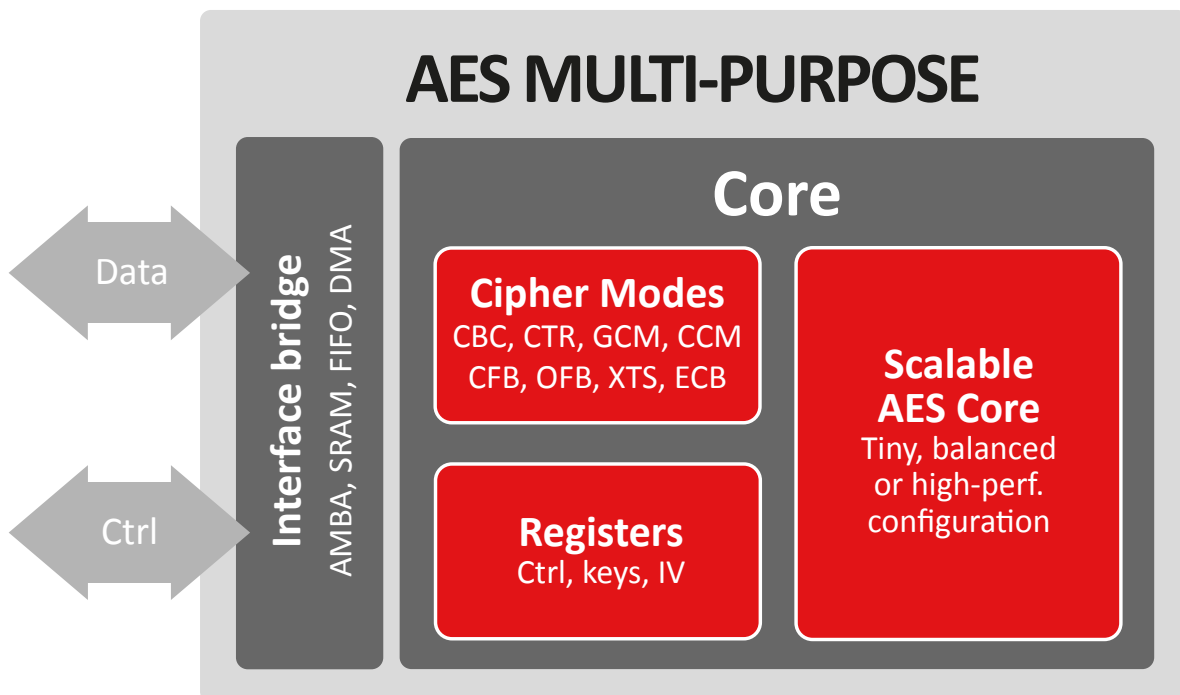




AES MULTI-PURPOSE

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 for the most advanced AES core.



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 (BA415)**, **AES-XTS Multi-Booster (BA416)** and **AES-GCM Ultra-Low Latency (BA415LL)**.

AES Crypto Engines

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

Configurable/scalable for perfect application fit

Cipher modes	All modes included
Full software/driver support	✔
Performance	Up to 10 Gbps
DPA countermeasures	✔
Fault injection countermeasures	✔
Key sizes supported	128, 192, 256 Bits
Optional Direct memory access (DMA)	✔
Power/area	Scalable
Context switching (multi-thread)	✔
Interface support	FIFO, AMBA
NIST/FIPS Support	SP800-38A, B, C, D, E, F FIPS 197
Applications	For any application, examples: • Communications • Digital Cinema • DRM • Encrypted data storage • Industrial • Cloud computing • Defence • Automotive • General MCU's • Etc...

AES
MULTI-PURPOSE

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

PRODUCT CODE
BA411e

AES-XTS
MULTI-BOOSTER

Unique architecture enables high throughput while maintaining an optimal resource usage

PRODUCT CODE
BA416

AES-GCM
MULTI-BOOSTER

Unique architecture enables high throughput while maintaining an optimal resource usage

PRODUCT CODE
BA415

AES-GCM
ULTRA-LOW LATENCY

Unique architecture enables ultra-low latency while maintaining an optimal resource usage

PRODUCT CODE
BA415LL

Product sheet
AES Multi-purpose
V1.4

Silex Insight
Rue Emile Francqui 11,
1435 Mont-Saint-Guibert, Belgium

Tel: +32 10 45 49 04
E-mail: contact@silexinsight.com
Web: www.silexinsight.com

www.silexinsight.com