

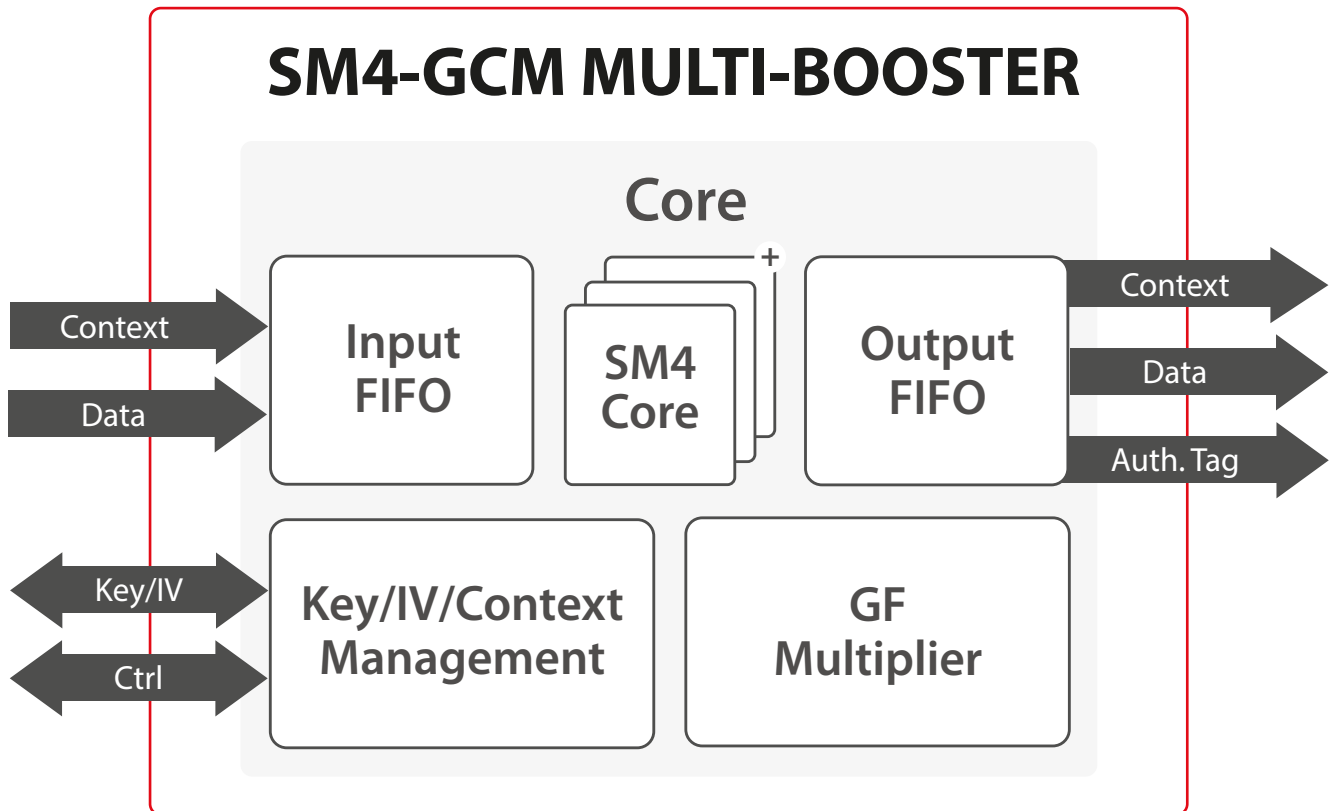
Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Security IP > Tunable Crypto > Symmetric > SCZ_IP_BA415

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
- ✓ Chinese market



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 RTL test-bench on referenced vectors
- ✔ Documentation

For other SM4 solutions, please see dedicated product sheets: **SM4 Standard Crypto Engine** (SCZ_IP_BA419) and **SM4-XTS Multi-Booster** (SCZ_IP_BA425).

SM4 Crypto Engines

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

Configurable/scalable for perfect application fit

| | SM4 STANDARD CRYPTO ENGINE | SM4-XTS MULTI-BOOSTER | SM4-GCM MULTI-BOOSTER |
|-------------------------------------|---|---|---|
| | The solution suitable for a wide range of low-cost & high-end applications | Unique architecture enables high throughput while maintaining an optimal resource usage | Unique architecture enables high throughput while maintaining an optimal resource usage |
| | ✔ | ✔ | ✔ |
| 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 | <ul style="list-style-type: none"> • Wireless communication • Payment | <ul style="list-style-type: none"> • Encrypted disk/data storage • External memory encryption | <ul style="list-style-type: none"> • Network communication (TLS...) • Data centers • Optical transport |
| | <p style="text-align: center;">PRODUCT CODE SCZ_IP_BA419</p> | <p style="text-align: center;">PRODUCT CODE SCZ_IP_BA425</p> | <p style="text-align: center;">PRODUCT CODE SCZ_IP_BA415</p> |

SECURE-ic
THE SECURITY SCIENCE COMPANY

V1.2

SECURE-ic
THE SECURITY SCIENCE COMPANY

HEADQUARTERS

Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US

www.secure-ic.com