

Features

- Throughput up to 40 Mbps
- Area: 8,000 ASIC gates for encrypt/decrypt, key expansion and interface logic
- 32 bit data and control bus interface
- Support for 128, 196 and 256 bit keys
- Automatic generation of key context from key data
- Core verified through NIST FIPS vectors to ensure complete standards compliance
- Test bench provided

Applications

- WLAN applications such as 802.11i
- IPSec designs in residential gateways, multi-service access products
- Military communications systems
- Secure video surveillance
- Secure audio communications

NIST has standardized on a new cipher called AES which can be implemented efficiently in hardware and software. It is becoming the cornerstone of cryptography and is now included in IPsec, 802.11i, 802.15 and 802.16 among many others.

The advanced encryption standard (AES) block from Elliptic is fully proven in silicon and now shipping in volume. The CLP-11 is a high performance cipher block that performs encryption, decryption and key expansion in a very small silicon area - perfect for applications where cost is paramount.

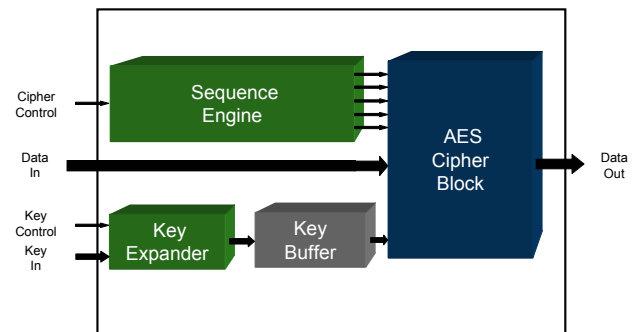
General Description

The Advanced Encryption Standard (AES) algorithm is a subset of the Rijndael algorithm. It was selected by NIST as a replacement algorithm for DES which is no longer considered cryptographically secure due to the susceptibility of brute force attacks using modern computational power. The AES algorithm is a 128 bit block cipher and supports three different key sizes; 128, 192, and 256 bits. The block diagram for the CLP-11 is shown in Figure 2 below.

The CLP-11 implementation fully supports the AES algorithm for all key sizes. The goal of the design was to create a design in a very small silicon footprint which is suitable for throughput in the 1 Mbps to 100 Mbps range. Unlike other small gate count cores, the CLP-11 implements the complete cipher operation including key expansion, encryption and decryption. The CLP-11 uses the base cipher mode AES-ECB (Electronic Code Book). The core can be wrapped with additional logic to support any other AES modes such as CBC, OFB, CRB, CTR, CCM, etc. Please contact Elliptic directly for more information.

The core operates in one of three modes:

- Key update - pass the key then expands the key for a cipher operation
- Encrypt plaintext at the input to ciphertext at the output
- Decrypt ciphertext at the input to plaintext at the output



The table below outlines the performance that can be achieved with different key sizes:

Key Size	Key Generation Cycles (per key)	Cipher Cycles (per block)
128 bits	117	262
192 bits	125	312
256 bits	154	362

Therefore, to calculate the throughput achieved for a given clock frequency provided to the core, the designer must understand the key rotation cycle and traffic characteristics. For example, if the core is clocked at 100 MHz and a 1024 byte packet is first encrypted with one 128 bit key then another 512 byte packet is decrypted with another 128 bit key the following throughput is achieved:

Cycles to load and expand the transmit key: 117
 Cycles to encrypt 1024 byte packet: $1024 / 16 * 262 = 16768$
 Cycles to load and expand the receive key: 117
 Cycles to decrypt 512 byte packet: $1024 / 16 * 262 = 8192$
 Total cycles required = 25194

With a clock frequency of 100 MHz (a clock period of 10 ns), the overall throughput achieved is 1536 bytes processed in 25194 clock cycles or 251.9 μ s. The instantaneous throughput is therefore 48.8 Mbps.

General Description cont'

Key Buffer

A key buffer memory is required for the CLP-11 core. It is expected that the designer will instantiate a technology specific memory into the provided wrapper. The requirements for the key buffer memory are:

- Single port
- Single synchronous read
- Single port write
- Size 60 words by 32 bits – for 256 bit keys

If only a single key size is required, the memory may be re-sized to support that specific requirement. Please contact Elliptic for more information.

An FPGA load can be made available under license for evaluation purposes.

The CLP-11 is part of a complete family of AES cores that range from small gate counts and moderate throughput to very wide data path cores capable of Gbps operation. Please see the Elliptic web site for more information.

Other Products of the Family of AES Cores

- CLP-15: Ultra-High Throughput AES-GCM Core - 40 Gbps
- CLP-16: Ultra-High Throughput AES-GCM Core - 10 Gbps
- CLP-20: High Throughput AES-CCM Core - 1 Gbps
- CLP-24: High Throughput AES-GCM Core - 5 Gbps
- CLP-28: 802.16/WiMAX AES Core
- CLP-33: XTS-AES Core
- CLP-34: AES Key Wrap Core
- CLP-45: Configurable Lookaside AES Core
- CLP-47: Configurable XTS-AES Core

Availability

The CLP-11 is available in soft IP form HDL Source. The deliverables available are:

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script & constraints
- Sample simulation script
- Documentation