News Release

SECURERF PAPER ON QUANTUM-RESISTANT DIGITAL SIGNATURE ALGORITHM ACCEPTED FOR NIST LIGHTWEIGHT CRYPTOGRAPHY WORKSHOP

Theoretical foundation of WalnutDSA™ and benchmarks vs ECC and RSA on constrained devices commonly used in the IoT to be presented

Shelton, CT – October 17, 2016. SecureRF, a leading provider of quantum-resistant security solutions for the Internet of Things (IoT), will be presenting its paper, "Walnut Digital Signature Algorithm: A lightweight, quantum-resistant signature scheme for use in passive, low-power, and IoT devices" at the NIST Lightweight Cryptographic Workshop 2016 being held October 17 – 18, 2016 at NIST headquarters in Gaithersburg, MD.

NIST is currently developing a report on lightweight cryptography in support of its decision to create a portfolio of dedicated lightweight algorithms through an open process similar to the selection of modes of operation of block ciphers.

Derek Atkins, chief technology officer at SecureRF said, "An issue with today's commonly implemented RSA and Diffie-Hellman type public-key protocols, including ECC, concerns the size of their computational footprint. While memory and energy usage is not a primary concern for high-resource platforms like smartphones and laptops, these issues, along with runtime, lie at the heart of any small computing device security discussion.

"Even ECC, with its lower resource usage than RSA or DH, provides inadequate performance in constrained devices to the point where developers are not even considering public-key solutions," continued Atkins. "Our WalnutDSA offers design engineers working with low-resource devices a very efficient and compact authentication solution that can be implemented today and will meet security requirements for the foreseeable future, including quantum resistance."

SecureRF's Atkins will present his paper at 12:15 p.m. on October 18. For those not registered to attend the event onsite, NIST is offering a live webcast which can be accessed at this link:
https://appam.certain.com/profile/form/index.cfm?PKformID=0x3190251bc

About NIST

The National Institute of Standards and Technology (NIST), is a non-regulated agency of the U.S. Department of Commerce that promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

About SecureRF

SecureRF Corporation uniquely offers computationally efficient and very strong security for the Internet of Things. The company's quantum-resistant security solutions, based on Public-Key cryptography, can be licensed for passive, battery-assisted, and active tags, wireless sensors, and embedded platforms including FPGAs, Microcontrollers, and ASICs. Applications include non-traditional payment systems, high-value supply chain management, cold chain management, and anti-counterfeiting applications in the pharmaceutical, consumer, defense, and homeland security sectors. Under the Veridify® banner, the company delivers a comprehensive cloud-based IoT solution for quickly and easily giving devices and products a secure place in the Internet of Things. For more information, please contact us at info@SecureRF.com or visit www.SecureRF.com.

# # #

Media Contact:
Joanne Kelleher
Marketing@SecureRF.com
203-227-3151