

### Features

- Implements 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
- Electronic Codebook (ECB) or Cipher Block Chaining (CBC) modes

### Applications

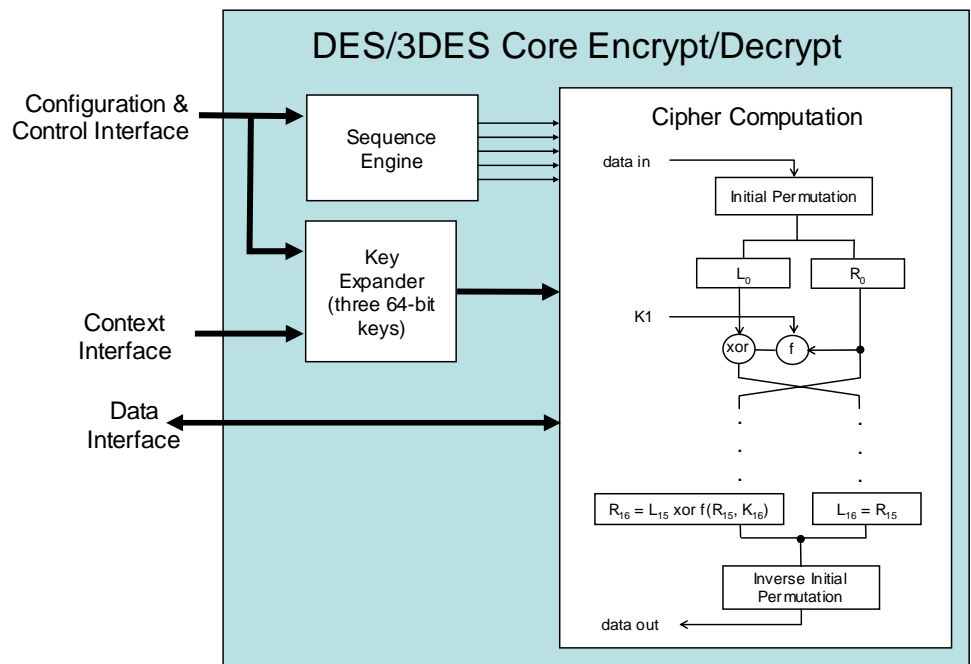
- IPSec designs in residential gateways, multi-service access products
- Storage – SAN/NAS applications
- Military communications systems

*One of the most popular ciphers in use today is 3DES. 3DES is a variant of the Digital Encryption Standard (DES) cipher improved through the implementation of additional cipher rounds and key mixing. The CLP-02f 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.*

### General Description

The CLP-02f DES/3DES core combines both algorithms into a single block which is selectable via a mode bit. The core supports both Electronic Code Book (ECB) and 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 (3)DES when it is operating in CBC mode. The context is accessed through the control processor port on the core.

The CLP-02f 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.



### General Description cont'

The following table outlines the resource utilization and performance achieved by the CLP-02 in target Lattice FPGAs.

| Lattice FPGA     | Resource Requirement (Slices) | Maximum Clock (MHz) | Throughput at Max. Clock (Mbps) |
|------------------|-------------------------------|---------------------|---------------------------------|
| ECP-DSP ECP33E05 | 1199                          | 87                  | 95                              |
| XPLFXP20E-5      | 1198                          | 87                  | 95                              |

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

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

The CLP-02f 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 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-02f is available in soft IP form as a Netlist. The deliverables available are:

### Netlist Licenses

- EDIF netlist
- Testbench
- Simulation script
- Documentation