SECURE RF
Securing the Internet of Things

News Release

SecureRF's Walnut Digital Signature Algorithm Accepted by NIST for Evaluation as a Quantum-Resistant Cryptography Standard

Shelton, CT, January 22, 2018 – SecureRF Corporation, a leading provider of quantum-resistant security tools for low-resource processors powering the Internet of Things (IoT), has announced that its Walnut Digital Signature Algorithm™ (WalnutDSA™) has been accepted by the US Commerce Department's National Institute of Standards and Technology (NIST) for evaluation in their post-quantum standardization project. NIST's collaborative evaluation is a planned three-to-five-year process to identify quantum-resistant security methods to address the security threat that will come with quantum computing.

In recent years, public and private organizations have made significant advancements in quantum computing technology, and this has started the security world down a path to a time when quantum computers will be used to break classical cryptographic protocols, such as ECC and RSA, and leave billions of processor-based devices vulnerable. Based on Group Theoretic Cryptography methods, WalnutDSA is a fast, future-proof, ultra-low-energy solution that provides authentication, integrity, and nonrepudiation for even the smallest 8-bit processors that power the IoT.

"With the arrival of larger quantum computers becoming more imminent, it is important to begin looking at how we address security in the IoT. NIST is taking a collaborative leadership role in charting this path, and we are excited to have met the initial screening requirement to now participate in this process evaluation," said Louis Parks, CEO of SecureRF. "Using WalnutDSA, our semiconductor and processor partners are looking to address authentication and data protection for the automotive, medical, industrial, consumer, payments, and government markets. These markets will need to address a post-quantum world and we are focused on delivering the necessary solutions."

NIST expects to perform multiple rounds of evaluation over a period of three to five years on all of the methods submitted, and it will periodically post updates on its Post-Quantum Cryptography webpage. While the NIST evaluation process will take years, SecureRF's Group Theoretic-based, quantum-resistant security solutions are available now for implementation in both software and hardware for a wide variety of 8-, 16-, and 32-bit processors. To request SecureRF's free IoT Embedded Security SDK, sign up online, call 1-203-227-3151, or email info@securerf.com.

# # #

About SecureRF

SecureRF Corporation (securerf.com) develops and licenses quantum-resistant, public-key security tools for low-resource processors powering the Internet of Things (IoT). The company's authentication and data protection solutions are highly efficient when compared to techniques

like ECC and RSA. SecureRF delivers ultra-low-energy, fast, and small footprint solutions ideally suited for 32-bit, 16-bit, and even 8-bit devices like the ARM Cortex M0/M3 and RISC-V processors. SecureRF security solutions are used to address wireless sensors, NFC, Bluetooth, and RFID tags as well as embedded platforms including FPGAs, microcontrollers, and ASICs. Software Development Kits, RTL, and tools are available for a wide range of environments.

# # #

Company Contact:
C. J. Abate
Marketing@SecureRF.com
+1 203-227-3151