

The CLP-34 implements the AES key wrap algorithm as specified by NIST. This standard has also been reflected in the IETF RFC 3394 and other applications. The CLP-34 implements the key wrap algorithm based upon the production proven CLP-03 AES core. Key wrap is used to encrypt sensitive key information into key blobs which can then be safely stored in Flash memory or on disk for disk, RAID and tape applications.

Key Features:

- Configurable core starting at 16,000 ASIC gates
- Support both key wrap (encryption) and key unwrap (decryption)
- Includes key expansion logic
- Support for 128 and 256 bit AES key encryption keys
- Flow through design
- No external memory required

Application:

- Disk/storage and RAID key wrap
- Tape key wrap
- Digital Rights Management

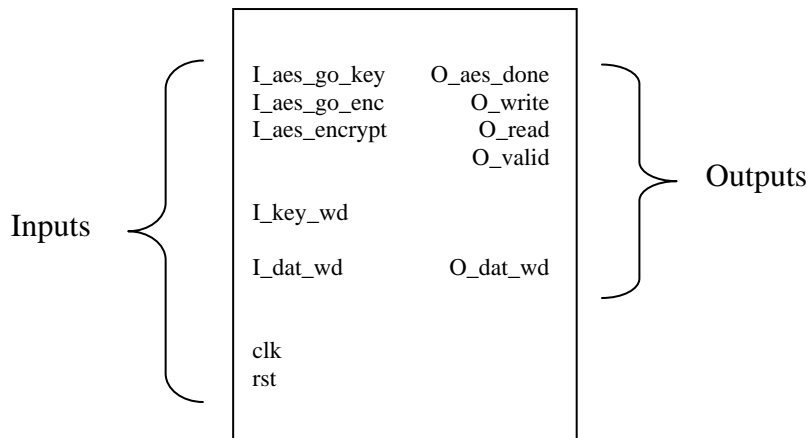


Figure 1 CLP-34 Block Diagram

General Description

NIST has specified a cryptographic algorithm called Key Wrap that uses the Advanced Encryption Standard (AES) to securely encrypt plaintext keys together with associated integrity data for secure storage of sensitive key information in external memory such as Flash, disk or tape storage devices. The algorithm operates on blocks of 64 bits, therefore before being wrapped, the key data is parsed into n blocks of 64 bits. The only restriction the key wrap algorithm places on n is that n must be at least two. $4n$ will therefore support all three AES key sizes (128, 192 or 256 bits). However, other cryptographic values often need to be wrapped such as the seed of the random number generator for a FIPS 186 digital signature standard (DSS) implementation. As such, no upper bound exists for n to provide an extensible design adaptable to any key wrap application.

The CLP-34 implements the AES algorithm required in NIST key wrap applications. It can be matched with Ellipsys middleware or a hardware solution to implement the entire key wrap algorithm depending on the performance requirement. The CLP-34 offers two KEK options – 128 bit and 256 bits. The table below indicates the performance and gate count requirement available as build time options for the CLP-34:

Core Option	Gate Count	Maximum Frequency	Throughput
Compact	16,000	350 MHz	122K wraps/s
Hi-Speed	25,000	350 MHz	484K wraps/s

Note: 1. Maximum frequency for 90 nm LVOD

The CLP-34 is available in soft IP form, either as a Netlist or HDL Source. The deliverables include:

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 or the core can be made available on either of Elliptic's evaluation systems – the EVAL-01 or the EVAL-02. For more information on pricing and a full data sheet, 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