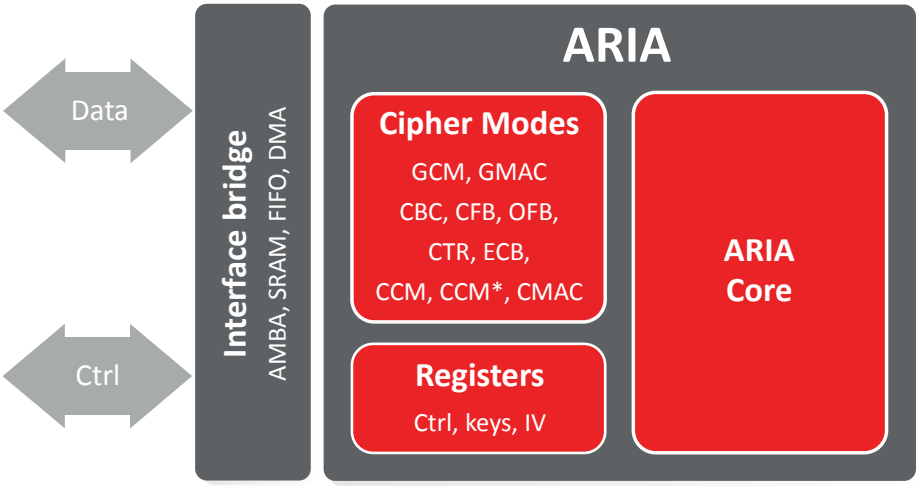
ARIA CRYPTO ENGINE

The ARIA crypto engine includes a generic implementation of the ARIA algorithm which is the block cipher standard of South Korea.

It is compliant with the RFC 6209 specification and can support several cipher modes including authenticated encryption. It is portable to ASIC and any FPGA's. This algorithm has been adopted in PKCS #11 in 2007 and is used in Secure Real-time Transport Protocol (SRTP).



Features

- ASIC and FPGA
- Supports a wide selection of programmable ciphering modes:
  - Non-chaining modes: ECB, CTR
  - Chaining modes: CBC, CFB, OFB
  - Authentication: CMAC
  - Authentication & Confidentiality: GCM, GMAC, CCM, CCM*
- Context switching
- Supports encryption & decryption
- Performs key expansion
- Supports 128-bit, 192-bit & 256-bit key sizes
- Data interface: AMBA (AHB/AXI:AXI-4) with optional DMA
- Control interface: APB or AXI4-lite

Applications

- Wireless communication
- Payment
- South Korean market

Implementation aspects

The BA424 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 Insight.

Deliverables

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

V1.2

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