Product Overview

Veridify Security

WalnutDSA™

Fast, Future-Proof Digital Signature Algorithm Designed for Low-Resource Devices

Foundation for Authentication and Identification

Digital signature algorithms are at the foundation of many of today's security applications. Secure boot, secure firmware update, device-to-device communication, authentication, and identification all rely on digital signature algorithms to protect devices against attack and compromise.

Fits on Even the Smallest Devices

Veridify's Walnut Digital Signature Algorithm™ (WalnutDSA™) is a public-key digital signature algorithm for low-resource devices—running on 8-, 16-, and 32- bit processors—that power the Internet of Things (IoT).

Fast, Compact, and Ultra-Low-Energy

WalnutDSA enables trusted authentication where legacy solutions cannot. WalnutDSA is easily deployable, in software, with great performance, on the widest range of devices, even after hardware designs are locked down. WalnutDSA is ideal for securing high volume automotive, consumer, medical, and industrial applications.

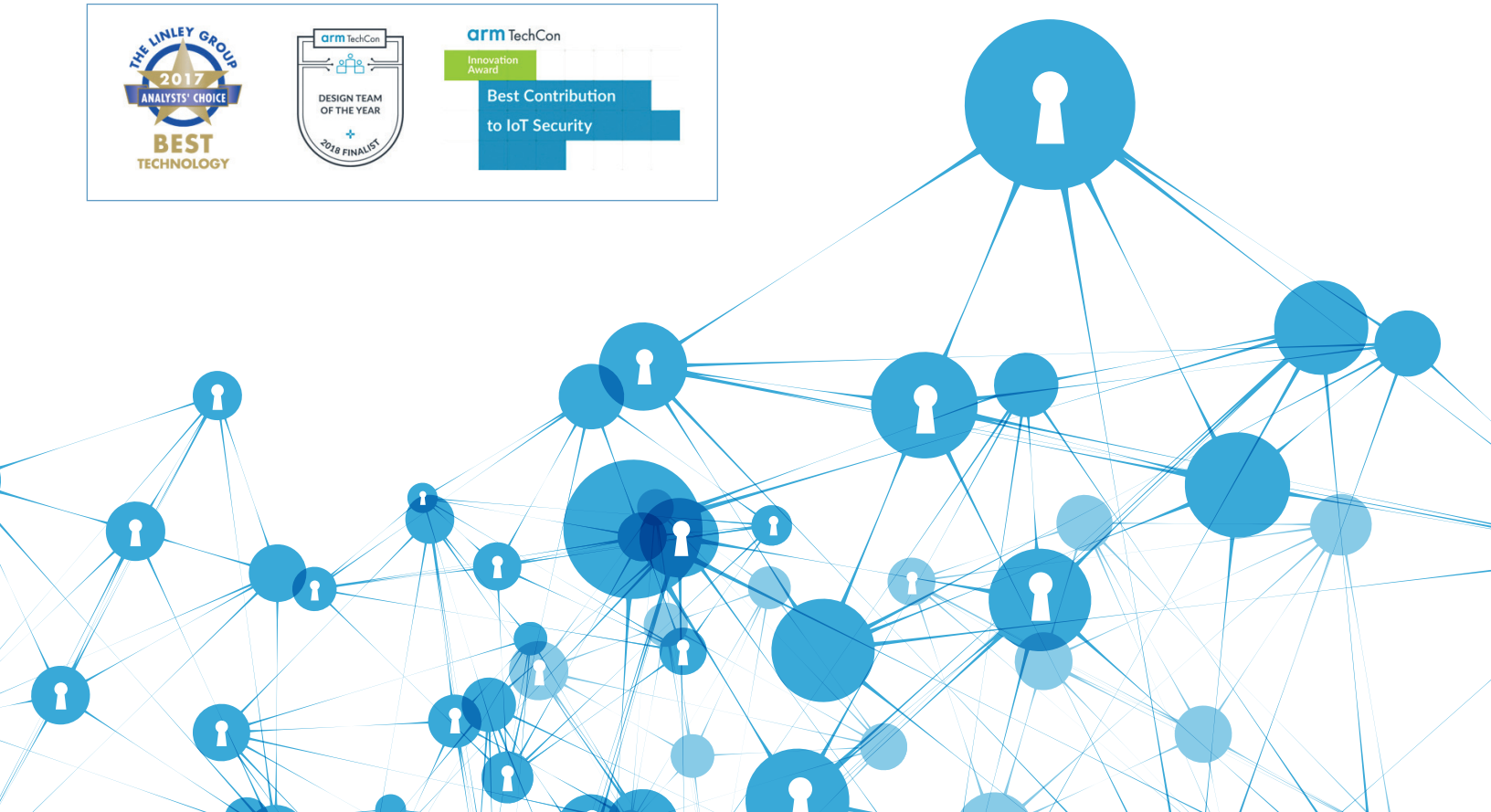
Future-Proof

If your connected devices are expected to be in the field for ten years or more, they will likely be vulnerable to threats from quantum computing. WalnutDSA is quantum-resistant against all known attacks.

THE LINLEY GROUP 2017 ANALYSTS' CHOICE BEST TECHNOLOGY

arm TechCon DESIGN TEAM OF THE YEAR 2018 FINALIST

arm TechCon Innovation Award Best Contribution to IoT Security



Overview

WalnutDSA™ is a fast, small footprint, future-proof, public-key digital signature solution for low-resource devices—running on 8-, 16-, and 32-bit processors—that power the Internet of Things (IoT).

Features and Benefits

- Drop-in replacement for ECDSA; up to 6x faster at 128-bit security levels
- Ideal for secure boot, secure firmware update, and authentication
- Software-only implementations save hardware cost, shorten time-to-market
- Free SDKs available for a wide range of 8-, 16-, and 32-bit processors
- Quantum-resistant to all known attacks

Software Implementations

- The WalnutDSA signature verification method is available now for a wide range of microcontrollers and processor cores including the 8051, AVR, STM-8, MSP430, ARM Cortex-M0, M3, M4, R4, R5, A9, RISC-V, Codasip BK, ARC EM, Andes S8, Renesas RL78, and others.
- A generation app is available for Windows or Linux to generate WalnutDSA signatures for evaluation. An HSM (Hardware Security Module)-based appliance is available to generate production keys and signatures for secure provisioning at a client or vendor site.

Hardware Implementations

A reference FPGA hardware implementation is available in Verilog RTL. The deliverables include:

- Synthesizable RTL— in Verilog
- Simulation and synthesis scripts— for easy evaluation and implementation
- Test vectors— facilitates rapid testing
- Verification and regression suites—full test coverage for design integrity
- Executable C models— verifies correct output from IP core
- Cryptographic keys— to exercise both the hardware core and the C models
- AHBLite 3.0 Interface— to interface processor to IP core for signature transfer and control
- Documentation and design support— for smooth implementation

Markets

- Automotive
- Consumer
- Industrial Process Controls
- Smart Building/Smart Grid
- Embedded Medical Devices
- Payments

Applications / Security Functions

- Authentication
- Identification
- Data Protection
- Secure Boot
- Secure Firmware Update
- Command Validation

Free Security Consultation

Our experts will provide an initial security consultation and can help accelerate time-to-market by creating a security solution design for your devices. Contact us at info@veridify.com

Free SDK to Get Started

Our IoT Embedded Security SDK allows easy implementation of our solutions. The toolkit includes: WalnutDSA, Ironwood KAP, and sample source code.

Request your SDK at:

info.veridify.com/iot-embedded-sdk-development-kit

Veridify Security

Corporate Headquarters:
100 Beard Sawmill Road, Suite 350
Shelton, Connecticut, 06484 USA

Silicon Valley Office:
75 East Santa Clara Street
San Jose, California, 95113 USA

1-888-272-1977
www.Veridify.com

©2019 Veridify Security Inc. All rights reserved. All trademarks are the property of their respective owners. Certain material is based upon work supported by the National Science Foundation; any views expressed are those of the author(s). For information covering our products, including trademarks, patents, and export control regulations, see Veridify.com/terms-of-use.