SILEX INSIGHT

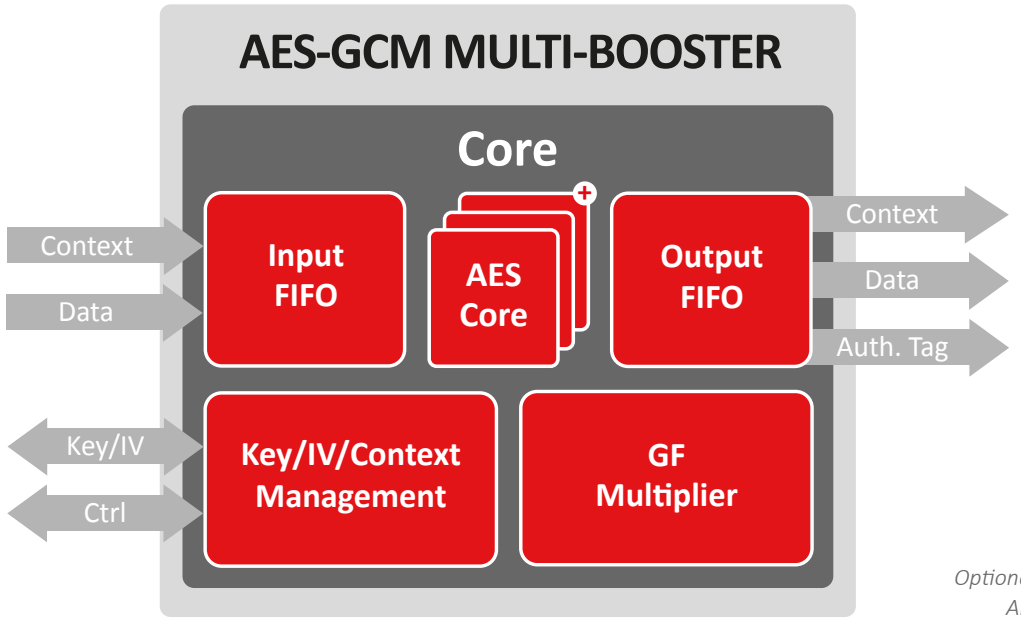
Product sheet
BA415

AES-GCM MULTI-BOOSTER

The AES-GCM Multi-Booster crypto engine is a scalable implementation of the AES-GCM algorithm compliant with the NIST SP 800-38D standard. The unique architecture enables high throughput while maintaining an optimal resource usage.

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.



Optionally support of both AES and SM4 ciphers

Features

- ASIC & FPGA
- High throughput:
  - ASIC: 2Tbps
  - FPGA: 100 Gbps
- Guaranteed performance with small packets
- Flexible datapath width (from 128 to 2048-bits)
- 128-bit and 256-bit key
- NIST SP 800-38D compliant
- Scalable solution
- Can be provided with AXI DMA & software
- Masking with excellent protection against SPA & DPA
- Context switching & management
- Low latency
- Best trade-off between area and performance
- Straight forward integration with simple FIFO interfaces

Applications

- MACsec/IPsec/TLS
- Optical transport
- Broadband access
- WPA3 support

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. It is easily portable to ASIC and FPGA technologies and addresses a wide range of networking applications where security is a concern.

The AES-GCM Multi-Booster crypto engine 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.

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking test-bench based on FIPS vectors
- Documentation

For other AES solutions, please see dedicated product sheets: **AES Multi-Purpose** (BA411e), **AES-XTS Multi-Booster** (BA416) and **AES-GCM Ultra-Low Latency** (BA415LL)

AES Crypto Engines

Encrypts the plain text (source data) into cipher text (encrypted data) and sends it to the NAND flash for storage.

	AES MULTI-PURPOSE The solution suitable for a wide range of low-cost & high-end applications	AES-XTS MULTI-BOOSTER Unique architecture enables high throughput while maintaining an optimal resource usage	AES-GCM MULTI-BOOSTER Unique architecture enables high throughput while maintaining an optimal resource usage	AES-GCM ULTRA-LOW LATENCY Unique architecture enables ultra-low latency while maintaining an optimal resource usage
Configurable/scalable for perfect application fit	✓	✓	✓	✓
Cipher modes	All modes included	XTS	CTR, GCM/GMAC	CTR, GCM/GMAC
Full software/driver support	✓	✓	✓	✓
Performance	Up to 10 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps
DPA countermeasures	✓	–	✓	✓
Fault injection countermeasures	✓	–	–	–
Key sizes supported	128, 192, 256 Bits	128, 256 bits	128, 256 bits	128, 256 bits
Optional Direct memory access (DMA)	✓	✓	✓	✓
Power/area	Scalable	Scalable	Scalable	Scalable
Context switching (multi-thread)	✓	–	✓	✓
Interface support	FIFO, AMBA	FIFO, AMBA	FIFO, AMBA	FIFO, AMBA
NIST/FIPS Support	SP800-38A, B, C, D, E, F FIPS 197	SP800-38E FIPS 197	SP800-38D FIPS 197	SP800-38D FIPS 197
Applications	For any application, examples: • Communications • Digital Cinema • DRM • Encrypted data storage • Industrial • Cloud computing • Defence • Automotive • General MCU's • Etc...	• Encrypted disk/data storage • SATA III	• MACsec/IPsec/TLS • Optical transport • Broadband access • WPA3 support	• CXL 2.0 • PCI Express 5.0
	PRODUCT CODE BA411e	PRODUCT CODE BA416	PRODUCT CODE BA415	PRODUCT CODE BA415LL

SILEX INSIGHT

Silex Insight
Rue Emile Francqui 11,
1435 Mont-Saint-Guibert, Belgium

Tel: +32 10 45 49 04
E-mail: contact@silexinsight.com
Web: www.silexinsight.com