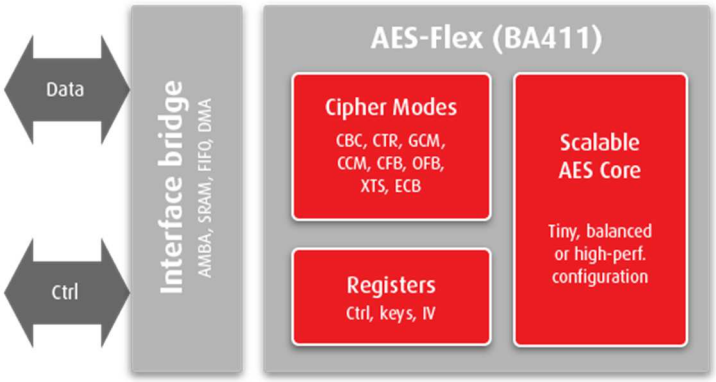
AES crypto Engine

BA411E-FLEX
Product sheet

The BA411E-FLEX multi-purpose AES crypto engine includes a generic & scalable implementation of the AES algorithm and a configurable wrapper making the solution suitable for a wide range of low-cost & high-end applications from < 6 K-Gates for the most compact AES Core to > 100 Gbps.



Applications

- Wireless and wired communications
- Digital Cinema
- DRM
- Encrypted data storage

Implementation aspects

The BA411E-FLEX IP core is easily portable to ASIC and FPGA (Altera, Xilinx, Microsemi). 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.

Deliverables

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

FEATURES

- Supports 128-bit, 192-bit & 256-bit key length
- Supports encryption & decryption
- Performs key expansion
- Masking option available with excellent protection against SPA & DPA
- Parallelizable configuration for ECB, CTR, GCM & XTS mode
- Data interface: AMBA (AHB/AXI:AXI-4) with optional DMA
- Control interface: APB or AXI4-lite
- 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