelligence (AI), voice and sensor processing. The solutions include embedded FPGA IP (eFPGA) for hardware acceleration and pre-processing, and heterogeneous multi-core SoCs that integrate eFPGA with other processors and peripherals. The Analytics Toolkit from our recently acquired wholly-owned subsidiary, SensiML Corporation, completes the end-to-end solution with accurate sensor algorithms using AI technology. The full range of platforms, software tools and eFPGA IP enables the practical and efficient adoption of AI, voice, and sensor processing across mobile, wearable, hearable, consumer, industrial, edge and endpoint IoT. For more information, visit www.quicklogic.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/securing-the-future-quicklogic-and-xiphera-partner-to-pioneer-post-quantum-cryptography-on-efpgas-301931699.html

SOURCE QuickLogic Corporation