

The IEEE is developing two new security standards for ‘data at rest’ in disk and tape storage applications. As a replacement for the AES-LRW algorithm, the IEEE 1619 committee is now set to standardize on a new tweakable narrow-block cipher designated as XTS-AES.

Key Features:

- Throughput up to 3 Gbps for SATA applications
 - Scalable throughput up to 30 Gbps also available
- Implements XTS-AES (also referred to as AES-XTS) as specified in draft IEEE standard P1619D17
- Fully compliant with P1619D17, with optional support for ciphertext stealing (CTS) mode
- Support for 2 key sizes for the AES core – 128 and 256 bits
- Gate count of 53K ASIC gates
- Test bench and sample synthesis scripts provided

Application:

- Disk/storage and RAID encryption

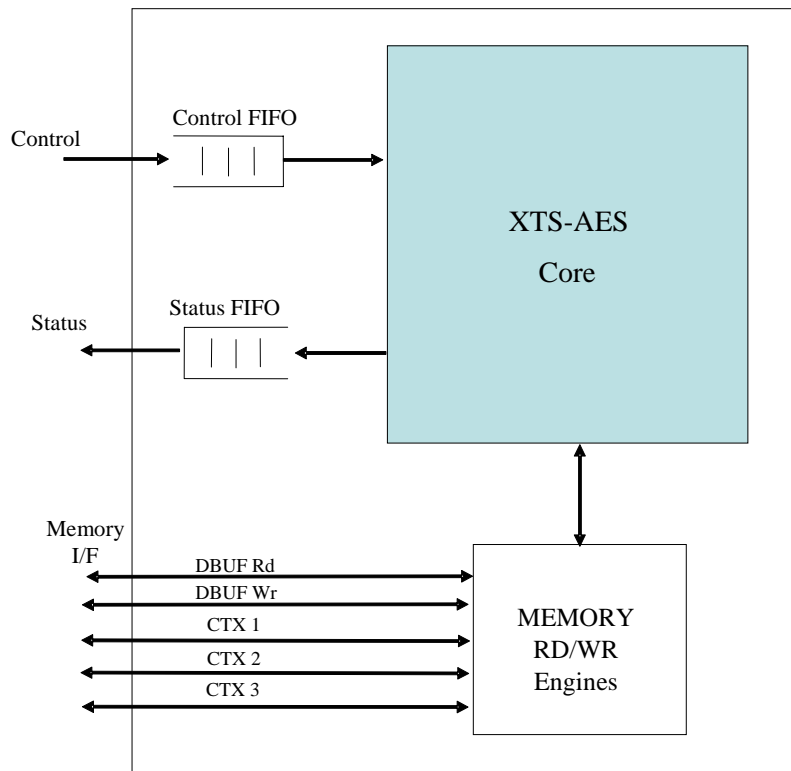


Figure 1 CLP-33 Block Diagram

Pin Description

Signal Name	Bit Width	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. Internal state returns to default value upon assertion (active high).
<i>FIFO Control pins</i>			
I_ctrl_fifo_push	1	input	Writes a word into the FIFO.
I_ctrl_fifo_data	configurable	input	Data word to write to FIFO.
O_ctrl_fifo_full	1	output	Indicates that the FIFO is full. Data must not be written to the FIFO when this signal is asserted.
<i>FIFO Status pins</i>			
I_status_fifo_pop	1	input	Pops a word of the status FIFO. The word will be available the next clock cycle.
O_status	1	output	Data returned from the status FIFO. The status bit is always set to 1.
O_status_fifo_empty	1	output	Indicates that the status FIFO is empty. Reading from the FIFO when this signal is asserted is not permitted.
<i>Data Buffer Read pins</i>			
O_rddbuf_en	1	output	Enable pin for the DBUF Rd memory interface. All other inputs for this memory are ignored unless this pin is asserted.
O_rddbuf_rd	1	output	Read enable signal to read data I_rddbuf_data from address O_rddbuf_addr.
O_rddbuf_addr	configurable	output	Address to perform a read. This bus is valid any time O_rddbuf_rd qualified with O_rddbuf_en is asserted.
I_rddbuf_data	128	input	Input data bus, result of a read.
<i>Data Buffer Write pins</i>			
O_wrdbuf_en	1	output	Enable pin for the DBUF Wr memory interface. All other inputs for this memory are ignored unless this pin is asserted.
O_wrdbuf_wr	1	output	Write enable signal to write data O_wrdbuf_data to address O_wrdbuf_addr.

Signal Name	Bit Width	Direction	Description
O_wrdbuf_addr	configurable	output	Address to perform a write. This bus is valid any time O_wrdbuf_wr qualified with O_wrdbuf_en is asserted.
O_wrdbuf_data	128	output	Output data bus for data to be written into memory.
<i>Context 1 (Key₁) Memory Interface pins</i>			
O_ctx1_en	1	output	Enable pin for the CTX1 memory interface. All other inputs for this memory are ignored unless this pin is asserted.
O_ctx1_rd	1	output	Read enable signal to read data I_ctx1_data from address O_ctx1_addr.
O_ctx1_addr	configurable	output	Address to perform a read. This bus is valid any time O_ctx1_rd qualified with O_ctx1_en is asserted.
I_ctx1_data	128	input	Input data bus, result of a read.
<i>Context 2 (Key₂) Memory Interface pins</i>			
O_ctx2_en	1	output	Enable pin for the CTX2 memory interface. All other inputs for this memory are ignored unless this pin is asserted.
O_ctx2_rd	1	output	Read enable signal to read data I_ctx2_data from address O_ctx2_addr.
O_ctx2_addr	configurable	output	Address to perform a read. This bus is valid any time O_ctx2_rd qualified with O_ctx2_en is asserted.
I_ctx2_data	128	input	Input data bus, result of a read.
<i>Context 3 (Logical Position Index) Memory Interface pins</i>			
O_ctx3_en	1	output	Enable pin for the CTX3 memory interface. All other inputs for this memory are ignored unless this pin is asserted.
O_ctx3_rd	1	output	Read enable signal to read data I_ctx3_data from address O_ctx3_addr.
O_ctx3_addr	configurable	output	Address to perform a read. This bus is valid any time O_ctx3_rd qualified with O_ctx3_en is asserted.
I_ctx3_data	128	input	Input data bus, result of a read.

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 P1619D17 draft standard for disk encryption and the P1619.1 draft standard for tape encryption. The P1619 committee has agreed to adopt a new cipher called XTS-AES 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 P1619 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-33 is capable of supporting up to 3 Gb/s of throughput, which is suitable for SATA disk drive interfaces. Other variants of Elliptic’s XTS-AES solutions can scale up to 70 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-33 is called a Tweak-Encrypt-Tweak algorithm. The algorithm is shown in Figure 2 below.

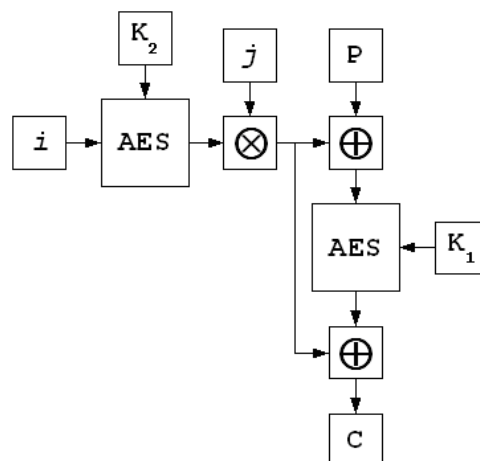


Figure 2 XTS-AES Flow Diagram

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 Key₁ and Key₂, respectively, in the P1619D17 standard.

The draft standard release D17 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, 520, 528 and 4096 bytes and as such 520 and 528 byte sector sizes required 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-33 is a member of a family of storage security solutions available from Elliptic spanning both disk and tape encryption as specified in draft IEEE standards P1619 and P1619.1. 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-33 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