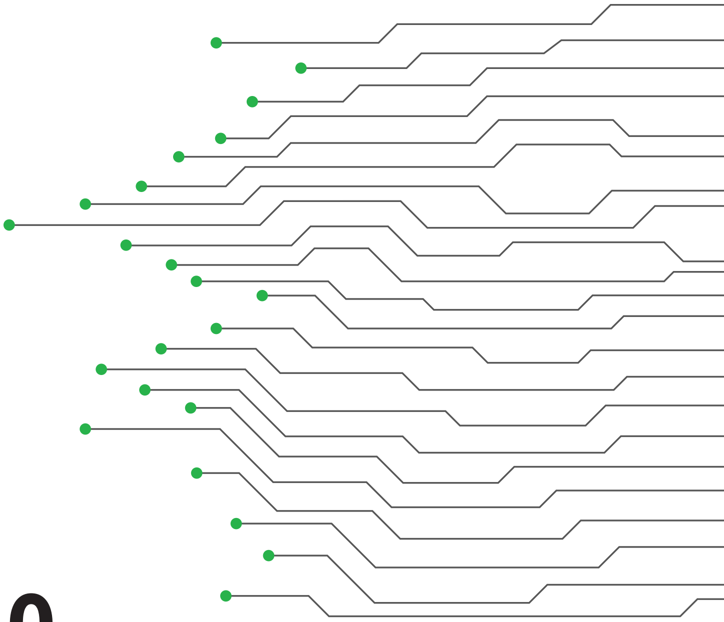
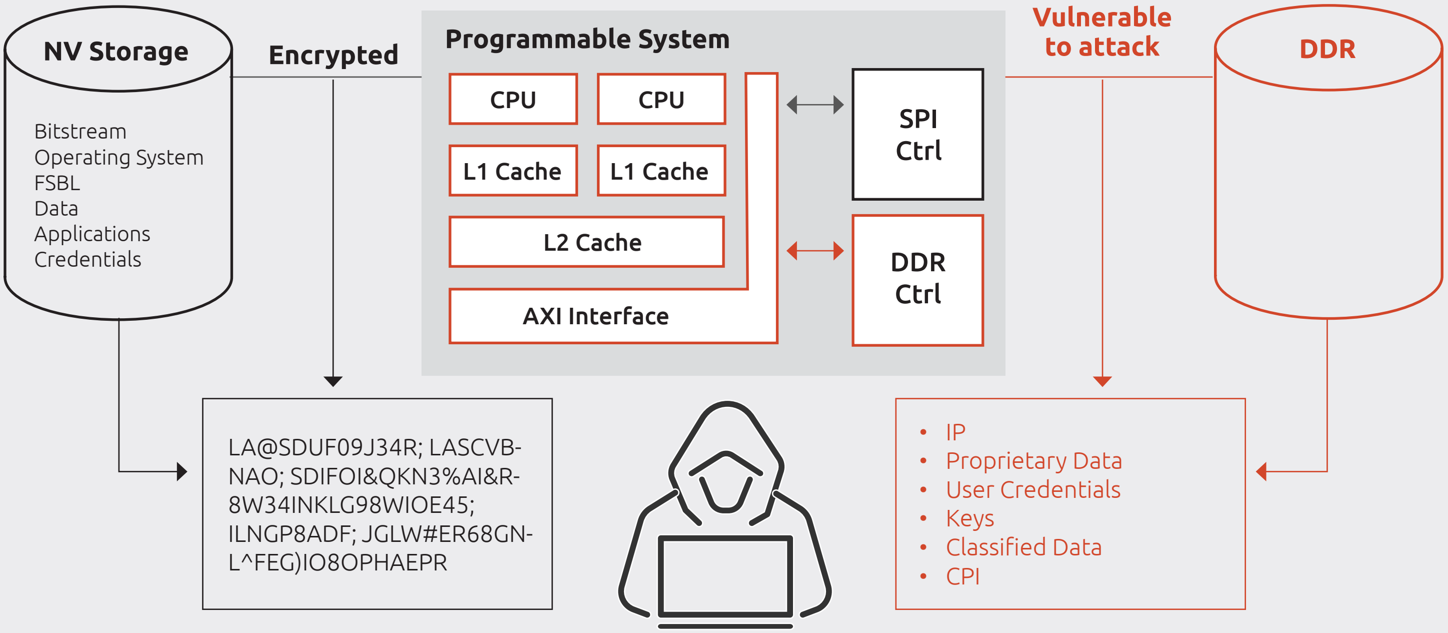
IDAHO SCIENTIFIC



Immunity
Inline Memory Encryption (IME) v3.0



NV Storage

- Bitstream
- Operating System
- FSBL
- Data
- Applications
- Credentials

Encrypted

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

Programmable System

CPU | CPU | L1 Cache | L1 Cache | L2 Cache | AXI Interface

SPI Ctrl

DDR Ctrl

Vulnerable to attack

DDR

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

What problem does this solve? Instructions and data stored in external memory are **vulnerable** to attack, introspection, or modification as they get loaded and executed.

How does it work? Immunity IME is shimmed in between the processor and memory controller to provide just-in-time encryption, decryption and authentication for all memory write and read requests.

What are the drawbacks of an IME? In the past, inline memory encryption came at too high of a cost in performance and physical attack vectors were not as prevalent. Immunity IME mitigates physical attack vectors with minimal performance impact.

Why Immunity IME?

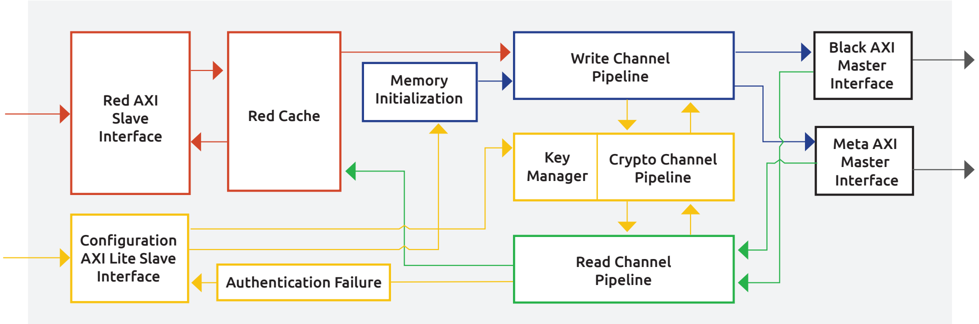
- Lower Technical Risk – simple integration, military-grade security
- More Performance – low latency, high throughput
- More Flexibility – features configurable at compile and/or run-time

Benefits

- **Security** for known run-time and at rest vulnerabilities
- **Tunable** to balance security while still maintaining system performance
- **Performance** includes simple integration and industry-leading latency

Features

- Performs encryption, decryption and/or authentication using AES Counter Mode (CTR) or Galois Counter Mode (GCM)
- Supports AES key sizes 128 or 256
- Internal key management with NIST-compliant key generation
- Encrypt memory space into user-defined vaults, each with a unique key
- Compatible with AMBA AXI4 interface
- Supports hard or soft memory controllers in Xilinx FPGA and SoC devices
- Supports multiprocessor systems
- Supports modern operating systems with and without MMUs
- Robust Side Channel Attack (SCA), Differential Power Analysis (DPA) countermeasures



Deliverables

- Xilinx IP-XACT Package (VHDL)
- Product Documentation
- Example design with tutorial
- Simulation test bench
- 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 IME support other devices?** IME is currently working in Xilinx ZU, ZU+ and Versal. Nothing in the design preventsporting to other devices

Performance

- **FPGA Resources utilized?** 25k–120k LUTs depending upon configuration
- **Impact to Application performance?** 1–6% depending upon configuration

Design Planning

- **What AXI bus configurations are supported?** Natively AXI4 at 128 bits wide. System designer can make use of AXISmart Interconnect to convert from other bus widths.
- **What memory overhead is required?** ~10–20% of available memory addresses are consumed for overhead. 0% system memory overhead is possible by using metadata on a separate bus.
- **How configurable are the uniquely keyed memory segment sizes?** User configurable, minimum is deposit size andmaximum is subject to block RAM availability
- **How is this product typically configured?** A reasonable configuration would be AES GCM with 256 bit keys and 4 GB of protected memory.

Functionality

- **How are errors handled?** IME has a IRQ output and a separate AXI interface for reading out the errors if they occur
- **How do you load keys?** Can the user provide key material? A driver is provided that has an API for programming entropy. Once entropy is entered, keys are generated automatically and stored internal to the core. Entropy is defined by the user.

Idaho Scientific: Solve the Problem, Not the Symptom

SymptomNamed 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.