

Future-Proof Security for Microsemi FPGAs and Low-Resource Processors

Fast, Easy to Deploy, Post-Quantum Ready Authentication and Data Protection

"Best Technology" – The Linley Group 2018
 "Best Contribution to IoT Security" – ARM TechCon 2017

Award Winning Security for IoT Designs

SecureRF provides fast, small footprint, low-energy, quantum-resistant, authentication and data protection solutions for Microsemi FPGAs and the 8-, 16-, and 32-bit endpoints they connect to. Use cases include secure boot, secure firmware updates and other applications that require rapid verification of digital signatures.

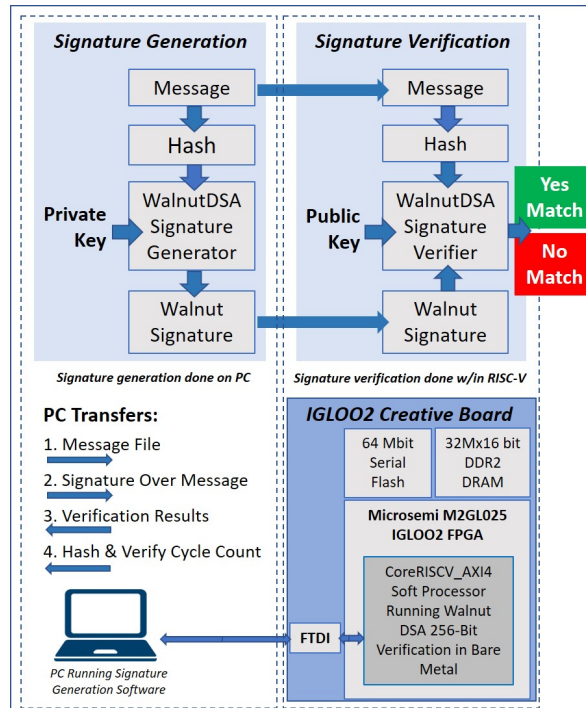
Post-Quantum Ready

Quantum computers will become powerful enough to break popular security methods like ECC and RSA within ten years. SecureRF's cryptography is resistant to all known quantum attacks.

Authenticate More Than gox Faster Than Other Methods

Walnut Digital Signature Algorithm™ (WalnutDSA™) and Ironwood Key Agreement Protocol™ (Ironwood KAP™) enable you to rapidly and securely communicate with sensors, actuators, and other highly constrained devices.

- SecureRF has implemented WalnutDSA on a Microsemi CoreRISCV_AXI4 soft processor core hosted by an IGLOO2 FPGA
- WalnutDSA verifies average length signatures in approximately 4 ms on a Mi-V core running at 66 MHz
- WalnutDSA will verify in about 1.3 ms with proposed RISC-V crypto extensions enabled
- The Mi-V core will also run SecureRF's Ironwood KAP



The diagram above describes a PC running Walnut DSA signing a message, then sending the message plus Walnut DSA signature to an IGLOO2 Creative Board where it is verified by WalnutDSA running on the RISC-V.

MARKETS

- Automotive
- Embedded Medical Devices
- Home Security/Home Automation
- Industrial Process Controls
- Low-Resource Network Hardware
- Smart Grid

FREE SECURITY CONSULTATION

SecureRF experts are available to solve your security issues and provide an initial security consultation for free.

FREE SDK AVAILABLE

The SecureRF IoT Embedded Security SDK enables you to easily implement SecureRF's public key security solutions. The toolkit includes: WalnutDSA, Ironwood KAP, and three separate demos.

ABOUT SECURERF

SecureRF develops and licenses quantum-resistant, public-key security tools for low-resource processors powering the Internet of Things (IoT). The company's small footprint authentication and data protection solutions deliver significant speed and energy performance enhancements when compared with ECC and RSA.

SecureRF security solutions are used to address wireless sensors, NFC, Bluetooth, and RFID tags as well as embedded platforms including FPGAs, microcontrollers, and ASICs. SDKs, RTL, and implementation tools are available for a wide range of environments.



SECURERF HEADQUARTERS
 100 Beard Sawmill Road, Suite 350
 Shelton, CT 06484, USA
 1-203-227-3151

CALIFORNIA OFFICE
 75 E. Santa Clara St., Floor 6
 San Jose, CA 95113 USA
 1-888-272-1977

www.SecureRF.com
 info@SecureRF.com
 www.twitter.com/SecureRF
 www.facebook.com/SecureRF

