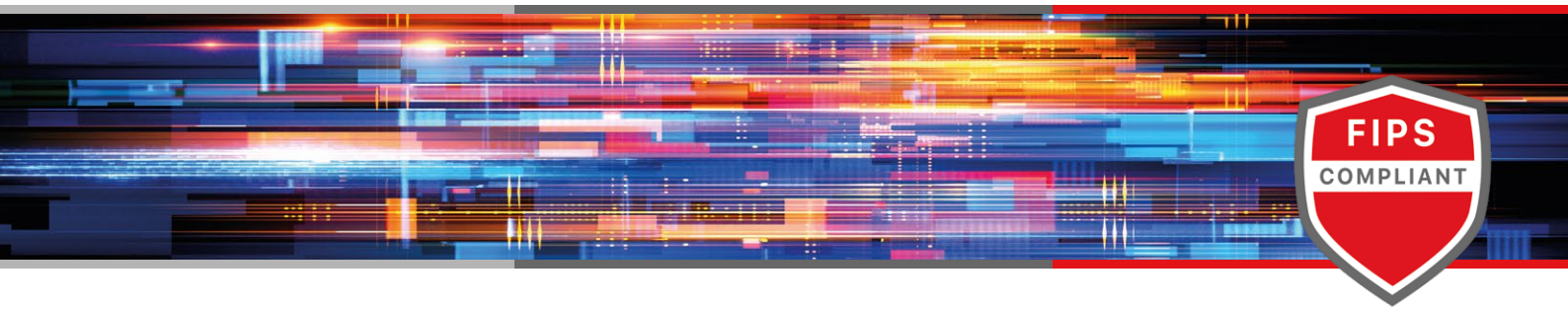
SILEX INSIGHT

Product sheet
BA415LL



AES-GCM ULTRA-LOW LATENCY

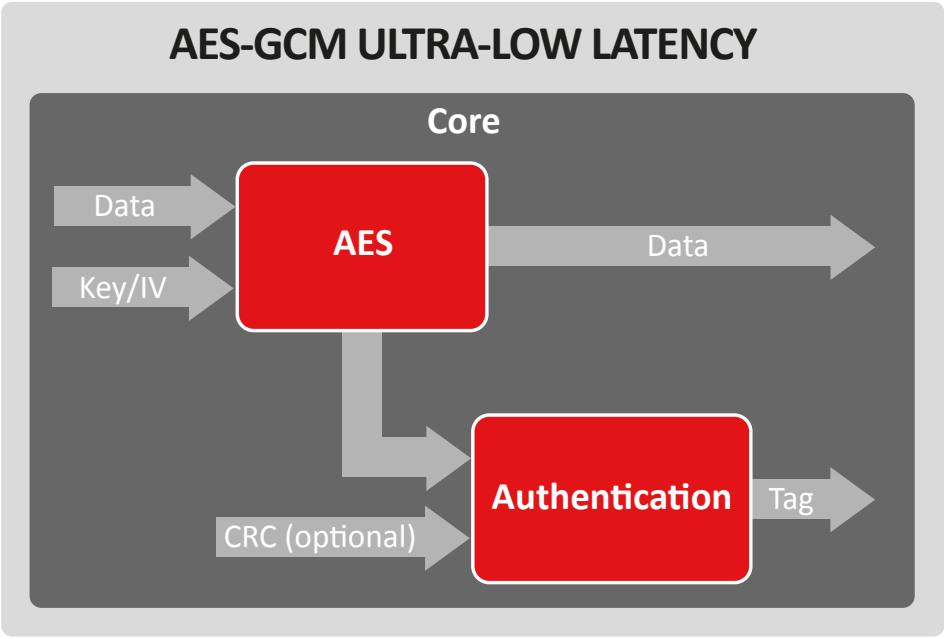
The AES-GCM Ultra-low latency crypto engine is targeted for CXL link encryption with an implementation of the AES-GCM algorithm compliant with the NIST SP 800-38D standard. The unique architecture enables high throughput while maintaining an optimal resource usage.

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.

The AES-GCM is the only authenticated encryption algorithm recommended by NIST enabling very high throughput. In addition, it also offers ultra-low latency:

• 0 clock cycle for encryption/decryption (combinational path)

In addition, it supports CXL 2.0. One of many new great features that comes with CXL 2.0 is the support for single level switching to enable fan-out to multiple devices. This will enable many devices in a platform to migrate to CXL, while maintaining the backward compatibility and the low-latency characteristics of CXL.



Features

- High throughput: 64 GB/s (512 Gbps)
- Ultra-low latency
- Optional CRC support for data integrity
- 128-bit and 256-bit key
- NIST SP 800-38D compliant
- Best trade-off between area and performance

Applications

- CXL 2.0
- PCI Express 5.0

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 Multi-Booster** (BA415).

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