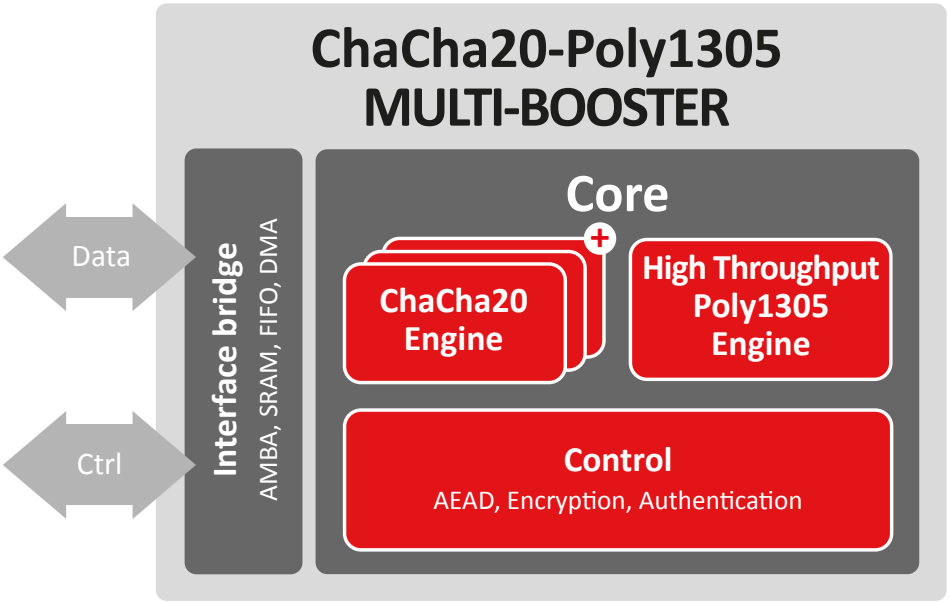
SILEX INSIGHT

Product sheet
BA420

ChaCha20-Poly1305 MULTI-BOOSTER

The ChaCha20-Poly1305 Multi-Booster Crypto Engine is RFC7539 compliant to provide Authenticated Encryption with Associated Data (AEAD) using the ChaCha20 stream cipher combined with the Poly1305 message-authentication code.

This Crypto Engine targets high-performance applications, where a high throughput is required (up to several hundred of Gbps). Thanks to its scalability, it can be tailored to reach the best trade-off between performances, area and technology.



Features

- ASIC and FPGA
- Fully compliant with RFC7539
- Supports authentication and encryption mode (AEAD)
- Scalable to reach the requested trade-off between performance, area and technology
- AMBA AHB/AXI bridges (with optional scatter/gather DMA)
- Low power features
- Poly1305 key generation by ChaCha20
- Full synchronous design

Applications

- Data center
- Cloud computing
- TLS/DTLS
- OpenSSH
- IPsec

Implementation aspects

The ChaCha20-Poly1305 Multi-Booster Crypto Engine is available for ASIC and FPGA, with simple interfaces and easy to integrate. 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 for any FPGA or ASIC technology. The Crypto Engine can be combined with scatter/gather DMA and AMBA interfaces (AHB/AXI) enabling very high throughput in SoC solutions.

This Crypto Engine is also available in the eSecure IP solution (BA470).

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