SECURE-iC
THE SECURITY SCIENCE COMPANY

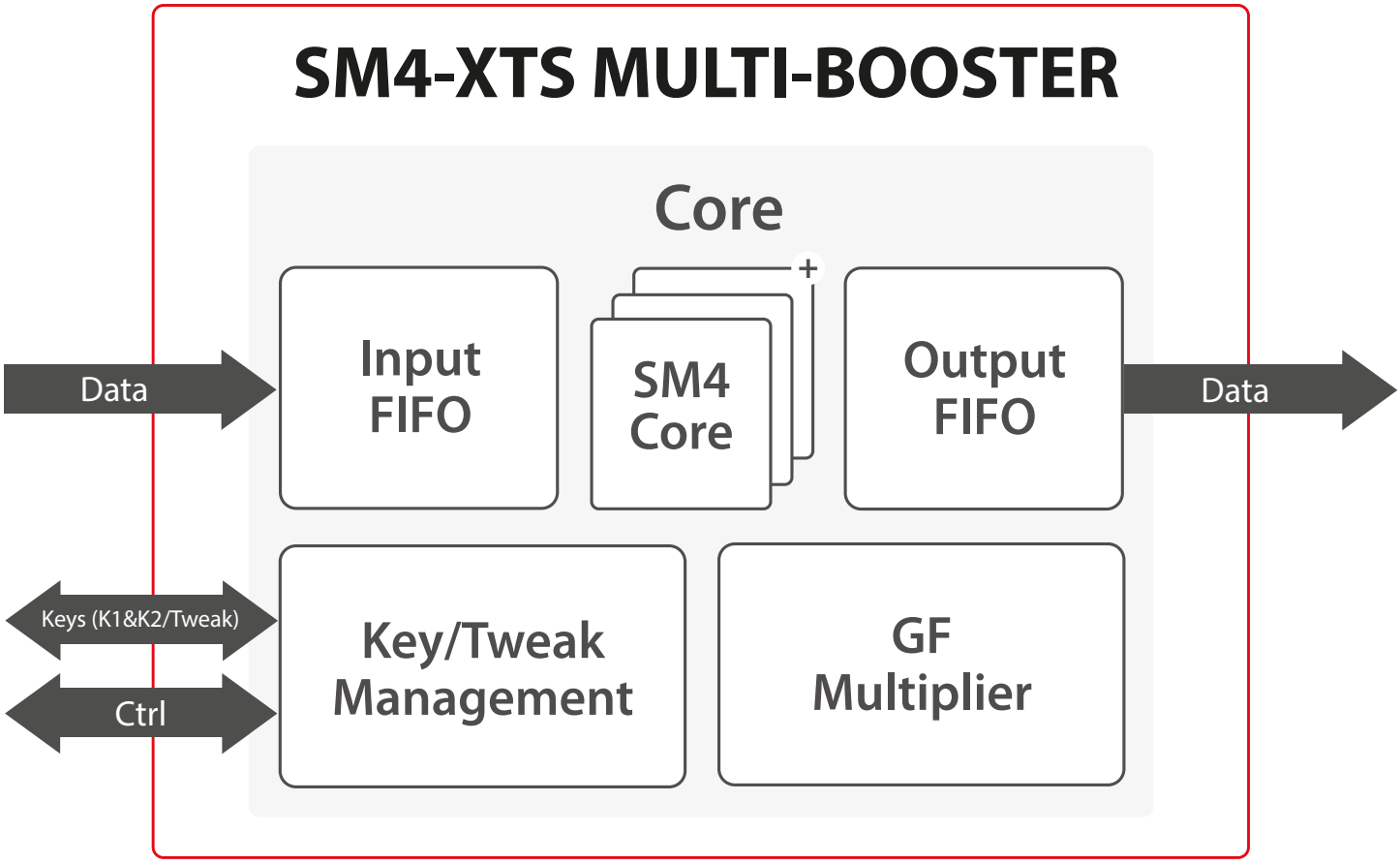
PRODUCT SHEET

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Security IP > Tunable Crypto > Symmetric > SCZ_IP_SM4_XTS

SM4-XTS MULTI-BOOSTER

The SM4-XTS Multi-Booster crypto engine includes a generic & scalable implementation of the SM4 algorithm (a block cipher specified by the OSCCA) making the solution ideal for high-end applications (including key, tweak, input and output registers and Galois field multiplier).

This crypto engine targets high-performance applications such as data storage and memory encryption. Thanks to its scalability, it can be tailored to reach the best trade-off between performances, area and technology.



Features

- ASIC & FPGA
- High throughput:
  - ASIC: 2Tbps
  - FPGA: 100 Gbps
- OSCCA compliant
- Scalable solution
- Can be provided with AXI DMA & software
- Masking with excellent protection against SPA & DPA (optional)
- Low power feature
- Cipher stealing (optional)
- Straight forward integration with simple FIFO interfaces

Applications

- Encrypted disk/data storage
- External memory encryption
- Chinese market

Implementation aspects

The SM4-XTS crypto engine is easily portable to ASIC and FPGA. It supports a wide range of applications on various technologies. The unique architecture enables a high level of flexibility. The throughput and features required by a specific application can be taken into account in order to select the most optimal and compact configuration.

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_SM4) and **SM4-GCM Multi-Booster** (SCZ_IP_AES_SM4-GCM).

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 SCZ_IP_SM4	PRODUCT CODE SCZ_IP_SM4_XTS	PRODUCT CODE SCZ_IP_AES_SM4-GCM

SECURE-IC
THE SECURITY SCIENCE COMPANY

V4.0

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

TAIWAN
sales-TAIWAN@secure-ic.com

CONTACT US
www.secure-ic.com