Immunity AES

Advanced Encryption Standard (AES) IP Core

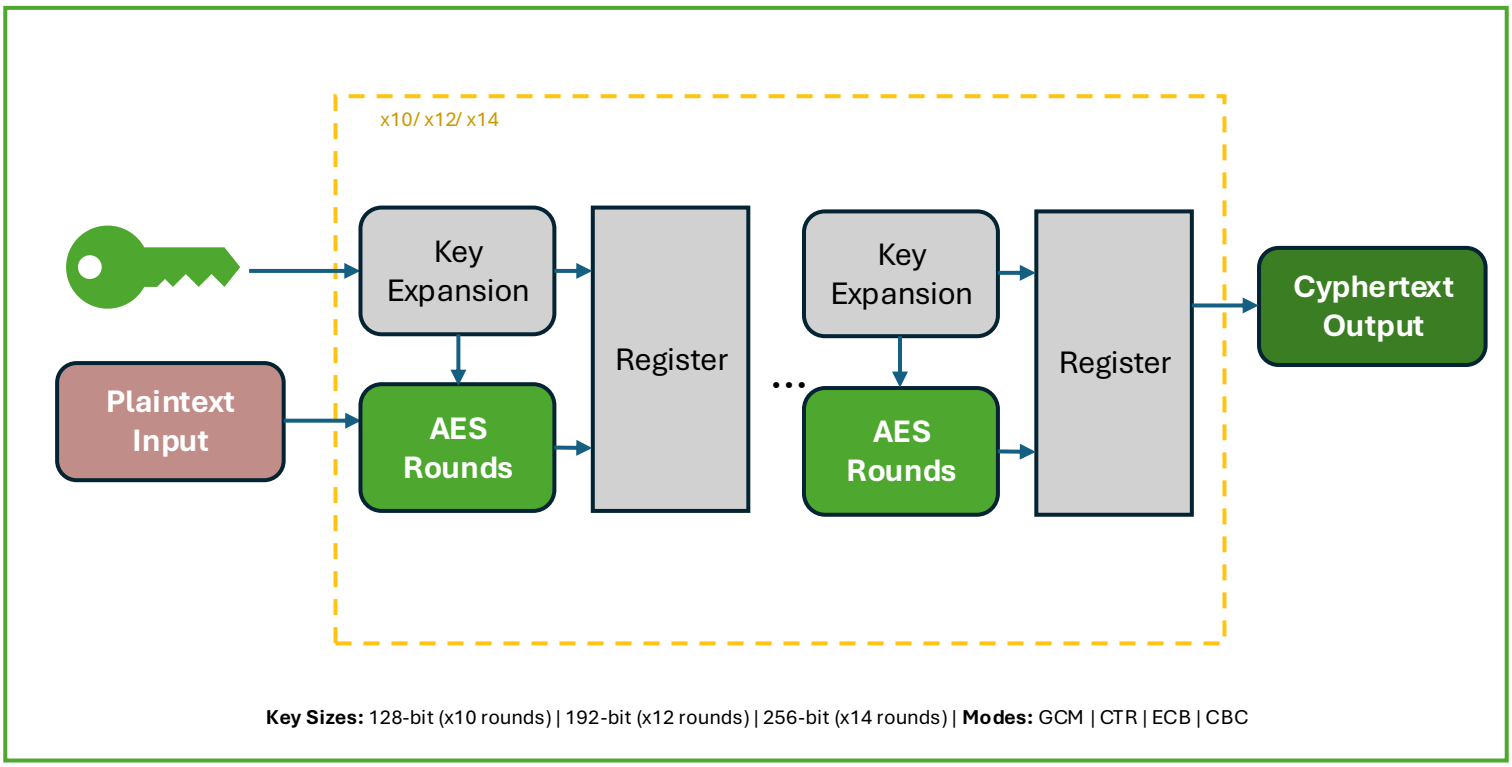
Overview

The Immunity™-AES IP Core performs encryption and decryption using the Advanced Encryption Standard (AES) cipher. Designed for embedded hardware and firmware protection, Immunity-AES is ideal for engineers working on DoW and defense-grade systems where data confidentiality and integrity are mission critical.

Immunity-AES is fully compliant with:

NIST FIPS-197 | NIST SP 800-38A | NIST SP 800-38D

A command interface is provided to load keys and set modes of operation. An AXI Streaming interface accepts initialization vectors and data, making integration straightforward and compatible with many third-party IP cores.



Key Sizes: 128-bit (x10 rounds) | 192-bit (x12 rounds) | 256-bit (x14 rounds) | **Modes:** GCM | CTR | ECB | CBC

Side Channel Countermeasures

Immunity-AES configurations are available with or without side channel countermeasures. Customers concerned with:

- Simple Power Analysis
- Differential Power Analysis
- Other side channel analysis (SCA) techniques

Contact Idaho Scientific for a full product brief and SCA testing assessment information.
info@idahoscientific.com | www.idahoscientific.com

GENERAL DYNAMICS
Mission Systems

IDAHO SCIENTIFIC

Benefits

Benefit	Description
Low Risk	Used in FPGAs and ASICs on Defense Programs. NIST-approved with proven side channel resistance.
Simple to Integrate	Drag-and-drop design delivered with reference designs and test benches using common interface IP.
Set and Forget	No annual maintenance contracts. Implementation of future updates is optional.
Trusted US DoW Supplier	Developed and supported by cleared US engineers who answer emails, take phone calls, and can travel to ensure smooth integration.

Features

Feature	Detail
Encryption/ Decryption	Full AES encrypt and decrypt capability
Key Sizes Supported	128-bit, 192-bit, 256-bit
Modes of Operation	GCM, CTR, ECB, CBC
Standards Compliance	NIST FIPS-197, SP 800-38A, SP 800-38D
Command Interface	Easy-to-use interface for loading keys and changing modes
AXI Streaming Interface	Industry-standard AMBA AXI4-Stream (AXIS) for plaintext/ciphertext, IV, and tag transfer
Side Channel Countermeasures	Optional robust SPA/ DPA countermeasures
NIST CAVP Test Vectors	Simulation test bench exercises supported NIST CAVP test vectors

Deliverables

Xilinx IP_XACT Package	Product Documentation
Example Designs	Simulation Testbench
Technical Support	Maintenance Updates

✓ ***NIST Certified*** ✓ ***Programs of Record*** ✓ ***Configurable***