News Release

SecureRF Selected to Present its Algebraic Eraser™ Method at NIST Lightweight Cryptography Workshop

A lightweight, efficient asymmetric key agreement protocol for the Internet of Things

Highlights:

- SecureRF has been selected to present the Algebraic Eraser at NIST's Lightweight Cryptography Workshop 2015, July 20-21, 2015 in Gaithersburg, MD.
- The Algebraic Eraser is an ultra-low power, very fast Public-Key cryptography method targeting the Internet of Things.
- SecureRF's technology provides identification, authentication and encryption security for low power sensors and is suitable for low-resource FPGAs and ASICs such as ARM Cortex-M0 based devices.
- The Algebraic Eraser is 70 to 200 times better than Elliptic Curve Cryptography in speed and power with an energy reduction of up to 98%.

Shelton, Connecticut June 17, 2015 – SecureRF, a leading provider of security solutions for the Internet of Things, has been selected by the National Institute of Standards and Technology (NIST) to present its lightweight, efficient asymmetric agreement protocol, the Algebraic Eraser (AE), at their upcoming Lightweight Cryptography Workshop 2015, July 20-21, 2015 in Gaithersburg, MD. At the event, which shines a spotlight on issues related to the security and resource requirements of applications in constrained environments, SecureRF will highlight key findings contained in their paper: *Algebraic Eraser: A lightweight, efficient asymmetric key agreement protocol for use in no-power, low-power, and IoT devices.*

In the paper, SecureRF outlines key performance advantages of its Public-Key Diffie-Hellman style agreement protocol, AE, and how it outperforms other commercially available solutions to provide identification, authentication and encryption security for low power devices found on the Internet of Things. Specifically, in comparison against Elliptic Curve Cryptography (ECC), AE performed significantly better in both hardware and software – showing a 70 to 200 times improvement over ECC in speed and power (65nm CMOS).

"SecureRF is honored to be selected to present what we believe to be a next generation asymmetric security protocol," said SecureRF CEO Louis Parks. "The Algebraic Eraser is the world's first and only linear-in-time algorithm that offers an ultra-low power, very fast security solution to address devices

that are part of the Internet of Things. We are excited to have our methods reviewed by NIST and look forward to presenting the details of the Algebraic Eraser to conference attendees."

In addition to authentication, AE's linear-in-time methods support a wide range of other cryptographic functions including identification, encryption/decryption, HASH functions, and is available via partnerships and licensing arrangements.

About the Algebraic Eraser

The Algebraic Eraser™ cryptographic method delivers ground-breaking performance for low-power and passive devices. Offering both symmetric (private key or secret key) and asymmetric (public key) cryptography methods to meet a wide array of security and authentication needs, the AE algorithm runs in linear time with respect to the key length, and employs highly non-linear operations in a non-commutative infinite monoid—yielding unprecedented security. SecureRF has been granted U.S. Patent 7,649,999 for its technology invention in the field of cryptography. The technology, described in the patent entitled "Method and apparatus for establishing a key agreement protocol," provides a system and method for generating a secret key to facilitate secure communications between users via an algorithmically efficient one-way function using a branch of mathematics referred to as braid group theory. The algorithm is computationally hard to reverse while rapidly computable, thus enabling it to run on devices with low computing resources.

About SecureRF

SecureRF Corporation – Securing the Internet of Things® – provides security solutions for embedded systems and wireless sensor technologies used in non-traditional payment systems, secure supply chain management, cold chain management, and anti-counterfeiting applications in the pharmaceutical, fashion, spirits, defense, and homeland security sectors. The company's technology is based on a breakthrough in public-key cryptography that is computationally efficient, yet highly secure and available as a software development kit, Verilog/VHDL, or as a core for FPGAs and ASICs. SecureRF also offers the LIME Tag™ - a range of highly secure NFC, UHF, and Bluetooth LE sensor tags along with its anti-counterfeiting solution – Veridify™.
For more information on anti-counterfeiting, cybersecurity or securing the Internet of Things, please contact us at info@SecureRF.com. More information about SecureRF can be found at http://www.SecureRF.com. SecureRF's insights on security can be found on its blog at http://www.SecureRF.com/blog. Follow us on Twitter: https://twitter.com/SecureRF.

# # #

Media Contact:
Danny Bepko
Marketing@SecureRF.com
203-227-3151