SECURE-iC
THE SECURITY SCIENCE COMPANY

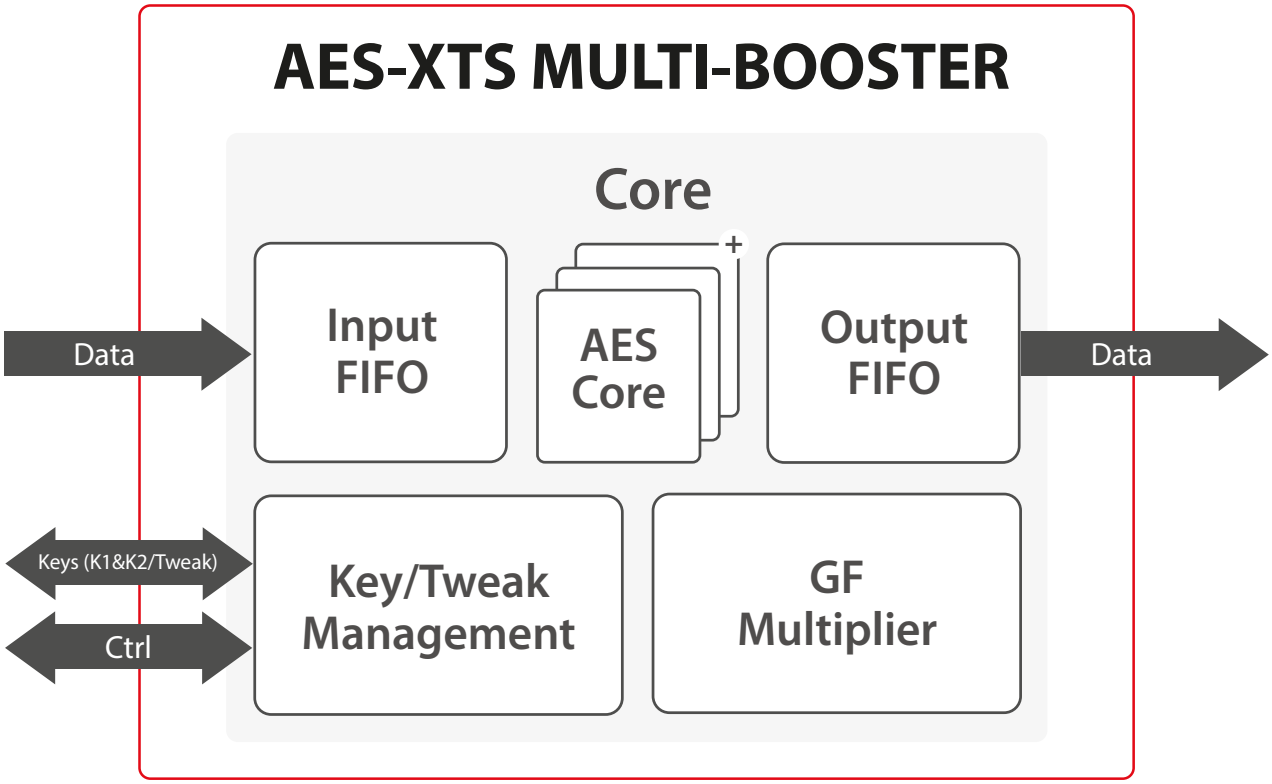
PRODUCT SHEET

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

AES-XTS MULTI-BOOSTER

The AES-XTS Multibooster crypto engine includes a generic & scalable implementation of the AES algorithm making the solution suitable for a wide range of low-cost & high-end applications (including key, tweak, input and output registers and Galois field multiplier).

This crypto engine targets high-performance applications, where a high throughput is required. Thanks to its scalability, it can be tailored to reach the best trade-off between performances, area and technology.



Implementation aspects

The AES-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.

Features

- ASIC & FPGA
- High throughput:
  - ASIC: 2Tbps
  - FPGA: 100 Gbps
- 128-bit and 256-bit key
- NIST SP 800-38D compliant
- Scalable solution
- Can be provided with AXI DMA & software
- Cipher stealing (optional)
- Low power feature
- Best trade-off between area and performance
- Straight forward integration with simple FIFO interfaces

Applications

- Encrypted disk/data storage
- SATA III

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking RTL test-bench on referenced vectors
- Documentation

For other AES solutions, please see dedicated product sheets: **AES Multi-Purpose** (SCZ_IP_AES), **AES-GCM Multi-Booster** (SCZ_IP_AES_SM4-GCM) and **AES-GCM Ultra-Low Latency** (SCZ_IP_AES_GCM_S8).

AES Crypto Engines

Encrypts the plain text (source data) into cipher text (encrypted data) and sends it to the NAND flash for storage.

	AES MULTI-PURPOSE The solution suitable for a wide range of low-cost & high-end applications	AES-XTS MULTI-BOOSTER Unique architecture enables high throughput while maintaining an optimal resource usage	AES-GCM MULTI-BOOSTER Unique architecture enables high throughput while maintaining an optimal resource usage	AES-GCM ULTRA-LOW LATENCY Unique architecture enables ultra-low latency while maintaining an optimal resource usage
Configurable/scalable for perfect application fit	✓	✓	✓	✓
Cipher modes	All modes included	XTS	CTR, GCM/GMAC	CTR, GCM/GMAC
Full software/driver support	✓	✓	✓	✓
Performance	Up to 10 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps	ASIC: 2 Tbps / FPGA: 100 Gbps
DPA countermeasures	✓	–	✓	✓
Fault injection countermeasures	✓	–	–	–
Key sizes supported	128, 192, 256 Bits	128, 256 bits	128, 256 bits	128, 256 bits
Optional Direct memory access (DMA)	✓	✓	✓	✓
Power/area	Scalable	Scalable	Scalable	Scalable
Context switching (multi-thread)	✓	–	✓	✓
Interface support	FIFO, AMBA	FIFO, AMBA	FIFO, AMBA	FIFO, AMBA
NIST/FIPS Support	SP800-38A, B, C, D, E, F FIPS 197	SP800-38E FIPS 197	SP800-38D FIPS 197	SP800-38D FIPS 197
Applications	For any application, examples: • Communications • Digital Cinema • DRM • Encrypted data storage • Industrial • Cloud computing • Defence • Automotive • General MCU's • Etc...	• Encrypted disk/data storage • SATA III	• MACsec/IPsec/TLS • Optical transport • Broadband access • WPA3 support	• CXL 2.0 • PCI Express 5.0
	PRODUCT CODE SCZ_IP_AES	PRODUCT CODE SCZ_IP_AES_XTS	PRODUCT CODE SCZ_IP_AES_SM4-GCM	PRODUCT CODE SCZ_IP_AES_GCM_S8

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