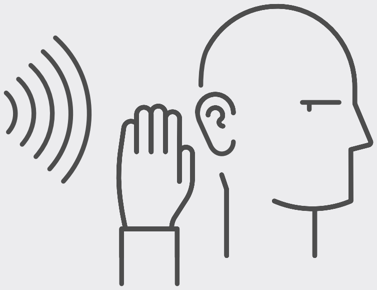
IDAHO SCIENTIFIC

Immunity
Side Channel Resistant Crypto Cores

Ever feel like your Alexa is listening to your conversation?

What sensitive information can be gathered
by eavesdropping on your system?

LA@SDUF09J34R; LASCVB-
NAO; SDIFOI&QKN3%AI&R-
8W34INKLG98WIOE45;
ILNGP8ADF; JGLW#ER68GN-
L^FEG)IO8OPHAEPR



- IP
- Proprietary Data
- User Credentials
- Keys
- Classified Data
- CPI

What problem does this solve? Instructions and data at rest and in transit are **vulnerable** to attack, introspection, or modification.

How does it work? The FPGA IP Cores encrypt, decrypt and authenticate information so that it cannot be exposed to anybody but the intended users. Crypto cores provides security for use cases including key generation/exchange/storage, digital signature, bulk encryption, packet encryption and message authentication.

What cores are offered? All Commercial National Security Algorithm (CNSA)/Suite B functions, available with and without DPA measures: AES, RSA, ECC, SHA2, SHA3, TRNG.

Why Immunity Cores?

- Lower Technical Risk – simple integration, reference designs and technical support from cleared US engineers who specialize in DOD systems security
- Proven Performance – NIST certified, Government validated and operating in Programs of Record
- More Flexibility – features configurable at compile and/or run-time

Benefits

- **Proven Security** through certification, assessment and operation in the field
- **Tunable sizing** to match security and performance within the constraints of the FPGA in your design
- **Simple Integration** thanks to industry-standard tools

Features

- Available cores:
  - **AES**: 128 or 256 key size and choice of Electronic Code Book (ECB), Cipher Block Chaining (CBC), CCM (Counter with CBC Message Authentication Code), Cipher Feedback (CFB), Counter Mode (CTR) or Galois Counter Mode (GCM). The core can be configured with variable S-boxes to minimize size or maximize performance.
  - **HMAC SHA-2/3**: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. SHA-224 and SHA-256 operate on 32-bit words and SHA-384, SHA-512, SHA-512/224, and SHA-512/256 operate on 64-bit words. Available as a compact or full core.
  - **Public Key Engine (PKE)**: RSA up to 8192, RSA-CRT, ECDSA/ECDH (NIST curves P 192-224-256-384-521), RFC7748 (Curve448, Curve25519, Ed25519, ANSSI-FRP256V1, Brainpoolr1
  - **True Random Number Generator (TRNG)**
- Robust Side Channel Attack (SCA), Differential Power Analysis (DPA) countermeasures with no leakage beyond 1 billion operations
- Available pre-packaged with a key management engine in a PCKS-11 compliant embedded Hardware Security Module
- Easy-to-use command interface for loading keys and changing the mode of operation
- Industry standard AMBA AXI4-Stream (AXIS) interfaces for initialization vector and data transfer

Deliverables

- Xilinx IP-XACT Package (VHDL)
- Product Documentation
- Example design with tutorial
- Simulation test bench to exercise NIST CAVP test vectors
- Technical support

Idaho Scientific

- Trusted U.S. Supplier
- Employees are cleared U.S. citizens
- Secure facilities
- No Foreign Ownership, Control, Influence (FOCI)

FAQs

Compatibility

- **Can the cores be used in only Xilinx devices?** The cores are all working and validated in Xilinx devices. Nothing in the design prevents porting to FPGAs and SoCs from other vendors.

Performance

- **FPGA Resources utilized?** 3k–40k LUTs depending upon which core(s) and which configuration. Contact Idaho Scientific for full performance data inclusing resource utilization, throughput and Fmax

Verification

- **What verification has been done on these Cores?** All Immunity Cores are NIST CAVP certified and have been assessed by third parties. Contact Idaho Scientific to discuss the status of Government assessment activities.

Ease of Integration

- **What should I expect to integrate the Cores into my design?** All Immunity Cores are delivered with a standard AXI-based interface and drag and drop from the IP catalog (Xilinx Vivado or other) into your design. Idaho Scientific also provides the driver stack, a reference design and complete documentation to simplify the integration process. If you run into any issues along the way, Idaho Scientific engineers are waiting by the phone in Boise, Idaho.
- **How are the Cores delivered?** Idaho Scientific mails a CD with Immunity Cores, documentation, reference design and a simulated test bench.

Idaho Scientific: Solve the Problem, Not the Symptom

Named as a 2019 Top 10 Security Company by Enterprise Security Magazine, Idaho Scientific is a specialized, embedded security firm with a proven track record of solving the hardest anti-tamper and cyber security problems for the Pentagon and National Labs with novel and scalable solutions. We prevent exploits at the device level, keeping your sensitive information and intellectual property safe from reverse engineering.

Learn more at idahoscientific.com or email us at info@idahoscientific.com to start a conversation.

© Copyright 2021 Idaho Scientific