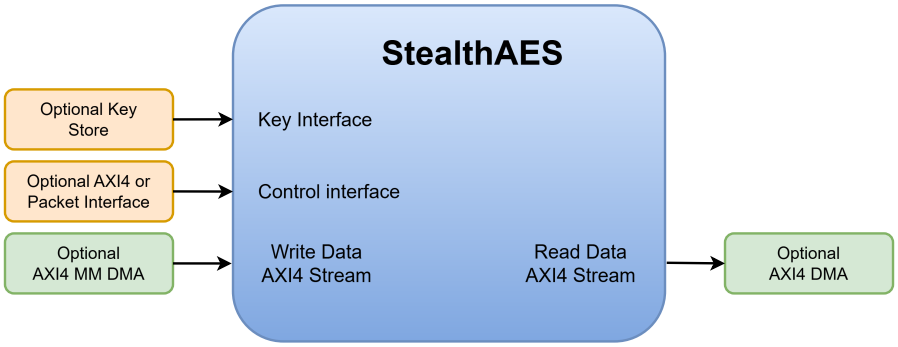
StealthAES

Industry-Leading AES-GCM Encryption IP With Advanced Side-Channel Countermeasures

Delivering optimal balance of area efficiency, throughput, and security with state-of-the-art protection against side-channel attacks for high-security FPGA and ASIC designs.

Up to 10 Gbps	1B+	8-58K
AES-256 GCM Performance	Trace SCA Resistance	LUT Range



Key Features

- **AES-GCM 256-bit Encryption**
  Complete implementation with authentication
- **Advanced Side-Channel Countermeasures**
  Proprietary, extensively tested protection
- **Streamlined Interface**
  AXI4-Stream with isolated key loading
- **NIST Standards Verified**
  Rigorously tested compliance
- **Customizable Integration**
  PCIe, DMA, and packet processing support
- **Easy FPGA/ASIC Integration**
  Comprehensive documentation included
- **Optional Key Storage**
  Simple key agility with key slot referencing
- **Scatter-Gather DMA**
  Optional support for efficient memory ops

Applications

Defense & Aerospace
- Secure communications
- Data at rest encryption
- Mission-critical systems
- Classified data protection

Financial Services
- Transaction security
- HW security modules
- Payment processing
- Secure key storage

Critical Infrastructure
- Industrial control systems
- Smart grid security
- Transportation systems
- Energy sector protection

Commercial Systems
- Data center security
- Cloud computing
- IoT device protection
- Enterprise networks

StealthAES Product Overview

Performance and Resource Utilization

FPGA Platform	Max Frequency	AES-256 GCM Performance	Area (LUTs)
AMD UltraScale+ and Versal	200 MHz	1.6-10 Gbps	8K-36K LUTs
Microchip PolarFire	100 MHz	0.8-5 Gbps	13K-58K LUTs
Intel Agilex 5	180 MHz	1.5-9 Gbps	9K-44K LUTs

Note: Performance numbers shown are example configurations. StealthAES is available in higher-performance configurations to meet your design requirements.

Side-Channel Security

StealthCores has verified StealthAES side-channel countermeasures with over **1 billion encryption operation measurements**, achieving a more than **10 million times improvement** in side-channel security compared to non-countermeasure designs. Our verification processes utilize industry-standard Test Vector Leakage Analysis (TVLA) and template attack testing, ensuring resistance to both power and electromagnetic leakage.

SCA Testing Methodology

- Power & EM side-channel analysis
- 500 MHz bandwidth, 5 GS/s sampling
- FPGA vendor dev kit testing
- High-frequency leakage detection

Security Features

- Multi-order masking
- Secure key storage architecture
- Hardware-enforced isolation
- Minimal performance impact

Why Choose StealthCores?

Expert Support

Decades of cryptographic implementation experience with dedicated integration support and comprehensive documentation.

Optimal Performance

Best balance of area efficiency, speed, and security with configurations ranging from 0.8 to 10 Gbps across multiple FPGA platforms.

Flexible Integration

Tailored implementations with PCIe, DMA, and packet processing options to match your specific design requirements.

Standards Compliance

NIST standards verified implementation ensuring reliable and trusted security for commercial and defense applications.

Ready to Secure Your Systems?

info@stealthcores.com | www.stealthcores.com | | Rev. 25.1