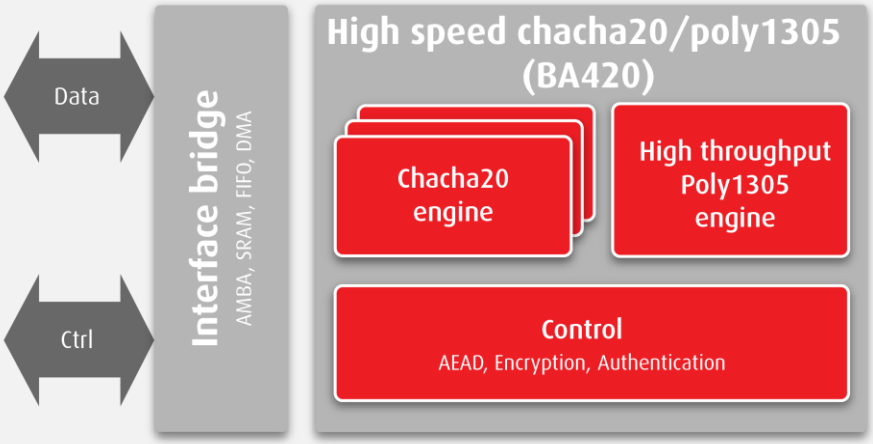
ChaCha20 Poly1305 HP Cryptography

BA420
Product sheet

The BA420 Chacha20-Poly1305 IP core is a RFC7539 compliant crypto engine to provide Authenticated Encryption with Associated Data (AEAD) using the Chacha20 stream cipher combined with the Poly1305 message-authentication code. The ChaCha20-Poly1305 HP IP core is available for ASIC and FPGA devices. It has simple interfaces and is easy to integrate. The maximum throughput of this high performance (HP) IP exceeds several hundred of Gbps and the separate engines can be fully configured to match the specific throughput requirements of the application.



Implementation aspects

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 IP Core can be combined with scatter/gather DMA and AMBA interfaces (AHB/AXI) enabling multi-Gbps throughput in SoC solutions.

This IP Core is also available in the BA470 eSecure IP solution.

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA

Features

- Fully compliant with RFC7539
- Supports encryption/decryption only (Chacha20)
- Supports authentication only (Poly1305)
- Supports authentication and encryption mode (AEAD)
- Default AXI4 stream interface
- AMBA AHB/AXI bridges with optional scatter/gather DMA)
- FPGA (Altera, Xilinx, Microsemi) and ASIC (TSMC, UMC, GF…) technologies
- Low power features
- Key generation for Poly1305
  - ChaCha20
  - Dedicated input
- Full synchronous design

Applications

- TLS/DTLS