

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

Key Features:

- Throughput of over 750 Mbps
- Supports ECB and CBC modes
- OFB, CFB, CCM and OMAC versions optionally available
- Support for 128, 192 and 256 bit keys
- Area: 25,000 ASIC gates
- Cores include context memory for rapid context switching (number of contexts is compile-time configurable)
- Flow-through or co-processor data flow formats available.
- 32 bit data interface
- Key expander options to suit the application
- Key memory accessible through separate memory interface
- Test bench and synthesis scripts provided

Applications:

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

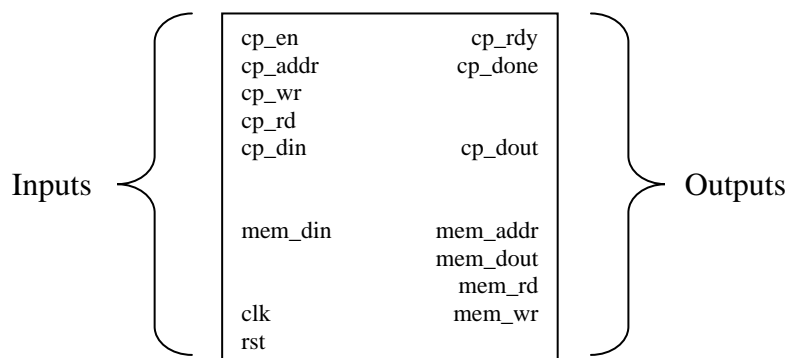


Figure 1 CLP-03 Block Diagram

Pin Description

Signal Name	Width (Bits)	Direction	Description
<i>System Pins</i>			
clk	1	input	System clock. All inputs are sampled on the rising edge of the clock.
rst	1	input	Asynchronous reset. All internal state returns to default value upon assertion (active high) of rst.
<i>Control Processor Interface</i>			
cp_en	1	input	Enable pin for the interface. All other inputs are ignored unless this pin is asserted.
cp_addr	13	input	Address to perform a read or write. This bus must be valid any time cp_wr or cp_rd (qualified with cp_en) are asserted.
cp_wr	1	input	Write signal for the data on cp_din and address on cp_addr.
cp_rd	1	input	Read signal for the address on cp_addr.
cp_din	32	input	Data to write. This bus must be valid any time cp_wr (qualified with cp_en) is asserted.
cp_dout	32	output	Result of a read. The value is qualified with cp_rdy.
cp_rdy	1	output	All control processor accesses to the AES engine are single cycle, so this output is set to a constant high value.
cp_done	1	output	This signal indicates that the encryption has completed. It remains asserted until another encryption operation is started.
<i>Memory Interface</i>			
mem_din	32	input	Result of a read operation. Must be valid one cycle after assertion of mem_rd.
mem_addr	11	output	Address of a read or write cycle. Valid whenever mem_wr or mem_rd is asserted.
mem_dout	32	output	Write value. Valid when mem_wr is asserted.
mem_rd	1	output	Read strobe. The result is expected on mem_din the next cycle.
mem_wr	1	output	Write strobe. The value of mem_dout is written to the address indicated by mem_addr.

Table 1: Pin description table.

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 possibly 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.

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 can also offer a FIFO interface to the core if that is a better integration strategy than the memory interface.

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 low speed key expander which occupies only 1000 ASIC gates but it does require 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 SoC is targeted at.

The CLP-03 is a member of a broad range of AES cores available from Elliptic Semiconductor. On the next page you will find a guide to the cores and performance capabilities:

Name	Throughput (Mbps)	Standard Operating Modes	ASIC Gate Count	Keys Supported
CLP-03	750	ECB, CBC, OFB, CFB	25,000	128, 192, 256
CLP-10	300	CCM	11,000	128
CLP-11	100	ECB	8,000	128, 192, 256
CLP-12	60	CCM, ECB	9,500	128
CLP-14	4000	ECB, CBC, OFB, CFB	41,000	128, 192, 256
CLP-15	40000	GCM	330,000	128
CLP-16	10000	GCM	190,000	128

The CLP-03 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:

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load can be made available under license for evaluation purposes or the core can be made available on the Elliptic evaluation system – the EVAL-01. For more information on pricing and a full data sheet, please contact:

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

Phone: +1 613 254-5456
Fax: +1 613 254-7260
Email: info@ellipticsemi.com