CERBERUS

Security Laboratories

Product Overview

ChaCha20-Poly1305 Accelerator

PUBLIC

Product overview

Feature summary

- Very fast throughput, 1.6 bytes/cycle for the base configuration
- Scalable to ultra-high speeds
- Fully autonomous packet processing capability
- Constant time implementation to prevent timing attacks
- Cryptographically masked version available for enhanced side-channel attack (SCA) protection
- Optional secret key table with protected key delivery bus for use with a hardware key manager
- Suitable for both ASIC and FPGA
- Further customisation available upon request

IP Overview

Chacha20-Poly1305 is a symmetric authenticated cipher with associated data (AEAD). It requires a 256 bit secret key and a unique per-operation value called a nonce, a number used once. As well as performing encryption or decryption, the cipher produces a 16 byte message authentication code (MAC) tag that can be used to validate the protected data.

This cipher was introduced as an alternative to AES-GCM and has gained much traction in the industry, particularly in resource-constrained environments. For example, it is now widely used to secure TLS sessions in Android devices.

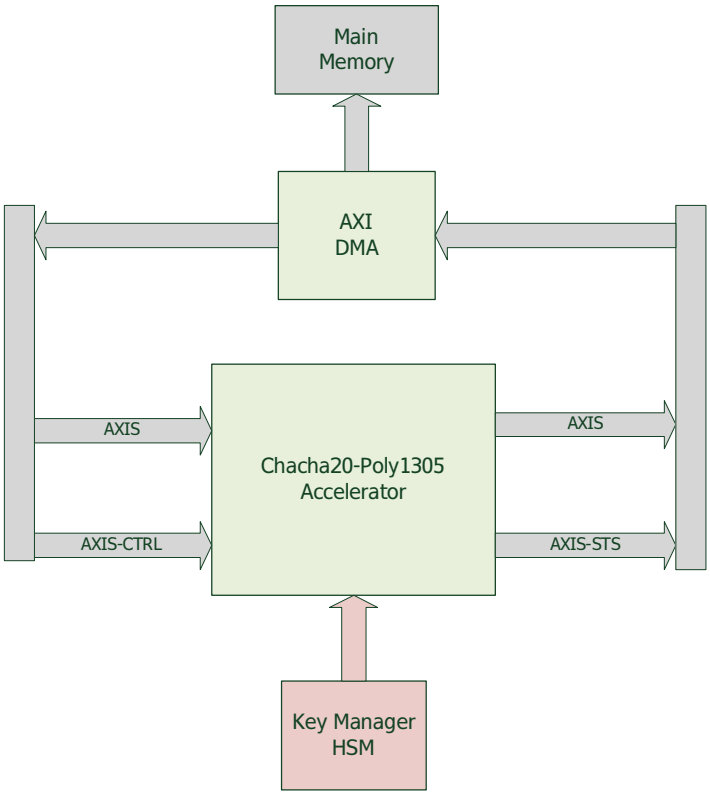
The Cerberus Chacha20-Poly1305 accelerator is a configurable hardware IP core capable of delivering high speed AEAD performance. The engine is provided as an AXI stream accelerator and can be driven entirely via a DMA engine and linked list using the AXI stream control and status interfaces. Alternatively, control may be managed through a traditional register interface such as an AXI4L slave port.

In addition to Chacha20-Poly1305, XChaCha20-Poly1305 is also supported, which better supports the use-case where the nonce is a randomly generated value.

The engine is capable of directly processing payloads that include associated data headers without CPU intervention, and ultra-high speeds are possible using advanced configurations that exploit parallel computation.

For more information, contact sales@cerb-labs.com

Product overview



Example Configuration

Value-added services

Based on your exact requirements, Cerberus deliver a fully tailored IP solution, suitable for ASIC or FPGA integration.

Cerberus are also able to offer a bespoke software driver development service to our customers.

We are happy to work closely with customers at an early stage, to help review their requirements, derive appropriate threat models and mitigations, and formulate a suitable security system architecture.

Contact details

Email: sales@cerb-labs.com

Phone: +44(0)117 214 1405

Web : https://cerberus-laboratories.com