

Features

- Throughput over 1300 Mbps in 3DES mode
- Electronic Codebook (ECB) or Cipher Block Chaining (CBC) modes
- Implemented against the FIPS 46-3 standard
- Input memory block is configurable with shadow memory to allow input of next block while 3DES/DES operation in progress
- Automatic generation of key context from key data
- Key memory accessible through memory interface
- Key memory sized to support up to 3-Key 3DES modes
- Shared memory interface or optional FIFO interfaces available

Applications

- IPsec designs in routers, switches, firewalls and network appliances
- Storage – SAN/NAS applications
- Military communications systems

One of the most popular ciphers in use today is 3DES. 3DES is a variant of the Digital Encryption Standard (DES) cipher.

The CLP-19 is an improved design through the implementation of timing and state machine optimizations to achieve throughput 30% greater than the CLP-08 core. The CLP-19 DES/3DES core combines both algorithms into a single block which is selectable via a mode bit.

General Description

The CLP-19 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 two or three 64 bit keys and a 64 bit IV. The IV is only used for DES/3DES when it is operating in CBC mode. The context is accessed through the control processor port on the core.

The CLP-19 is a high throughput optimization of the CLP-08 design. This requires modestly more gates but offers the opportunity to build Gigabit throughput IPsec router or switch blades and VPN appliances.

The CLP-19 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-19 supports a number of configuration options and operations. These are:

- DES or 3DES operation
- Electronic Codebook (ECB) or Cipher Block Chaining (CBC) modes
- 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.

Elliptic offers a variety of SoC interfaces tailored to the architecture chosen by the designer. This includes the shared memory interfaces documented in this data sheet, FIFOs or standard SoC bus interfaces.

Core Implementation	Operating Mode	Max Clk Frequency (MHz)	Throughput@ Max Clk Freq (bits/sec)	ASIC Gate Count (NAND2 Equivalent Gates) @ 100MHz
High-Performance	ECB only	250	1.3 G	13.3
	ECB/CBC	246	1.3 G	16.4



Embedded security you can trust

Ultra-High Throughput DES/3DES Core 1.3Gbps

CLP-19 Product Brief

The CLP-19 is a member of a family DES Cores.

In addition, Elliptic offers a broad range of security cores including random number generators, hashing cores and public key acceleration supporting both RSA and Elliptic Curve operations that can be used for storage security and other applications such as virtual private networks, digital rights management and wireless security.

Other Products of the Family of DES Cores

- CLP-02: DES/3DES Core
- CLP-08: High Throughput DES/3DES Core – 1+Gbps
- CLP-19: Ultra-High Throughput DES/3DES Core – 1.3 Gbps

Availability

- The CLP-19 is available in soft IP form HDL Source. The deliverables available are:

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script & constraints
- Sample simulation script
- Documentation