

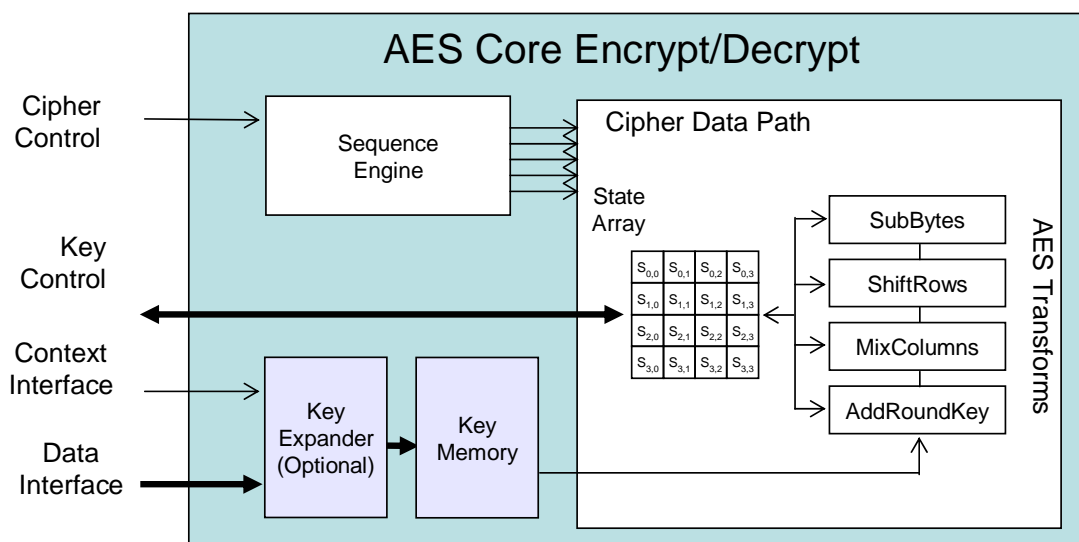
NIST has standardized on a new cipher which can be implemented efficiently in hardware and software. It is becoming the cornerstone of cryptography and is now included in IPsec, 802.11i, 802.15 and 802.16 among many others. The advanced encryption standard (AES) block from Elliptic is fully proven in 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

### Key Features:

- Electronic Code Book algorithm
- Optional support for CBC mode if required
- 32 bit data and control bus interface
- Support for 128, 196 and 256 bit keys
- Core verified through NIST FIPS vectors 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



## 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 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 40 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 Semiconductor 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 in different Lattice FPGAs

Lattice FPGA	Resource Requirement (Slices)	Maximum Clock (MHz)	Throughput at Max. Clock (Mbps)
ECP-DSP ECP33E05	1917	33	16 <sup>1</sup>
LFXP20E-5	2995	58	29 <sup>1</sup>

Note: 1. For 128 bit keys

## Availability

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

- EDIF netlist
- Testbench
- Documentation

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 contact Elliptic Semiconductor for more information:

Elliptic Semiconductor Inc.  
62 Steacie Drive, Suite 201  
Ottawa, ON, K2K 2A9

Phone: +1 613 254-5456  
Fax: +1 613 254-7260  
Email: [info@ellipticsemi.com](mailto:info@ellipticsemi.com)