SILEX INSIGHT

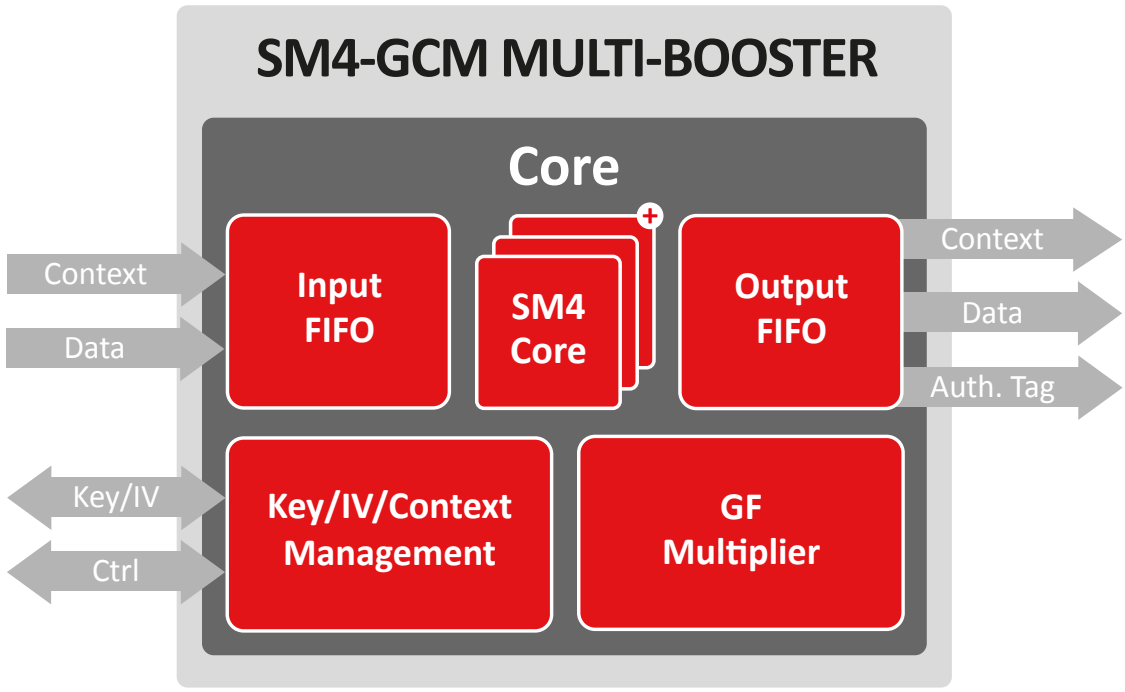
Product sheet
BA415

SM4-GCM MULTI-BOOSTER

The SM4-GCM Multi-Booster crypto engine is a scalable implementation of the SM4-GCM algorithm compliant with the standard GBT.32907-2016 published by the Organization of State Commercial Administration of China. The unique architecture enables high throughput while maintaining an optimal resource usage.

The SM4-GCM (Galois Counter Mode) is an authenticated encryption algorithm which combines the SM4 counter mode for encryption and the Galois field multiplier for the authentication. The encryption and authentication occur in parallel to enable high throughput.

The GCM cipher mode is well suited to secure high speed communication channels and is widely used in different standards.



Features

- ASIC & FPGA
- High throughput:
  - ASIC: 2Tbps
  - FPGA: 100 Gbps
- Guaranteed performance with small packets
- Supports AES cipher
- OSCCA 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

- Network communication (TLS...)
- Data centers
- Optical transport

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 SM4-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 SM4-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 reference vectors
- Documentation

For other SM4 solutions, please see dedicated product sheets: **SM4 Standard Crypto Engine** (BA419) and **SM4-XTS Multi-Booster** (BA425).

SM4 Crypto Engines

SM4 is a block cipher used in the Chinese National Standard for Wireless LAN WAPI (Wired Authentication and Privacy Infrastructure).

	SM4 STANDARD CRYPTO ENGINE The solution suitable for a wide range of low-cost & high-end applications	SM4-XTS MULTI-BOOSTER Unique architecture enables high throughput while maintaining an optimal resource usage	SM4-GCM MULTI-BOOSTER Unique architecture enables high throughput while maintaining an optimal resource usage
Configurable/scalable for perfect application fit	✓	✓	✓
Cipher modes	All modes included	XTS	CTR, GCM/GMAC
Full software/driver support	✓	✓	✓
Performance	Up to 10 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps
DPA countermeasures	✓	✓	✓
Context switching (multi-thread)	✓	–	✓
Optional Direct memory access (DMA)	✓	✓	✓
Power/area	Scalable	Scalable	Scalable
Interface support	FIFO, AMBA	FIFO, AMBA	FIFO, AMBA
OSCCA Support	GB/T 32907-2016 SP800-38A, B, C, D, E, F	GB/T 32907-2016 SP800-38E	GB/T 32907-2016 SP800-38D
Applications	• Wireless communication • Payment	• Encrypted disk/data storage • External memory encryption	• Network communication (TLS...) • Data centers • Optical transport
	PRODUCT CODE BA419	PRODUCT CODE BA425	PRODUCT CODE BA415

SILEX INSIGHT

SILEX INSIGHT

Product sheet

BA415 - SM4-GCM multi-booster

V1.2

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