SECURE-iC
THE SECURITY SCIENCE COMPANY

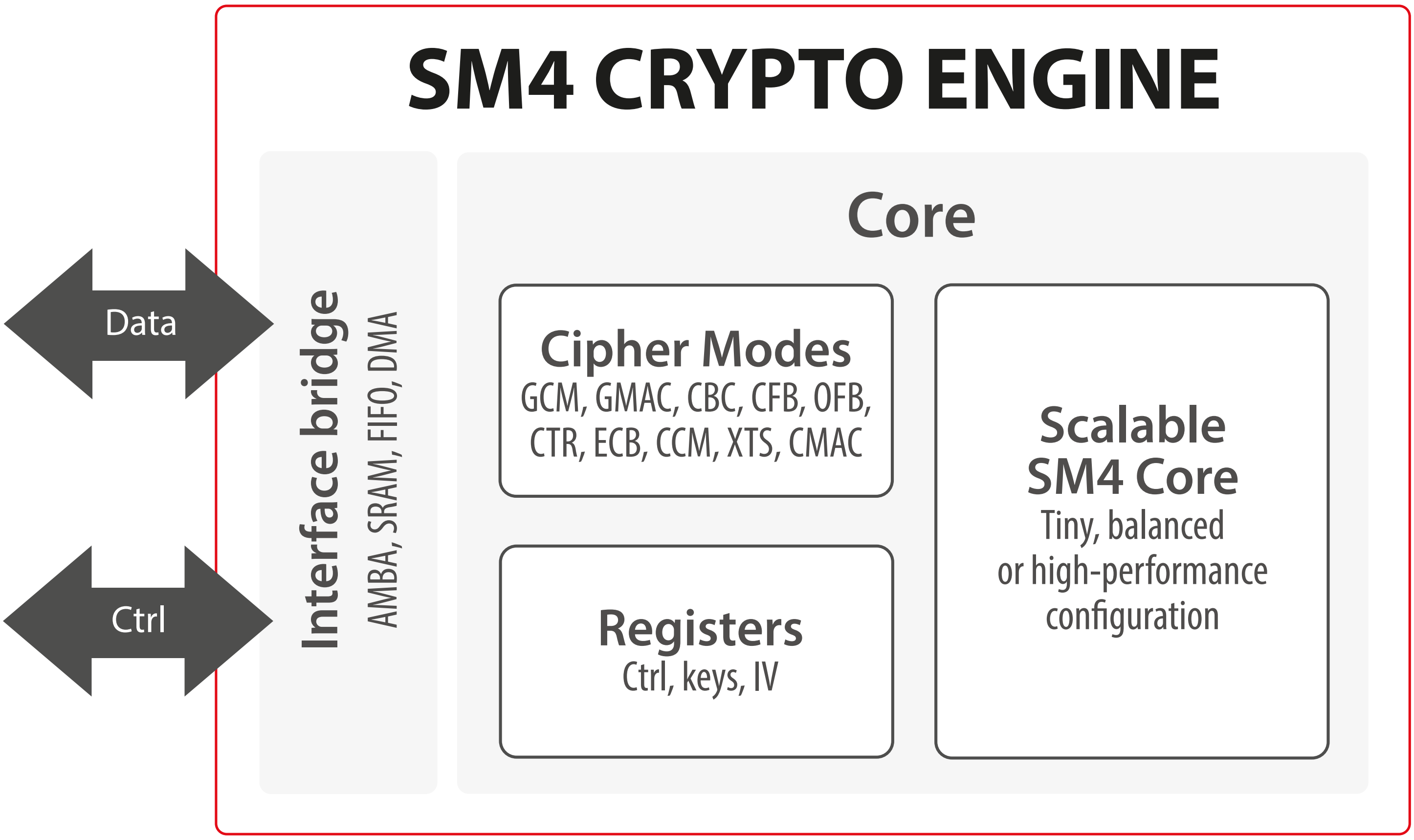
PRODUCT SHEET

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Security IP > Tunable Crypto > Symmetric > SCZ_IP_BA419

SM4 CRYPTO ENGINE

The SM4 crypto engine includes a generic & scalable implementation of the SM4 algorithm which is the block cipher standard of China.

It is compliant with the GBT.32907-2016 specification and can support several cipher modes including authenticated encryption. It is portable to ASIC and any FPGA's. This algorithm has been adopted in TPM2.0 of the Trust Computing Group (TCG) standard.



Features

- ✓ ASIC & FPGA
- ✓ Scalable solution
- ✓ OSCCA compliant
- ✓ DPA countermeasures
- ✓ Context switching
- ✓ Supports encryption & decryption
- ✓ Performs key expansion
- ✓ Compliant with GBT.32907-2016
- ✓ Data interface: AMBA (AHB/AXI:AXI-4) with optional DMA
- ✓ Control interface: APB or AXI4-lite
- ✓ Supports a wide selection of programmable ciphering modes based on NIST SP 800-38:
  - Non-chaining modes: ECB, CTR
  - Chaining modes: CBC, CFB, OFB
  - Authentication: CMAC (OMAC1)
  - Authentication & Confidentiality: CCM, GCM, GMAC
  - Confidentiality on storage devices: XTS

Applications

- ✓ Wireless communication
- ✓ Payment
- ✓ Chinese market

Implementation aspects

The SM4 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 IP Core is available in the Crypto Coprocessors (SCZ_IP_BA450 / 456 / 457) and the Secure Element/Root of Trust/HSM (SCZ_iSE_100_BA470) from Secure-IC.

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-XTS Multi-Booster** (SCZ_IP_BA425) and **SM4-GCM Multi-Booster** (SCZ_IP_BA415).

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_BA419	PRODUCT CODE SCZ_IP_BA425	PRODUCT CODE SCZ_IP_BA415

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