

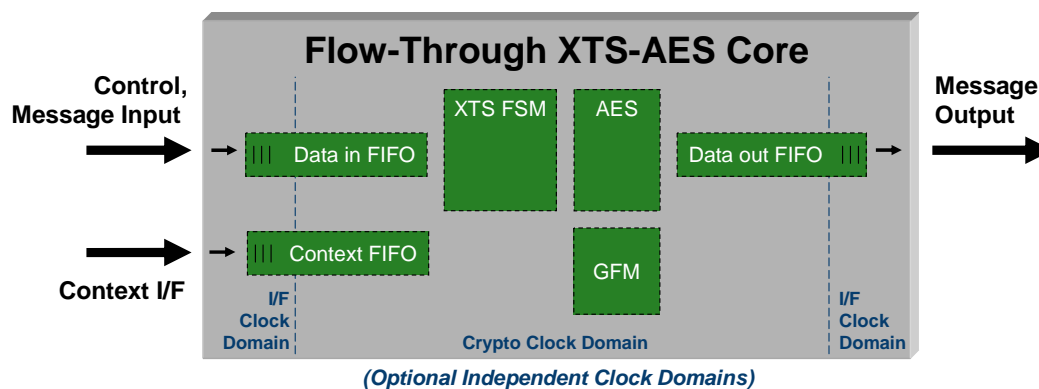
The IEEE has developed two new security standards for ‘data at rest’ in disk and tape storage applications. As a replacement for the AES-LRW algorithm, the IEEE Std 1619-2007 committee selected a new tweakable narrow-block cipher designated as XTS-AES. XTS stands for the XEX-based Tweaked CodeBook mode (TCB) with CipherText Stealing algorithm.

### Key Features:

- Throughput up to 10 Gbps for SAS-G1 through G3 and Fibre Channel applications
  - Scalable throughput up to 40 Gbps also available
- Implements XTS-AES (also referred to as AES-XTS) as specified in IEEE Std 1619-2007
- Fully compliant with IEEE Std 1619-2007, with optional support for ciphertext stealing (CTS) mode
- Support for 2 key sizes for the AES core – 128 and 256 bits
- Gate count of 132K ASIC gates
- Test bench and sample synthesis scripts provided

### Application:

- Disk/storage and RAID encryption
  - Serial Attached SCSI (G1 through G3)
  - Fibre Channel (all currently defined traffic rates)



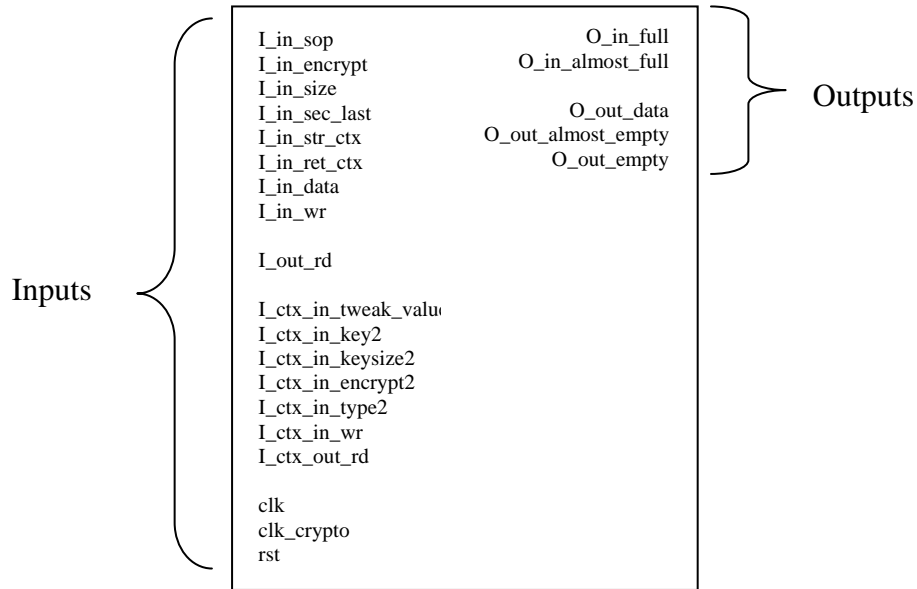


Figure 1 CLP-35 Block Diagram

### Pin Description

Signal Name	Direction	Bit Width	Description
<i>System Pins</i>			
clk	Input	1	Synchronous clock input. All I/O signals except rst are referenced to the rising clk.
clk_crypto	Input	1	Synchronous clock input for the internal crypto XTS-AES core.
rst	Input	1	Active high, asynchronous reset input.
<i>Data Ingress FIFO</i>			
I_in_sop	Input	1	Indicates the beginning of the data unit or data unit segment to be processed.
I_in_encrypt	Input	1	Selects encrypt/decrypt mode.

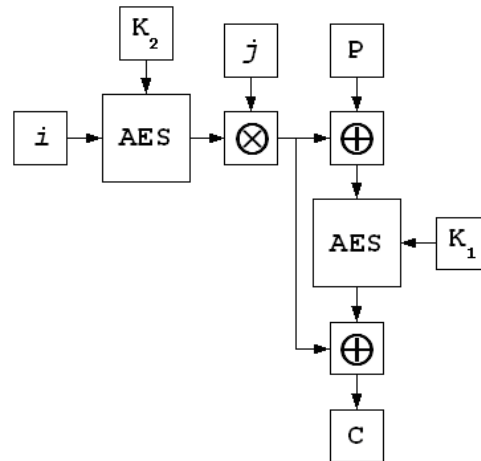
Signal Name	Direction	Bit Width	Description
I_in_size	Input	4	Indicates the number of bytes that are valid in the 16-byte word. (CTS mode only)
I_in_sec_last	Input	1	Indicates when the second last block of data is available. (CTS mode only)
I_in_str_ctx	Input	1	Indicates that the intermediate context data (T) has to be loaded into the context store FIFO.
I_in_ret_ctx	Input	1	Indicates that data to be processed re-uses the context.
I_in_data	Input	128	Data to be processed (encrypted/decrypted).
I_in_wr	Input	1	Push the value of I_in_data, I_in_sop, I_in_encrypt, I_in_size, I_in_two_last, I_in_str_ctx, I_in_ret_ctx onto the ingress FIFO.
O_in_full	Output	1	Indicates that the ingress FIFO is full.
O_in_almost_full	Output	1	Indicates that the ingress FIFO can only accept one more write before filling.
<b>Data Egress FIFO</b>			
O_out_data	Output	128	Processed data. Byte ordering is big endian within the word.
I_out_rd	Input	1	Pop a value from the egress FIFO.
O_out_almost_empty	Output	1	Indicates that the egress FIFO can only accept one more read before emptying.
O_out_empty	Output	1	Indicates that the egress FIFO is empty.

Signal Name	Direction	Bit Width	Description
<b>Context Load FIFO</b>			
I_ctx_in_tweak_value2	Input	128	Input tweak value or intermediate tweak if context is reused.
I_ctx_in_key2	Input	256	If context is not reused: XTS-AES Key2 in the first FIFO word, and XTS-AES Key 1 in the second FIFO word. For context reuse: XTS-AES Key1 (only one FIFO word required)
I_ctx_in_keysize2	Input	1	XTS-AES Key1/Key2 size
I_ctx_in_encrypt2	Input	1	Selects encrypt/decrypt mode for loading the key
I_ctx_in_type2	Input	1	Indicates whether the context is one or two words.
I_ctx_in_wr	Input	1	Push the value of I_ctx_in_tweak_value, I_ctx_in_keysize and I_ctx_in_key onto the context load FIFO.
O_ctx_in_full	Output	1	Indicates that the context load FIFO is full.
O_ctx_in_almost_full	Output	1	Indicates that the context load FIFO can only accept one more write before filling.

**Table 1: Pin Description Table**

## General Description

Recent loss of personal data on disk and tape drives has resulted in tough legislation, fines and other remedies for this breach of confidentiality. This has in turn generated renewed interest in storage security. The IEEE is drafting two new standards aimed at storage security – the IEEE Std 1619-2007 for disk encryption and the IEEE Std 1619.1-2007 standard for tape encryption. The 1619 committee has agreed to adopt a new cipher called XTS-AES for 1619-2007 which is a Tweakable Narrow-block Encryption algorithm. The authors of the algorithm have indicated to the IEEE that they will not



assert their patent rights to the design for developers implementing XTS-AES in storage security applications.

Encrypted data at rest is subject to unique attacks. Foremost among these is the cut and paste attack which occurs when a hacker substitutes ciphertext on a disk which when decrypted would serve the needs of the hacker, i.e. by substituting personal or commercial information to modify important records such as salaries or other financial information. In addition, the standard implements a security design which does not result in an increase in record size as is commonly found with security designs that include message authentication fields or initialization vectors. Disk encryption also requires a cipher which can scale to very high throughput to satisfy the needs of high performance RAID applications. The CLP-35 is capable of supporting up to 10 Gb/s of throughput, which is suitable for SATA, SAS and Fibre Channel disk drive interfaces. Other variants of Elliptic’s XTS-AES solutions can scale up to 40 Gb/s of throughput in advanced processes using high speed libraries and memories; contact Elliptic for details.

The tweakable block cipher implemented in the CLP-35 is called a Tweak-Encrypt-Tweak algorithm. The algorithm is shown in Figure 2 below.

**Figure 2 XTS-AES Flow Diagram**

Note that a “key” in the XTS-AES context is 256 or 512 bits, and is composed of two 128-bit or 256-bit AES-sized keys which are referred to as Key<sub>1</sub> and Key<sub>2</sub>, respectively, in the 1619 standard.

The standard release also includes a concept called ciphertext stealing (CTS). This mode of operation removes the need for padding and was added to permit support for common disk sector sizes that are not integer multiples of the block size used in the AES cipher

while maintaining transparent encryption (identical amounts of plaintext and ciphertext). The disk sector sizes frequently chosen for disk systems are 512 and 4096, with optional 8 or 16 byte Data Integrity Fields (DIF). The 8 byte DIFs lead to 520 and 4104 byte sector sizes that require CTS. The CTS algorithm is accomplished by padding the last block with the low order bits from the second to last ciphertext block (stealing the ciphertext from the second to last block). The last block is encrypted, and then exchanged with the second to last ciphertext block, which is then truncated to the length of the final plaintext block (thus removing the bits that were stolen), resulting in ciphertext of the same length as the original message size.

The CLP-35 is a member of a family of storage security solutions available from Elliptic spanning both disk and tape encryption as specified in IEEE Std 1619-2007 and Std 1619.1-2007. 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.

The CLP-35 is available in soft IP form, either as a Netlist or HDL Source. The deliverable available are:

**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 the Elliptic evaluation system – the ELP-01. 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](mailto:info@ellipticsemi.com)