BarcoSilex

AES-GCM 10 to 100 Gbps

BA415
Product sheet

The BA415 is a scalable implementation of the AES-GCM algorithm compliant with the NIST SP 800-38D standard. The unique architecture enables high throughput from 10 Gbps to 100 Gbps while maintaining an optimal resource usage.

The scalability of the IP enables to find a trade-off between resources, performance and technology. It is easily portable to ASIC and FPGA (Xilinx, Altera) technologies. The BA415 addresses a wide range of networking applications where security is a concern.

General Description

The AES-GCM (Galois Counter Mode) is an authenticated encryption algorithm which combines the AES counter mode for encryption and the Galois field multiplier for the authentication. The encryption and authentication occur in parallel to enable high throughput. Part of the data, such as the protocol header, may only be authenticated as it is done for MACsec.

The AES-GCM is the only authenticated encryption algorithm recommended by NIST enabling very high throughput. The GCM cipher mode is well suited to secure high speed communication channels and referenced in several standards such as MACsec (IEEE 802.1A), Fiber Channel Security Protocol (FC-SP), IPsec.

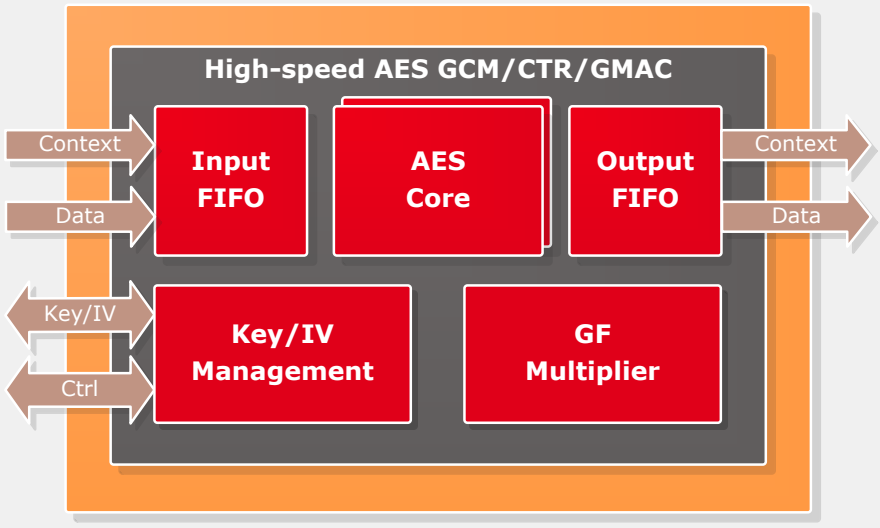

Figure 1: High-speed AES-GCM/CTR/GMAC block diagram

Features

- Scalable architecture from 10 to 100 Gbps
- Guaranteed performance with small packets
- Packet-based context and key switching without penalty in performance
- 128-bit and 256-bit key
- NIST SP 800-38D compliant
- Full AES-GCM, including key expansion
- Low latency
- Best trade-off between area and performance
- Straight forward integration with simple FIFO interfaces.
- Portable to any FPGA and ASIC technology

Applications

- MACsec/IPsec
- Optical transport
- Broadband access
- Storage

Implementation aspects

The unique architecture enables high level of flexibility. The throughput and features requested will be taken into account in order to select the most optimal configuration.

The BA415 AES-GCM includes key management and context switching. The optimized context switching enables handling of multiple virtual streams of data within a single core. The key can be selected for each packet independently. The advanced pipelined architecture of the AES-GCM core enables small data packets to be processed without penalty on performance.

Resource usage example

The following table indicates the resource usage for some specific configuration (128-bit key with key expansion) and target devices. Other figures are available on request.

Configuration	Target technology	Resource
40 Gbps	Xilinx Kintex-7	5120 slices
40 Gbps	Altera Arria V	10224 ALM
100 Gbps	Xilinx Virtex-7	14172 slices
100 Gbps	Altera Stratix V	33200 ALM

Table 1: Implementation figures

Deliverables

- Netlist or RTL
- Scripts for implementations
- Self-checking test-bench based on FIPS vectors
- Documentation (datasheet, integration guide…)

Similar products

- **BA411E-FLEX** AES core for low/medium throughput and multiple cipher modes.
- **BA411E-CCM** AES core with CCM mode (Counter with CBC-MAC).
- **BA411E-XTS** AES-XTS for multi-Gbps applications.

About Barco Silex

Barco Silex is an electronic design house (ASICs, FPGAs, DSP, boards, embedded SW) specialized in video compression, security and memory controllers. Barco Silex offers the best guarantee for continuous support throughout the complete lifecycle of products.

For more information, please contact us.

Barco Silex SA
Rue du Bosquet, 7
1348 Louvain-la-Neuve
Belgium

Website www.barco-silex.com
Email barco-silex@barco.com
Phone +32 (0) 10 454 904