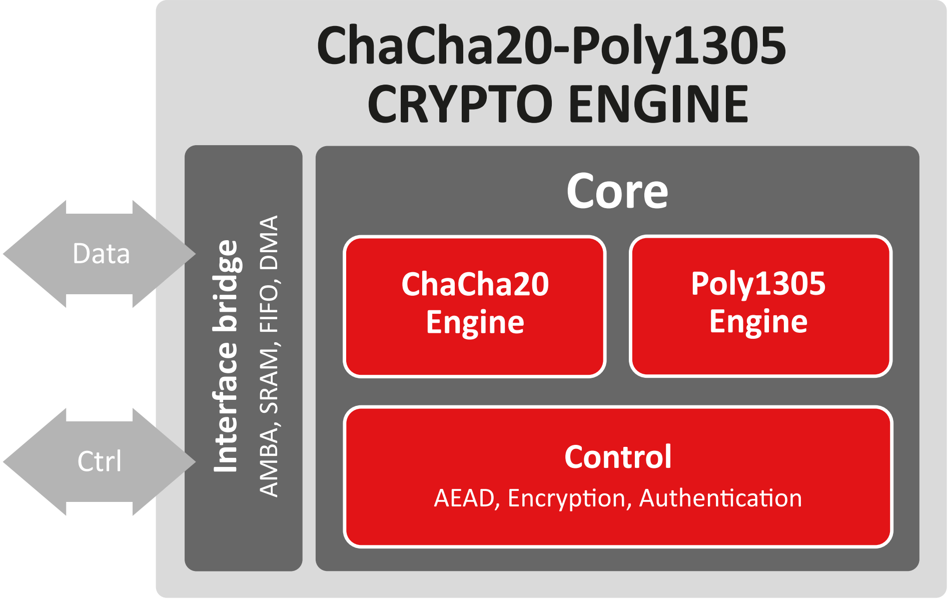
Product sheet
BA417

ChaCha20-Poly1305 CRYPTO ENGINE

The ChaCha20-Poly1305 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.



Features

- ASIC and FPGA
- Fully compliant with RFC7539
- Supports authentication and encryption mode (AEAD)
- Supports stand-alone encryption/decryption (ChaCha20)
- Supports stand-alone authentication (Poly1305)
- Context switching
- AMBA AHB/AXI bridges (with optional scatter/gather DMA)
- Low power features
- Key generation for Poly1305
  - ChaCha20
  - Dedicated input
- Full synchronous design

Applications

- TLS/DTLS
- OpenSSH
- IPsec

Implementation aspects

The ChaCha20-Poly1305 Crypto Engine is available for ASIC and FPGA, with simple interfaces and easy to integrate. It supports a wide range of applications on various technologies. The IP Core can be combined with scatter/gather DMA and AMBA interfaces (AHB/AXI) enabling multi-Gbps 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