BERTEN
Secure Communications

AEST-X256 IP Cores

AES-XTS Crypto Engine

High-Performance and Balanced Versions

Register-based Configuration

Ciphertext Stealing (CTS)

Features

- XTS and ECB Modes
- FPGA Performance up to 110 Gbps
- Minimum Area Version
- Ultra-Low Latency
- 128- and 256-bit Key Sizes
- FIPS 197, FIPS 140-3 Compliant
- NIST 800-38E Compliant
- IEEE 1619 Compliant
- Portable to any FPGA or ASIC
- AMBA AXI Interfaces

Applications

- Full Disk Encryption (FDE)
- Data Confidentiality
- NVMe SSD Storage Protection
- SATA, PCIe, Gigabit Ethernet
- Secure UFC, SD, eMMC Memories
- Data-at-Rest Encryption

AEST-X256 is a family of IP Cores for hardware offloading of AES-XTS disk encryption in FPGA, SoC, and ASIC technologies.

The engine also supports the ECB (Electronic Codebook) mode for data encryption and decryption. Ciphertext Stealing (CTS) is available to allow arbitrary-length inputs.

Three AEST-X256 implementations are available to trade off area and performance: Balanced, High-Speed, and Ultra High-Speed. All of them feature end-to-end latencies between 17 and 25 clock cycles.

Portable to any AMD (Xilinx), Intel (Altera), or Microchip (Microsemi) device, the AEST-X256 is compliant with NIST 800-38E, FIPS 197, IEEE 1619-2018, and FIPS 140-3 standards.

The IP Cores include AMBA AXI interfaces and a user-programmable register map to configure the key size and mode of operation. ANSI C drivers are provided for a fast integration into the target platform.

© BERTEN DSP S.L.

www.bertendsp.com sales@bertendsp.com +34 942 18 10 11

Resources

		AEST-B256 Balanced			AEST-H256 High-Speed			AEST-U256 Ultra High-Speed		
		LUT	Register	BRAM	LUT	Register	BRAM	LUT	Register	BRAM
AMD / Xilinx	7 Series	4.5K	5.0K	8 RAMB36	19.7K	7.1K	56 RAMB36	37.6K	10.8K	112 RAMB36
	Ultrascale	4.4K	5.0K	8 RAMB36	19.6K	7.1K	56 RAMB36	37.5K	10.8K	112 RAMB36
	Ultrascale+	4.4K	5.0K	8 RAMB36	19.6K	7.1K	56 RAMB36	37.5K	10.8K	112 RAMB36
	Versal ACAP	4.5K	5.0K	8 RAMB36	20.3K	7.0K	56 RAMB36	38.5K	10.6K	112 RAMB36
Intel / Altera	MAX 10, Cyclone 10 LP	9.5K^{LE}	6.0K	16 M9K	78.2K^{LE}	6.6K	120 M9K	-	-	-
	Cyclone V	4.1K^{ALM}	6.1K	16 M10K	20.9K^{ALM}	8.4K	112 M10K	40.5K^{ALM}	13.6K	224 M10K
	Arria 10	3.8K^{ALM}	6.1K	16 M20K	20.7K^{ALM}	8.4K	112 M20K	40.7K^{ALM}	13.8K	224 M20K
	Stratix V	4.0K^{ALM}	6.1K	16 M20K	20.7K^{ALM}	8.5K	112 M20K	10.5K^{ALM}	13.9K	224 M20K

Modes of Operation

The AEST-X256 family of IP Cores provides low-latency AES encryption in three implementations to trade off resource utilisation and throughput.

The engine includes a Control Unit to manage the block cipher according to the following NIST SP 800-38 modes of operation:

- **XTS**: encrypts or decrypts XORing the user data with an internally generated value derived from the tweak, both at the cipher input and output.
- **ECB**: encrypts or decrypts input data with the AES cipher to generate a ciphertext or a plaintext. Based on the ECB, other modes of operation may be implemented (e.g., CBC, CFB, OFB).

Clock, MHz	Performance, Gbps		
	AEST-B256	AEST-H256	AEST-U256
150	1.4	19	38
300	2.7	38	76
435	-	55	111

Interfaces

The IP Cores implement four AXI4-Stream interfaces for Tweak and Key configuration, and transfer of Input/Output Data. One AXI4-Lite provides access to the register map to configure the key size, mode of operation, and zeroisation.

An input port is used to select encryption or decryption for each message. A Status port is available for event notification.

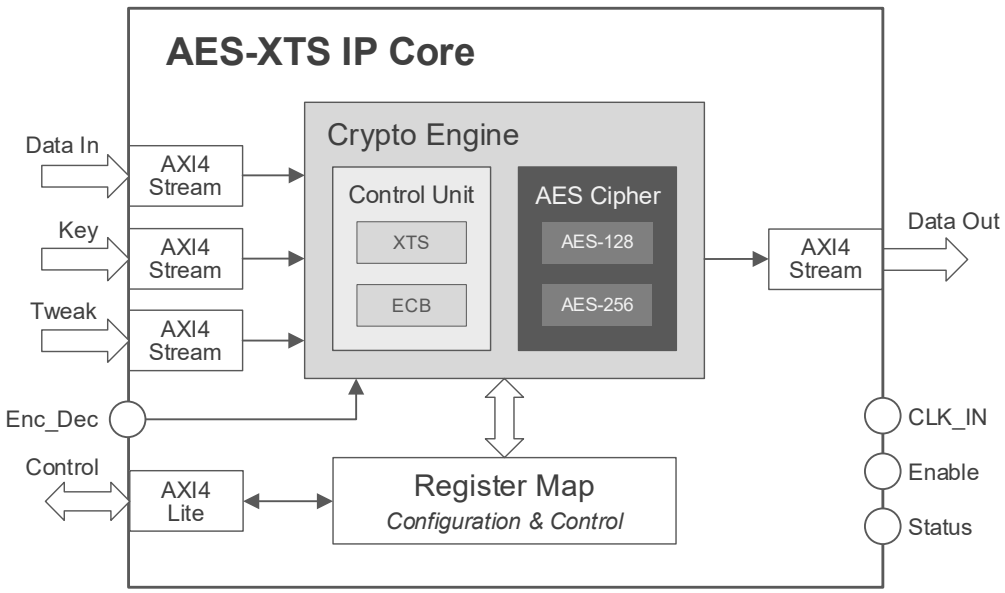
Licensing

Each IP Core is provided as encrypted netlist for one device family, under a perpetual Site Licence. It includes 12 months of maintenance and integration support into the target platform.

Export Classification: 5D002.c.1 / 5A002.a.1.

Deliverables

- Targeted, timing closed Netlist
- Design Constraints
- Simulation Model
- User Manual
- ANSI C drivers



© BERTEN DSP S.L.
www.bertendsp.com sales@bertendsp.com +34 942 18 10 11