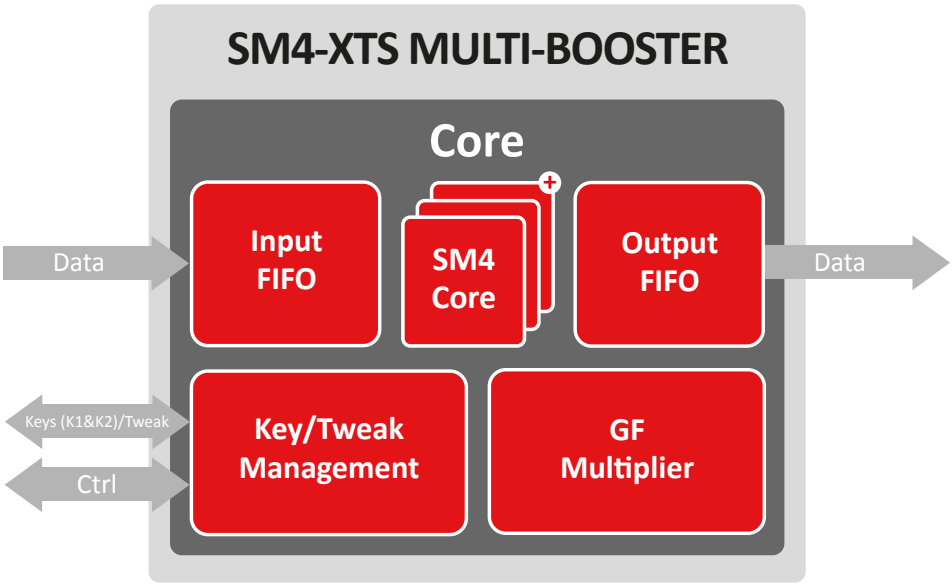
SILEX INSIGHT

Product sheet
BA425

SM4-XTS MULTI-BOOSTER

The SM4-XTS Multi-Booster crypto engine includes a generic & scalable implementation of the SM4 algorithm (a block cipher specified by the OSCCA) making the solution ideal for high-end applications (including key, tweak, input and output registers and Galois field multiplier).

This crypto engine targets high-performance applications such as data storage and memory encryption. Thanks to its scalability, it can be tailored to reach the best trade-off between performances, area and technology.



Features

- ASIC and FPGA
- High throughput:
  - ASIC: >400 Gbps
  - FPGA: 100 Gbps
- Scalable solution
- Can be provided with AXI DMA & software
- Masking with excellent protection against SPA & DPA (optional)
- Cipher stealing (optional)
- Low power feature
- Straight forward integration with simple FIFO interfaces

Applications

- Encrypted disk/data storage
- External memory encryption
- Chinese market

Implementation aspects

The SM4-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.

For other XTS Multi-Booster solutions, please see dedicated product sheet: **AES-XTS Multi-Booster (BA416)**. We also offer a multi-purpose **SM4 Crypto Engine (BA419)**.

Deliverables

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

V1.1

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