

One of the most popular ciphers in use today is 3DES. 3DES is a variant of the Digital Encryption Standard (DES) cipher improved through the implementation of additional cipher rounds and key mixing. The CLP-02 DES/3DES core combines both algorithms into a single block which is selectable via a mode bit. This core is a robust, proven solution that is in volume production at major foundries.

### Key Features:

- Throughput up to 400 Mbps in 3DES mode
- Area: 10,000 ASIC gates
- Implemented against the FIPS 46-3 standard
- Input memory block is configurable with shadow memory to allow input of next block while DES operation in progress
- Automatic generation of key context from key data
- Key memory accessible through memory interface
- Key memory sized to support 3-Key 3DES modes
- Flow-through or co-processor data flow
- Electronic Codebook (ECB) or Cipher Block Chaining (CBC) modes
- Test bench provided

### Applications:

- IPSec designs in residential gateways, multi-service access products
- Storage – SAN/NAS applications
- Military communications systems
- Secure video surveillance
- Secure audio communications

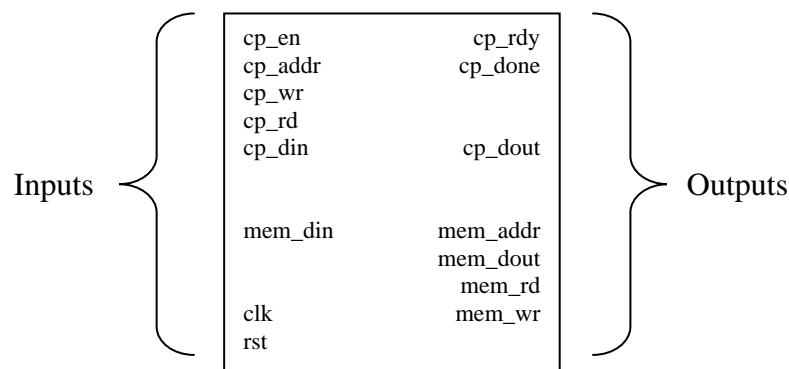


Figure 1 3DES Core Pin Diagram

## 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 CLP-02 are single cycle, so this output is set to a constant high.
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	-	output	Address of a read or write cycle. Valid whenever mem_wr or mem_rd is asserted. The width of this port is configurable at build time.
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 CLP-02 DES/3DES core combines both algorithms into a single block which is selectable via a mode bit. The core supports either Electronic Code Book (ECB) or Cipher Block Chaining (CBC) modes of operation. The DES context consists of a single 64 bit key and a 64 bit initialization vector (IV). The 3-DES context consists of three 64 bit keys and a 64 bit IV. The IV is only used for DES when it is operating in CBC mode. The context is accessed through the control processor port on the core.

The CLP-02 has two major interfaces - 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 encrypted or decrypted.

The CLP-02 supports a number of configuration options and operations. These are:

- DES or 3DES operation
- Electronic Codebook (ECB) or Cipher Block Chaining (CBC) modes
- Flush request – clears internal states, plain-text memory, cipher memory and key contexts
- Encrypt or decrypt mode
- Swap request between main and shadow memory blocks
- Flow-through or co-processor mode
- 2 or 3 key 3DES mode
- Start/finish signals triggers encryption and signals completion.

The CLP-02 is available in soft IP form, either as a Netlist or HDL Source. The deliverables available are:

### Netlist Licenses:

- Post synthesis EDIF netlist
- Testbench
- Simulation script
- Documentation

### HDL Source Licenses:

- HDL
- Testbench
- Synthesis script
- Documentation

An FPGA load can be made available under license for evaluation purposes. 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](mailto:info@ellipticsemi.com)