

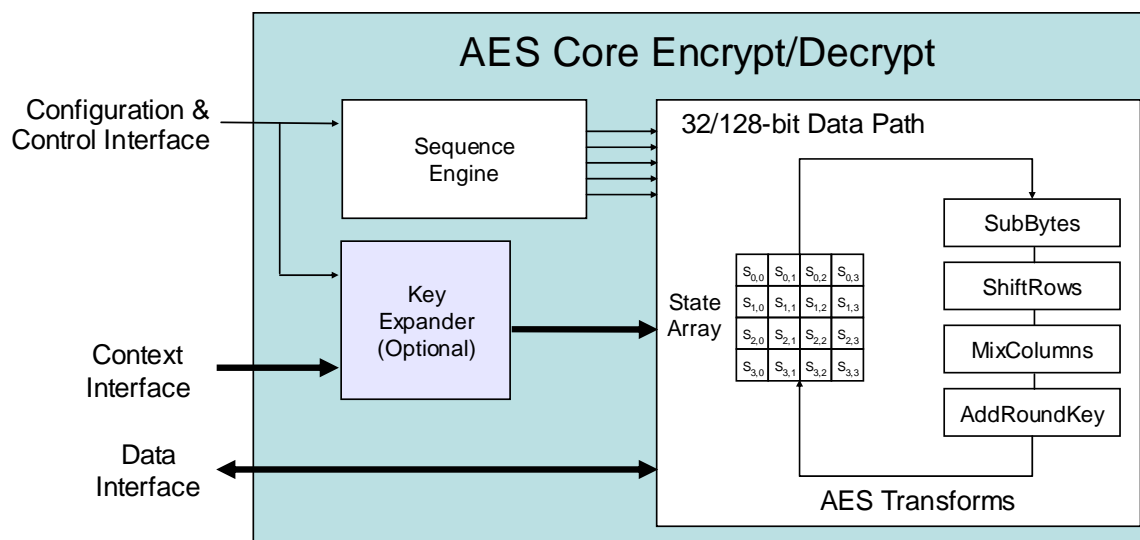
The Advanced Encryption Standard (AES) has been standardized by NIST to replace the Data Encryption Standard. It is rapidly becoming the cornerstone of cryptography and is now included in 802.11i, WiMAX, SSL, IPsec and many other applications. The CLP-03 core is a fully proven block available for immediate licensing.

### Key Features:

- Supports ECB and CBC modes
- OFB, CFB, CCM and OMAC versions optionally available
- Support for 128, 192 and 256 bit keys
- 32 bit data interface
- Key expander options to suit the application
- Key memory accessible through separate memory interface
- Test bench provided

### Applications:

- IPsec and SSL designs in residential gateways, multi-service access products
- Storage – SAN/NAS applications
- Wireless applications such as 802.11i and 802.16
- Military communications systems
- Secure video surveillance
- Secure audio communications



## General Description

The Advanced Encryption Standard (AES), a subset of the Rijndael algorithm, has been standardized by NIST to replace DES which is no longer considered secure. The AES algorithm is a 128 bit block cipher that supports three different key sizes: 128, 192, and 256 bits.

The CLP-03 implementation fully supports the AES algorithm for all three key sizes. The core supports both Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes. It can be augmented to support Counter Mode (CTR), Counter Mode with CBC-MAC (CCM), and One-key MAC (OMAC) methods of operation. The AES context consists of a key which is one of 128, 192, or 256 bits, and, where required, an initialization vector, counter, and other data depending on the mode of operation. The context is accessed through the control processor port on the block.

The following table outlines the resource utilization and performance achieved by the CLP-03 in target Lattice FPGAs.

Lattice FPGA	Resource Requirement (Slices)	Maximum Clock (MHz)	Throughput at Max. Clock (Mbps)
ECP-DSP ECP33E05	4301	55	146 <sup>1</sup>
LFXP20E-5	2995	58	154 <sup>1</sup>

Note: 1. Throughput stated for 128 bit keys.

The CLP-03 is a member of a broad range of AES cores available from Elliptic Semiconductor. Please contact us for further information for cores that range from small footprint designs to ultra-high throughput capability all available in Lattice FPGAs

There are two major interfaces which must be connected. The control processor interface is a slave memory bus which allows an external processor to access the internal configuration registers. The memory interface is a master memory bus which accesses the data to be processed.

Elliptic offers a variety of key expander options for the CLP-03 which are outlined in more detail below:

1. For customers that want to use the core with a fixed key that seldom changes, the key expansion can be done in an embedded processor and the expanded key stored in registers for use by the CLP-03.
2. Elliptic also offers a small footprint key expander which requires 300 clock cycles to expand the key. This option also requires registers to store the expanded key.

3. Finally for high performance applications where keys are rotated or multiple key contexts must be provided to the core, a high speed key expander is available.

The choice of key expander options can be discussed with Elliptic applications engineering to determine which choice is appropriate for the application that the FPGA is targeted at.

The CLP-03 is available in soft IP form in EDIF format. The deliverables available are:

**Netlist Licenses:**

- EDIF netlist
- Testbench
- Documentation

For more information, please contact Elliptic Semiconductor at:

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

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