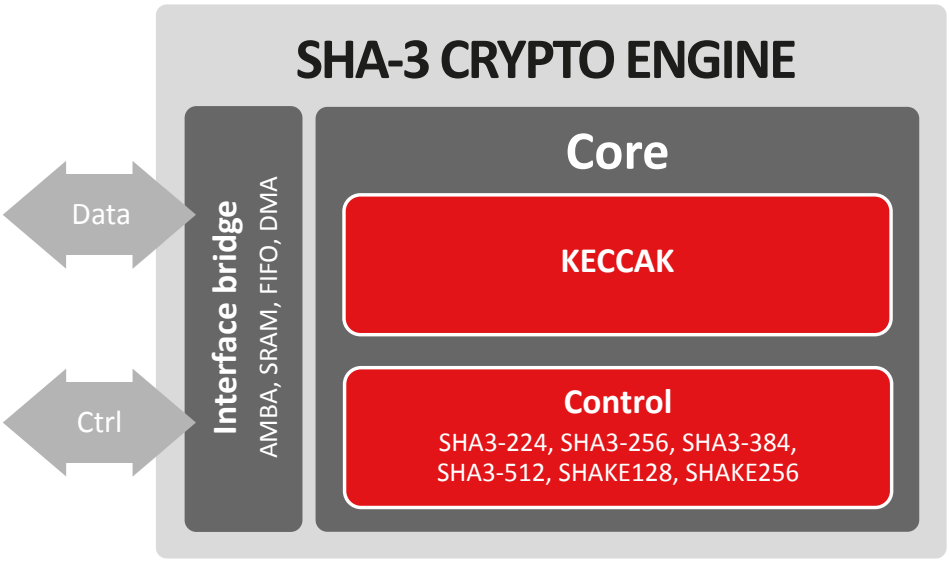
SILEX INSIGHT

Product sheet
BA418

SHA-3 CRYPTO ENGINE

The SHA-3 crypto engine has integrated flexibility and scalability to allow for high throughput and a configurable number of hashing rounds per clock cycle to optimize the silicon resource/performance ratio. Fixed-length or extendable-output (XOF) functions can simply be chosen per individual message through configuration settings.



Implementation aspects

Standardized AXI-4 and AHB (optional) I/O simplifies system integration. Accountability is guaranteed by single RTL database for all configurations in either ASIC or FPGA application. It is delivered with software drivers for easy integration.

Features

- ASIC and FPGA
- FIPS 202 compliant
- Supported fixed-length functions:
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- Supported XOF functions:
  - SHAKE128
  - SHAKE256
- Context save and load
- Very high throughput
- Low power feature
- Compact solution
- Data interface: AMBA (AXI/AHB) with optional DMA
- Control interface: APB/AXI4-lite

Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce
- VPN
- Financial Transactions

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