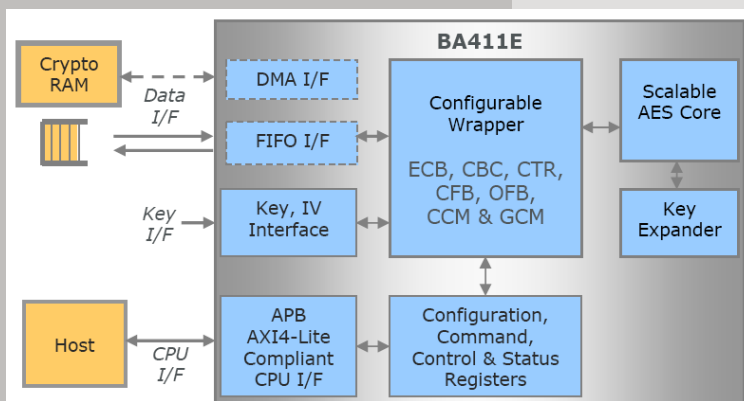


AES Crypto Engine

- **Description**
 - Multi-Purpose AES Crypto Engine developed, validated & licensed by Barco Silex
 - Includes a generic & scalable implementation of the AES algorithm and a configurable wrapper making the solution suitable for a wide range of low-end & high-end applications
- **Portability**
 - ASIC, Actel, Altera, Xilinx
- **Key Features**
 - Scalable AES Core
 - Configurable Block Cipher Wrapper
 - Supports 128-bit, 192-bit & 256-bit key length
 - Supports Encryption & Decryption
 - Performs Key Expansion
 - Masking option available for applications requiring higher level of security with a very good protection against SPA & DPA (Simple/Dual Power Analysis)
 - Supports interleaved ECB, CTR, CCM & GCM modes for higher performances
 - Supports a wide selection of programmable ciphering modes:
 - Non-Chaining Modes (SP800-38A): ECB & CTR
 - Chaining Modes (SP800-38A): CBC, CFB & OFB
 - Chaining Modes (SP800-38B): OMAC
 - Encryption + Auth. (SP800-38C): CCM
 - Encryption + Auth. (IEEE 802.1ae): GCM
 - Supports 'Bypass' or 'NULL Cipher' mode for streaming applications
 - Stallable core
- **Interfaces**
 - Control interface: APB-compliant or AXI4-Lite
 - Data interface: Slave, FIFO/AXI4-Stream or DMA
- **Performance – Size**
 - See Datasheet for more information
 - ASIC 90nm: Max Freq=500MHz, Throughput: up to 3.5Gbps
 - Low-end FPGA: Max Freq=150MHz, Throughput: up to 1Gbps
 - High-end FPGA: Max Freq=275MHz, Throughput: up to 1.8Gbps
 - Higher performances can be obtained in interleaved mode (see datasheet)
- **Benefits**
 - Supports wide range of applications on various technologies
 - Ease of integration
 - Off-the-shelf & silicon-proven solution
- **Deliverables**
 - RTL or netlist
 - Scripts for synthesis & STA
 - Self-checking Testbench based on FIPS vectors



BA411E – Block diagram

For more information contact:

e-mail: barco-silex@barco.com
www.barco-silex.com

International : + 32 (0)10 454 904
 France : + 33 (0)1 47 38 30 89

