

The IEEE has ratified the 802.16e security standard. It requires an AES core capable of supporting multiple modes including ECB, CBC and CCM. The CLP-28 core is based upon Elliptic's high performance, silicon proven AES multi-mode core and has been tailored specifically to the needs of WiMAX developers.

### Key Features:

- AES-ECB compliant to the NIST FIPS PUB 197 specification
- Implementation of AES-CBC and AES-CTR to NIST Special Publication 800-38A.
- Implementation of AES-CCM to the NIST SP 800-38C specification
- 128 bit keys - extensible to 192 and 256 bit keys if required
- Gate count of 23K ASIC gates
- Optional interfaces include FIFO and dual-port RAM
- Test bench provided

### Applications:

- 802.16 WiMAX in base station and subscriber applications

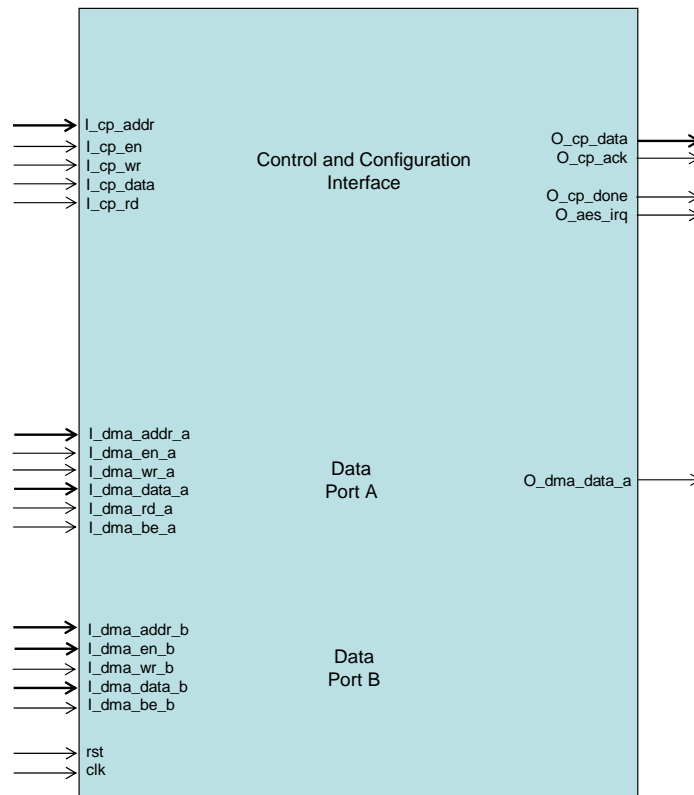


Figure 1 CLP-28 Pin Diagram

## General Description

The Advanced Encryption Standard (AES), is based on the Rijndael algorithm. It has been standardized by NIST to replace DES which is no longer considered secure. The algorithm is a 128 bit block cipher and supports three different key sizes; 128, 192, and 256 bits. The IEEE standards body is nearing ratification of the security requirement for WiMAX and in the P802.16e/D12 draft of the standard has AES specified as a mandatory cipher with 128 bit key size and support for the following modes:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter Mode (CTR)
- CCM (Counter mode with Cipher block chaining Message authentication)

The CLP-28 implementation supports all of these modes exclusively with 128 bit keys in order to optimize gate count. The core can easily be expanded to include all three key sizes.

## Throughput

The CLP-28 achieves different throughput depending on the mode of operation. The throughput is gated however by CCM mode as it requires two passes through the data – one for encryption and one for message authentication. The table below illustrates the throughput of the core at 125 MHz and 200 MHz as reference points for implementations in 0.18 $\mu$  and 0.13 $\mu$  respectively

Key Size (bits)	Mode	Throughput bits/Hz	Throughput at 125 MHz	Throughput at 200 MHz
128 bit	AES-CCM	1.33	166 Mbps	220 Mbps
192 bit	AES-CCM	1.14	152 Mbps	189 Mbps
256 bit	AES-CCM	1.00	125 Mbps	166 Mbps
128 bit	AES-CTR, -CBC, -ECB	2.6	325 Mbps	431 Mbps
192 bit	AES-CTR, -CBC, -ECB	2.2	275 Mbps	365 Mbps
256 bit	AES-CTR, -CBC, -ECB	1.9	238 Mbps	315 Mbps

**Table 1 Throughput Capabilities**

WiMAX implementations require throughput anywhere from 1 Mbps to 100 Mbps and as such the core is profiled to meet this performance goal.

## Key Expansion Options

Elliptic offers a variety of key expander options for the CLP-28 as outlined 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-28.
2. Elliptic also offers a low speed key expander which occupies only 1000 ASIC gates. 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 table below illustrates the choices that a designer has in key expansion options.

Key Expander Implementation	ASIC Gate Count (NAND2 Equivalent Gates)
Software	0 <sup>1</sup>
Compact Key Generator	1000 <sup>2</sup>
Fast Key Generator 128-bit Key Size	9000
<sup>1</sup> Memory for key storage required. <sup>2</sup> Key and cipher computations share a common S-box. This gate count value does not include S-box and dedicated memory gate count.	

The choice of key expander options can be discussed with Elliptic applications engineering to determine which choice is appropriate for the markets targeted for the SoC.

## Context Memory

The CLP-28 can be configured at build time to support multiple contexts. The context memory is constructed from single port memory specified in pages with each page occupying 24 words × 32 bits (96 bytes). The keys and any other relevant data such as initialization vectors or counters are loaded into context memory prior to starting the engine.

The CLP-28 is available in soft IP form, either as a Netlist or HDL Source. The deliverables available are:

**Netlist Licenses:**

- Post synthesis netlist
- Testbench
- Sample simulation script
- Documentation

**HDL Source Licenses:**

- HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load can be made available under license for evaluation purposes either as a bit file or optionally on the EVAL-01 evaluation system. For more information on pricing and the complete user's manual, please contact:

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)