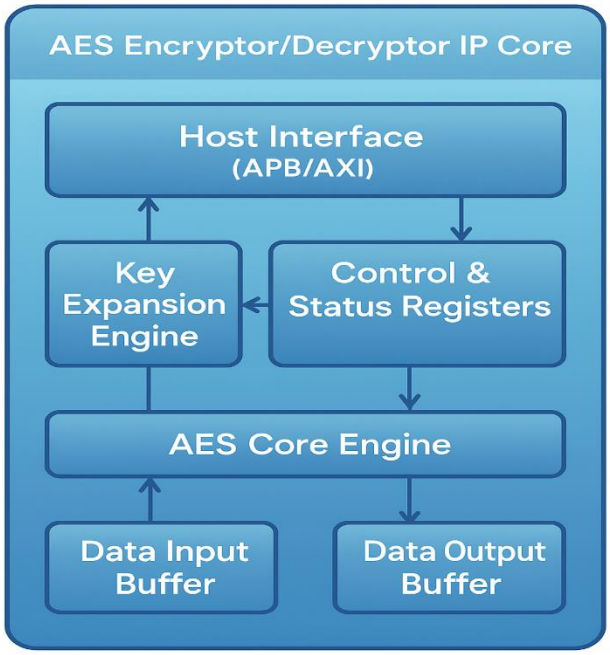
DESIGN IP PRODUCT SHEET

AES - Encryptor/Decryptor

The silicon proven **AES Encryptor/Decryptor IP Core** delivers high-performance, standards-compliant data security for SoC, ASIC, and FPGA platforms. Supporting AES-128, AES-192, and AES-256 key lengths, this silicon-proven IP implements the full Advanced Encryption Standard (AES) algorithm as specified by NIST FIPS 197. Designed for seamless integration, the core enables real-time, low-latency encryption and decryption with configurable operating modes, offering robust protection for sensitive data in embedded, networking, storage, and consumer applications.

Ideal for: High-performance embedded processors, Network switches, routers, and storage controllers, Consumer multimedia and gaming devices Industrial and automotive computing AI/ML accelerators, HPC, and datacenter



Deliverables

Synthesizable RTL (Verilog/VHDL), Comprehensive testbench (UVM) Integration and synthesis scripts Documentation (user guide, register map) and Reference designs

Features

- Full compliance with AES (FIPS 197) standard
- Supports key sizes: **128, 192, and 256 bits**
- Encryption and decryption in ECB, CBC, CTR, GCM, and XTS modes
- High throughput: **Configurable pipelined or iterative architecture**
- Low latency
- Supports streaming and block processing
- Integrated key expansion and secure key storage
- APB/AXI4-Lite host interface for easy SoC integration
- Programmable interrupts, status, and error reporting
- Optional side-channel countermeasures (masking, SCA resistance)