Product Overview

Veridify Security

Ironwood KAP™

Fast, Future-Proof Key Agreement Protocol Designed for Low-Resource Devices

Foundation for Authentication and Identification

Key agreement protocols are at the foundation of many of today's security applications. Veridify's Ironwood KAP™ is a future-proof, Diffie–Hellman-like Key Agreement Protocol (KAP) for the low-resource devices—running on 8-, 16-, and 32-bit processors—that power the Internet of Things (IoT).

No Key Database Required

Ironwood has characteristics of a public-key solution and a shared-key solution; it does not require a secure key database in order to produce a mutual shared secret.

Fast, Efficient, Compact, and Ultra-Low-Energy

Ironwood is computationally asymmetric; when two parties of different computational workload are interacting – like a gateway device and an 8- or 16-bit endpoint - you can put a greater computational workload on the gateway – enabling fast, compact, and ultra-low-energy, and performance that legacy solutions cannot match.

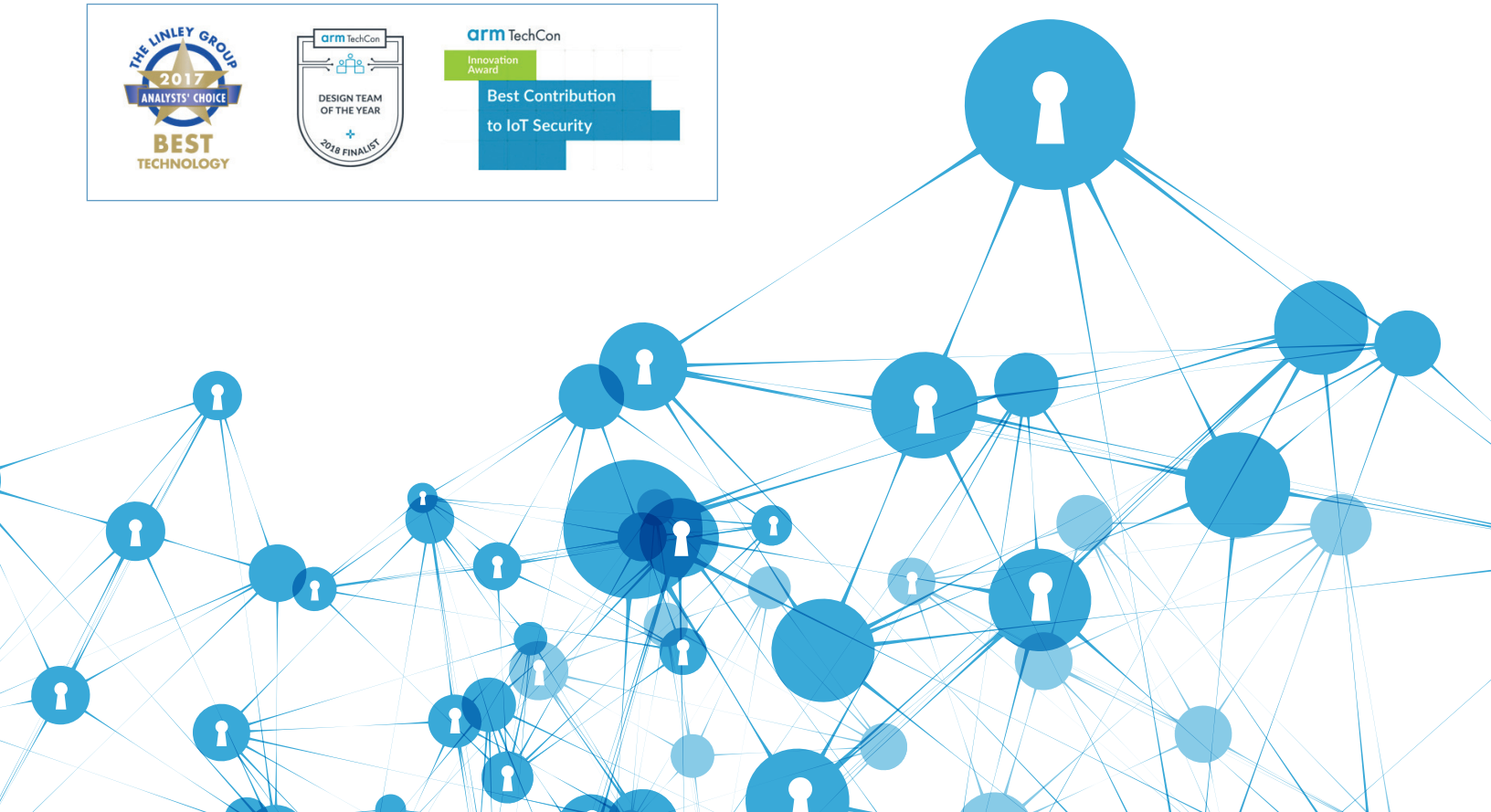
Future-Proof

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. Ironwood 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

Ironwood KAP™ is a future-proof, Diffie–Hellman-like Key Agreement Protocol (KAP) for the low-resource devices—running on 8-, 16-, and 32-bit processors—that power the Internet of Things (IoT).

Features and Benefits

- Up to 60x faster than ECDH at 128-bit security levels
- Ideal for secure boot, secure firmware update, and identification
- 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

- Ironwood is available 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 , and others. SDKs are available for several development environments including Eclipse, Code Composer Studio, IAR, Keil, Infineon DAVE, Atollic TrueSTUDIO, GCC, and others.
- SDKs are available to run Ironwood on Linux, Windows, and Android. SDKs include a pre-compiled Veridify crypto library, sample keys, certificates, signatures, and sample code.

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

Application

- 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