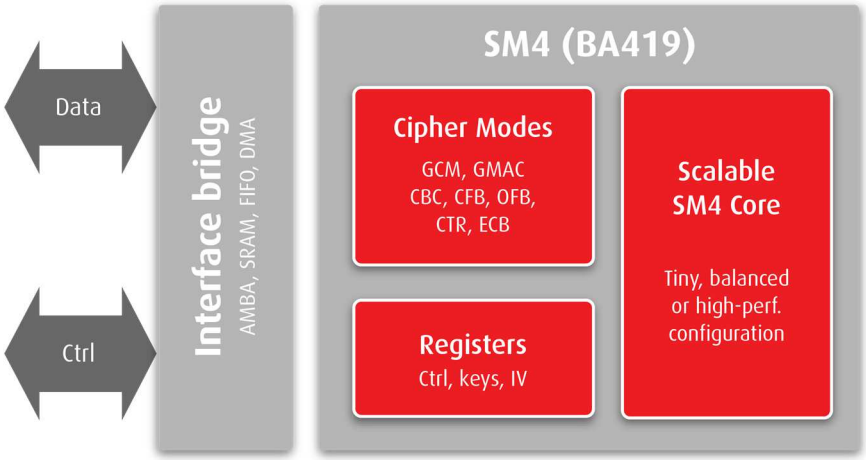
SM4 crypto Engine

BA419
Product sheet

The BA419 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 authentication 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

- Supports encryption & decryption
- Performs key expansion
- Compliant with GBT.32907-2016
- Data interface: AMBA (AHB/AXI:AXI-4) with optional DMA
- Control interface: APB or AXI4-lite
- ASIC and FPGA
- Supports a wide selection of programmable ciphering modes:
  - Non-chaining modes: ECB, CTR
  - Chaining modes: CBC, CFB, OFB
  - Authentication & Confidentiality: GCM, GMAC

Applications

- Wireless communication
- Payment
- Chinese market

Implementation aspects

The BA419 IP core 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 is available in the crypto coprocessor (BA450) and the Root of Trust/HSM (BA470) from Silex Inside.

Deliverables

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