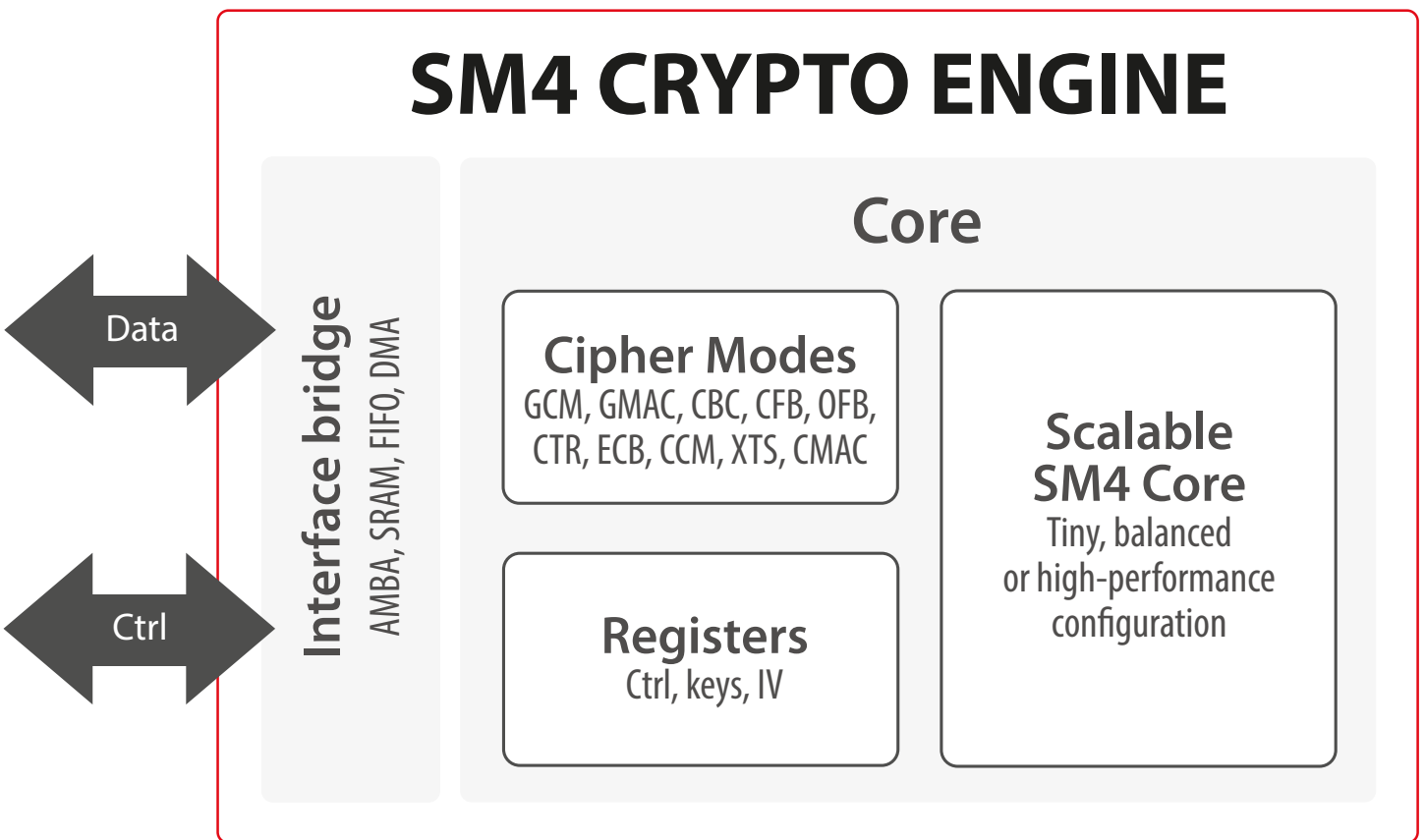


Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Security IP > Tunable Crypto > Symmetric > SCZ_IP_SM4

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 | ✓ Supports encryption & decryption | ✓ Supports a wide selection of programmable ciphering modes based on NIST SP 800-38: |
| ✓ Scalable solution | ✓ Performs key expansion | • Non-chaining modes: ECB, CTR |
| ✓ OSCCA compliant | ✓ Compliant with GBT.32907-2016 | • Chaining modes: CBC, CFB, OFB |
| ✓ DPA countermeasures | ✓ Data interface: AMBA (AHB/AXI:AXI-4) with optional DMA | • Authentication: CMAC (OMAC1) |
| ✓ Context switching | ✓ Control interface: APB or AXI4-lite | • 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 can be hosted in Securyzr™ neo Crypto Solution Platform and in Securyzr™ neo Core Platform for iSE.

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_SM4_XTS) 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).

Configurable/scalable for perfect application fit

Cipher modes

Full software/driver support

Performance

DPA countermeasures

Context switching (multi-thread)

Optional Direct memory access (DMA)

Power/area

Interface support

OSCCA Support

Applications

SM4 STANDARD CRYPTO ENGINE

The solution suitable for a wide range of low-cost & high-end applications

✓

All modes included

✓

Up to 10 Gbps

✓

✓

✓

Scalable

FIFO, AMBA

GB/T 32907-2016
SP800-38A, B, C, D, E, F

- Wireless communication
- Payment

PRODUCT CODE
SCZ_IP_SM4

SM4-XTS MULTI-BOOSTER

Unique architecture enables high throughput while maintaining an optimal resource usage

✓

XTS

✓

ASIC: 2 Tbps / FPGA: 100 Gbps

✓

—

✓

Scalable

FIFO, AMBA

GB/T 32907-2016
SP800-38E

- Encrypted disk/data storage
- External memory encryption

PRODUCT CODE
SCZ_IP_SM4_XTS

SM4-GCM MULTI-BOOSTER

Unique architecture enables high throughput while maintaining an optimal resource usage

✓

CTR, GCM/GMAC

✓

ASIC: 2 Tbps / FPGA: 100 Gbps

✓

✓

✓

Scalable

FIFO, AMBA

GB/T 32907-2016
SP800-38D

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

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