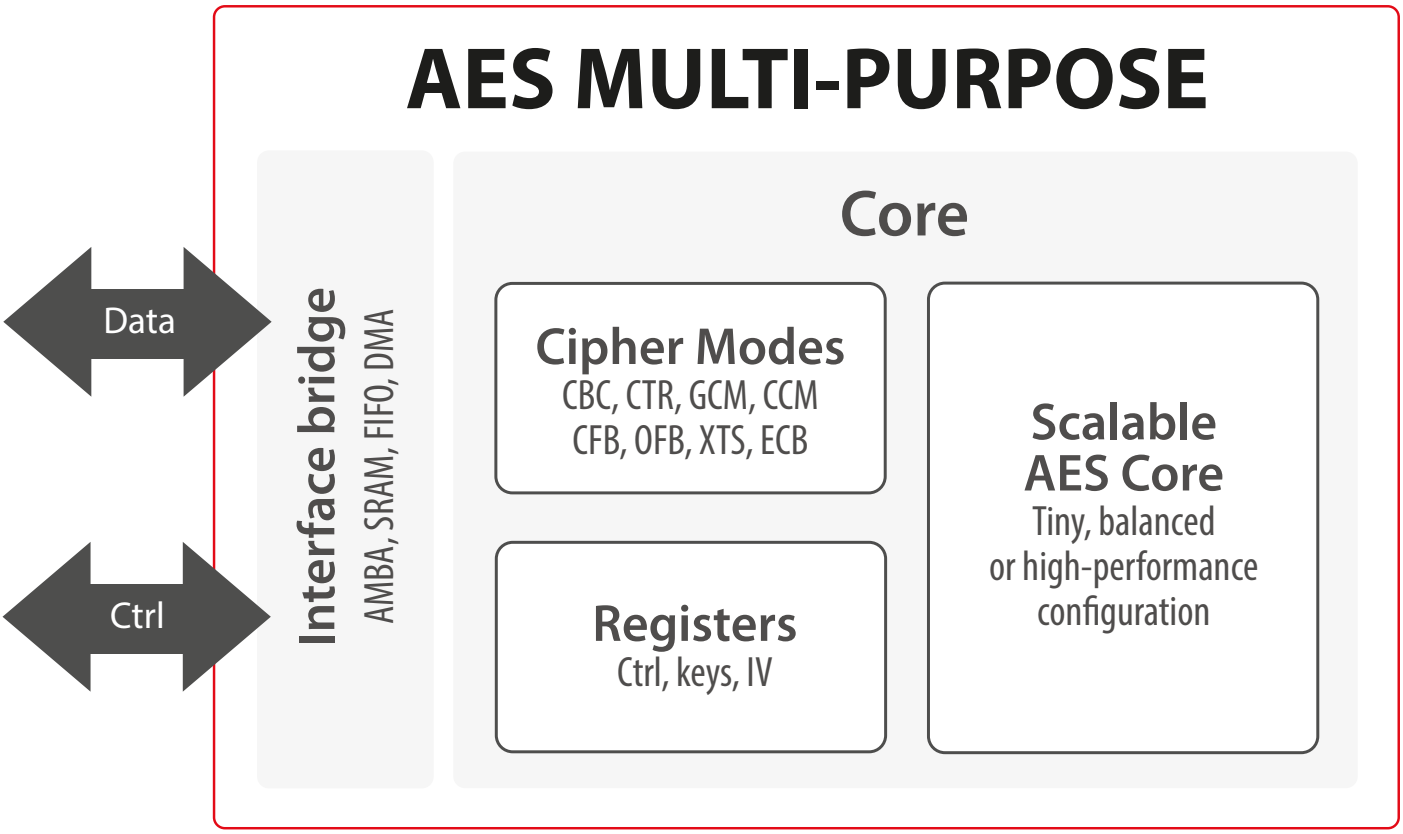
SECURE-iC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Crypto Security IP > SCZ_IP_BA411e

AES MULTI-PURPOSE

The AES Multi-Purpose crypto engine includes a generic and scalable implementation of the AES algorithm and a configurable wrapper making the solution suitable for a wide range of low-cost & high-end applications.



Implementation aspects

The AES Multi-Purpose 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 configuration.

Features

- ASIC and FPGA
- Supports a wide selection of programmable ciphering modes based on NIST SP 800-38:
  - Non-chaining modes: ECB, CTR
  - Chaining modes: CBC, CFB, OFB
  - Cyphertext stealing modes: CBC-CS
  - Authentication: CMAC (OMAC1)
  - Authentication & Confidentiality: CCM, GCM
  - Confidentiality on storage devices: XTS/XTS-CS
- Masking option available with excellent protection against SPA & DPA
- Context switching
- Data interface: AMBA (AHB/AXI:AXI-4) with optional DMA
- Control interface: APB or AXI4-lite

Applications

- Ideal for any application, examples:
  - Wireless and wired communications
  - Digital Cinema
  - DRM
  - Encrypted data storage
  - Industrial
  - Cloud computing
  - Defence
  - Automotive
  - General MCU's
  - Etc...

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-GCM Multi-Booster** (SCZ_IP_BA415), **AES-XTS Multi-Booster** (SCZ_IP_BA416) and **AES-GCM Ultra-Low Latency** (SCZ_IP_BA415LL).

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_BA411e	PRODUCT CODE SCZ_IP_BA416	PRODUCT CODE SCZ_IP_BA415	PRODUCT CODE SCZ_IP_BA415LL

SECURE-IC
THE SECURITY SCIENCE COMPANY

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