News Release

SecureRF Announces Algebraic Eraser™ Core to provide Public Key security for FPGAs, ASICs, and embedded devices

Ultra-Fast and very low power solution to address devices that are part of the Internet of Things.

Highlights:

- Public Key core delivers greater than 60X performance improvement over ECC at a 128-bit security level (ECC 256)
- Core suitable for FPGAs, ASICs, and other low resource platforms including the ARM Cortex-M processors
- Addresses privacy and security needs for the Internet of Things including consumer products, medical devices, building/home automation, credentials, automotive, and mobile payments
- Tools support integration into new or existing product platforms

Shelton, Conn. (February 10, 2015) – SecureRF, a leading provider of security solutions for the Internet of Things, announced today its first Algebraic Eraser (AE) Core providing Public Key functions that deliver better than a 60X efficiency improvement, in timing, power consumption, and reduced footprint, over Elliptic Curve Cryptography (ECC) at a 128-bit security level (ECC 256). Due to the linear characteristics of the AE Core, even great efficiency over ECC is attained at higher security levels. The AE Core is designed for a wide range of Field Programmable Arrays (FPGAs), Application-Specific Integrated Circuits (ASICs) and the ARM Cortex-M family of processors.

This AE Core addresses the need for a high-performance Public Key authentication method that is optimized for cost and power. AE Core solutions target the Internet of Things (IoT) endpoints that are used for connectivity, credentials, the Smart Grid, industrial controls, and microcontrollers. Strong security and privacy is also required for consumer products, appliances, medical devices, and automotive. The AE protocol enables higher levels of security on very low-power or passive devices and supports many of the standard platforms now being developed.

“Device-level security is critical to protecting commercial and government solutions now relying on sensors and other embedded technologies that our AE Core is designed to address,” states SecureRF CEO Louis Parks. “Our recent benchmarks show that the AE Core is a breakthrough in size, power, and speed over today’s existing Public Key methods.”

The initial AE Core provides a Diffie-Hellman like authentication protocol and can be integrated with existing asymmetric and symmetric methods. In addition to synthesizable RTL in both Verilog and VHDL, SecureRF provides support for industry-standard tool chains such as Synopsys and ModelSim, executable C models, synthesis scripts, verification and regression suites, and interfaces for the 8051, and an AMBA 3.0 Lite Cortex-M0 core processor blocks on FPGA's. Additionally, products and devices developed with the AE Core may also choose to use SecureRF's back-end infrastructure and cloud-based dashboard for data management and reporting.

The AE Core with Public Key functions is based on SecureRF's breakthrough Algebraic Eraser algorithm, the world's first linear-in-time method. AE's linear-in-time engine supports additional protocols including a symmetric cipher, a stream cipher, a pseudo-random number generator, a HASH function, and a digital signature. The AE method has been published in peer-reviewed journals, presented at conferences around the world, and has been submitted for review and certification at world standards bodies. SecureRF also offers and supports an NSA Suite B family of cores that can be used alone or in conjunction with its AE Core.

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 on its Web site 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