SECURE RF
Securing the Internet of Things®

PRESS RELEASE

SecureRF to Launch IoT Security Solution for Low-Resource RISC-V Devices at 5th RISC-V Workshop

Shelton, Conn. – November, 28, 2016. Until now, design engineers working with low-resource variants of RISC-V processors have been unable to implement asymmetric (public-key) cryptography to secure these devices due to size and performance limitations. SecureRF today announced commercial availability of its WalnutDSA™ digital signature algorithm and Ironwood™ key agreement protocol for processors based on the RISC-V instruction set, making it possible to secure even the smallest RISC-V-based devices.

"ECC and RSA provide suitable security against current attacks in resource-rich environments. But when you need to provide security on constrained devices using the 32-bit RocketChip built with 'TinyConfig,' these solutions either don't fit or won't perform acceptably. Considering the life expectancy of RISC-V-based devices, the community must also plan for quantum attacks," said Louis Parks, president and CEO at SecureRF. "We are now delivering quantum-resistant asymmetric cryptography that works on low-resource RISC-V-based devices."

Upon the arrival of quantum computers (expected as soon as 10 to 15 years from today), contemporary asymmetric cryptographic methods, including RSA and ECC, will be rendered ineffective.

Derek Atkins, Chief Technology Officer at SecureRF said, "to optimize WalnutDSA for the RISC-V community, we coded it in RISC-V assembly language. Programs written in processor-specific assembly language run faster than their C counterparts, occupy less ROM and require less RAM. In the case of WalnutDSA on RISC-V, we achieved a 40% speed improvement (3.0 ms vs. 4.9 ms), and reduced the ROM footprint from 3,244 bytes to 2,952 bytes by moving from C to assembly. Ironwood will be released in RISC-V assembly language shortly."

Atkins will present "The Challenges of Securing and Authenticating Embedded Devices and a Suggested Approach for RISC-V" on November 29 at 4:00 p.m. PDT at the 5th RISK-V Workshop being held at Google's Quad Campus in Mountain View, CA. Atkins will explain the challenges that occur when attempting to add public-key security services to small processors. The presentation will also explore constraints in space, time, and energy, and how that restricts various potential solutions. Importantly, it also provides performance comparisons running SecureRF's WalnutDSA verification vs. ECDSA,

including: runtimes 93 or 430 times faster (faster time for ECDSA is with hardware multiply/divide instructions enabled); 1/500th of the instruction cycles to execute; ROM required reduced by 90 percent; and, RAM required reduced by 71 percent.

SecureRF is offering WalnutDSA and Ironwood as part of its IoT Embedded Security Development Kit (SDK). Readers may request the SDK in person from any SecureRF attendee at the Workshop or at http://info.securerf.com/iot-embedded-sdk-development-kit.

In addition to software implementations, SecureRF's cryptography can be integrated within hardware, enabling secure boot, device authentication and a root of trust. A root of trust is a non-malleable ability to embed security in hardware where even a firmware update will not change it, and any change to the software on the device, including firmware, can be validated against it.

About SecureRF

SecureRF Corporation uniquely offers computationally efficient and very strong security for the Internet of Things (IoT). 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:
Lauren LaFronz
Marketing@SecureRF.com
203-227-3151