BERTEN
Secure Communications

AESG-X256 IP Cores

AES-GCM Crypto Engine

High-Performance and Balanced Versions
GCM/GMAC, CTR, and ECB Modes
Register-based Configuration

Features

- GCM/GMAC, CTR, ECB Modes
- FPGA Performance up to 110 Gbps
- Minimum Area Version
- Ultra-Low Latency
- 128- and 256-bit Key Sizes
- Configurable Tag Length
- FIPS 197, FIPS 140-3 Compliant
- NIST 800-38A, 800-38D Compliant
- Portable to any FPGA or ASIC
- AMBA AXI Interfaces

Applications

- Data-in-Transit Encryption
- Network Security: MACsec, IPsec
- Transport Protocols: TLS, SSL
- Gigabit Ethernet, PCIe
- Fiber Security Protocol (FC-SP)
- Data Confidentiality
- Secure Communications
- Electronic Transactions

AESG-X256 is a family of IP Cores for hardware offloading of AES-GCM (Galois/Counter Mode) authenticated encryption in FPGA, SoC, and ASIC technologies.

The AES engine also supports CTR (Counter) and ECB (Electronic Codebook) confidentiality modes of operation for data encryption, and GMAC (Galois Message Authentication Code) for authentication.

Three AESG-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 14 and 28 clock cycles.

Portable to any AMD (Xilinx), Intel (Altera), or Microchip (Microsemi) device, the AESG-X256 is compliant with NIST 800-38A, 800-38D, FIPS 197, and FIPS 140-3 standards.

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

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

Resources

		AESG-B256 Balanced			AESG-H256 High-Speed			AESG-U256 Ultra High-Speed		
		LUT	Register	BRAM	LUT	Register	BRAM	LUT	Register	BRAM
AMD / Xilinx	7 Series	3.6K	2.6K	4 RAMB36	14.1K	8.9K	36 RAMB36	28.1K	15.2K	72 RAMB36
	Ultrascale	3.5K	2.6K	4 RAMB36	13.9K	8.9K	36 RAMB36	28.0K	15.2K	72 RAMB36
	Ultrascale+	3.5K	2.6K	4 RAMB36	13.9K	8.9K	36 RAMB36	28.0K	15.2K	72 RAMB36
	Versal ACAP	3.2K	2.6K	4 RAMB36	13.3K	8.8K	36 RAMB36	27.9K	15.2K	72 RAMB36
Intel / Altera	MAX 10, Cyclone 10 LP	6.7K	2.7K	8 M9K	40.5K	8.4K	80 M9K	81.0K	14.5K	160 M9K
	Cyclone V	3.3K	2.7K	8 M10K	15.0K	8.4K	72 M10K	30.5K	15.0K	144 M10K
	Arria 10	3.3K	2.7K	8 M20K	15.0K	8.4K	72 M20K	30.3K	15.0K	144 M20K
	Stratix V	3.3K	2.7K	8 M20K	15.0K	8.4K	72 M20K	30.3K	15.0K	144 M20K

Modes of Operation

The AESG-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 parallel execution of the block cipher and the GHASH Authentication module. It supports the following NIST SP 800-38 modes:

- **GCM/GMAC**: provides Authenticated Encryption and Decryption with Associated Data (AEAD). GMAC is applied when all the bytes in a message are labelled as Additional Authenticated Data (AAD).
- **CTR**: encrypts and decrypts XORing the input data blocks with a pseudorandom sequence internally generated with the AES cipher.
- **ECB**: encrypts input data with the AES cipher to generate a ciphertext.

Other modes of operation may be implemented based on the AESG-X256 engine:

- **CFB, OFB**: chaining modes using the ECB encryptor.
- **CCM, EAX**: using the CTR encryptor and decryptor.

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

Interfaces

The IP Cores implement six AXI4-Stream interfaces for Initialisation Vector and Key configuration, and transfer of Input/Output Data and Tag.

One AXI4-Lite provides access to the register map to configure the key size, mode of operation, authentication tag length, zeroisation, and AAD forwarding.

An input port is used to select encryption or decryption for each message. Status and Tag Verification ports are also available for events and tag validity notifications.

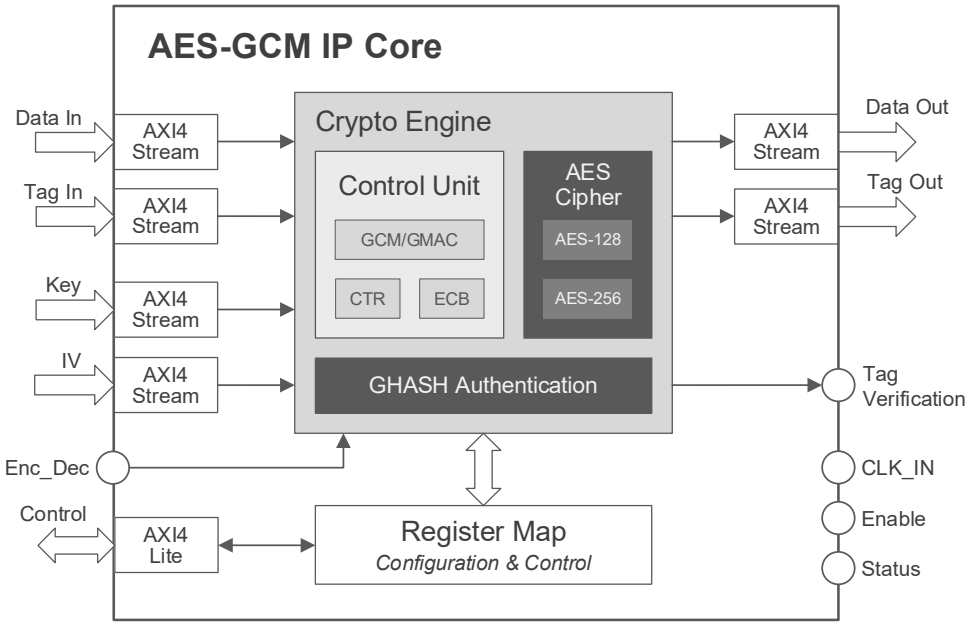
Licensing

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



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