

Application Areas

- ▶ AES ECB
- ▶ AES GCM for IEEE 802.1 AE-2006
- ▶ AES GCM for IPsec RFC 4106
- ▶ AES GMAC for IPsec RFC 4543
- ▶ AES XCBC for IPsec RFC 3566
- ▶ AES CCM for IPsec RFC 4309
- ▶ AES CCM for IEEE802.16 WiMax
- ▶ AES CCM for IEEE802.11 WLAN

Features

The AES IP has the following features

- ▶ Optimised for both ASIC and FPGA targets
- ▶ Per packet dynamic selection of key size
- ▶ Dual-ported key expansion memory for FPGA
- ▶ On-the-fly key expansion option
- ▶ AMBA AHB or APB memory mapped option
- ▶ Fully synchronous
- ▶ Verilog 2005
- ▶ Operates in 11, 13 and 15 clock cycles for keys of 128, 192 and 256 respectively
- ▶ 2.3 Gbps encryption/decryption on Stratix III
- ▶ Support for all authentication modes

Specification

The Advanced Encryption Standard (AES) is an encryption algorithm originally intended for securing sensitive but unclassified material by US Government agencies. Since its publication FIPS-197 (Federal Information Processing Standards Publication 197) it has been widely adopted by commercial and private organizations and included in many international standards, most notably 802.11 WLAN, IPsec and IEEE 1619 for hard disks.

EnSilica provide a sophisticated suite of AES related IP for use in ASIC or FPGA target technologies. As each configuration is specific to customer requirements we have prepared individual IP modules that enable a flexible trade-off of throughput with area to get the most optimized solution. The base suite consists of Encryption, Decryption, Key Expansion and Cryptographic Mode modules that together cover all the combinations required for encryption and authentication. All modules support the three key sizes, dynamically selectable per-packet. For the lowest gatecount the modules can be configured to support only one key size. In addition all modules are available with AMBA AHB or APB interfaces.

The Encryption module has 128-bit input and output buses for both Plaintext and Ciphertext respectively, as shown in Figure 1. It makes single cycle accesses to a 128-bit Round Key memory during the encryption process. Encryption therefore takes just 11 clock cycles for a 128-bit key. The Round Keys can either be generated on-the-fly or stored in a memory.

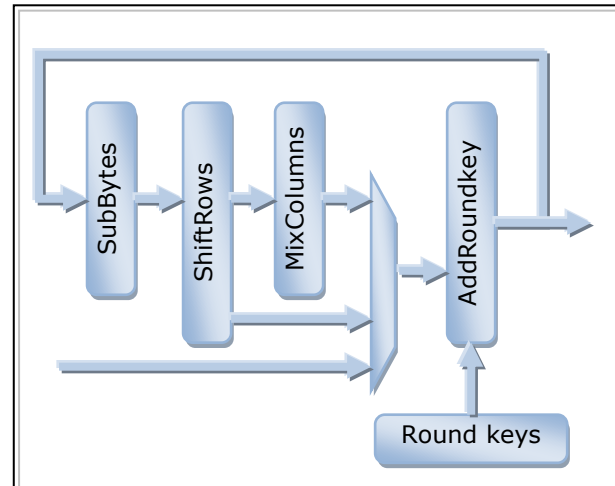


Figure 1: Encryption architecture

The Decryption module also has 128-bit input and output buses for both Ciphertext and Plaintext respectively. Decryption also takes just 11 clock cycles for a 128-bit key. The Round Keys must be pre-stored in a memory because they are read out in reverse order, and cannot be generated on-the-fly.

The Key Expansion module works in synchronization with the encryption module and produces a new round key every clock cycle. The Key Expansion module may not be needed in some application if a processor is available to calculate the Round Keys offline.

For FPGA targets the IP makes full use of block memory for intermediate results storage and Round Keys. Where appropriate for simultaneous encryption and decryption it instances a dual-ported Round Key memory, which can be shared for efficiency.

Resources

The following represent typical logic and memory resources for an Altera Stratix III, where run-time programmable key size is specified. The single key size cores are smaller.

Variant	LEs	Mem Bits	Fmax MHz	Throughput
Encrypt	305	34 K	235	2.3 Gbps
Decrypt	448	34 K	211	2.3 Gbps
Key expansion	623	8 K	204	

Depending on the technology used, encryption with on-the-fly key expansion hardware occupies 30k ASIC gates. Combining encryption, decryption and key expansion requires 60k ASIC gates and a round key memory.