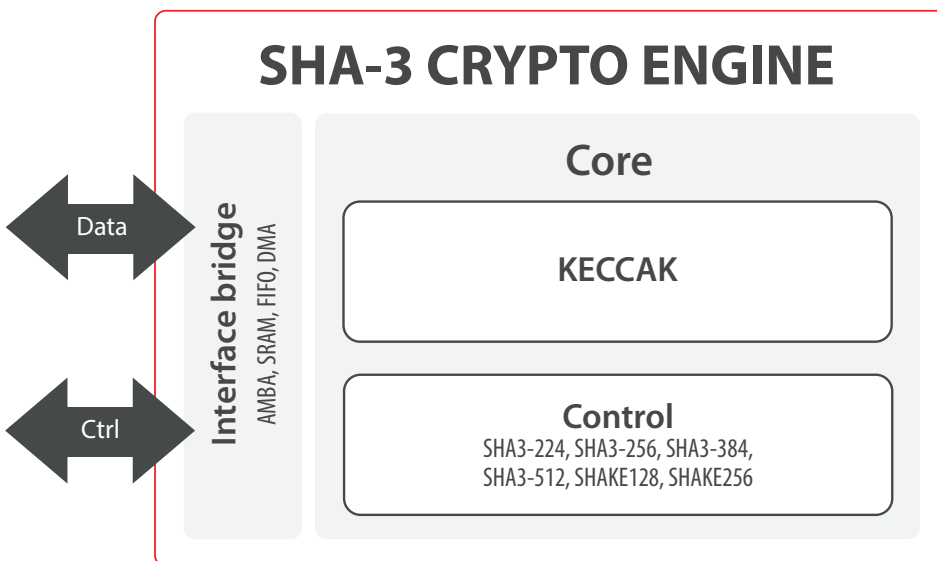


Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Security IP > SCZ_IP_SHA3

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 simplify system integration.

Accountability is guaranteed by single RTL database for all configurations in either ASIC or FPGA application.

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 (only for Crypto Solutions)
- ✓ Control interface: APB/AXI4

Applications

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

Deliverables

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

V4.0

CONTACT US

EMEA

sales-EMEA@secure-ic.com

AMERICAS

sales-US@secure-ic.com

APAC

sales-APAC@secure-ic.com

JAPAN

sales-JAPAN@secure-ic.com

CHINA

sales-CHINA@secure-ic.com

SECURE-ic
THE SECURITY SCIENCE COMPANY

HEADQUARTERS

Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
[+33 \(0\)2 99 12 18 72](tel:+33299121872) - contact@secure-ic.com