CERBERUS

Security Laboratories

Product Overview

Elliptic Curve Accelerator

PUBLIC

Product overview

Feature summary

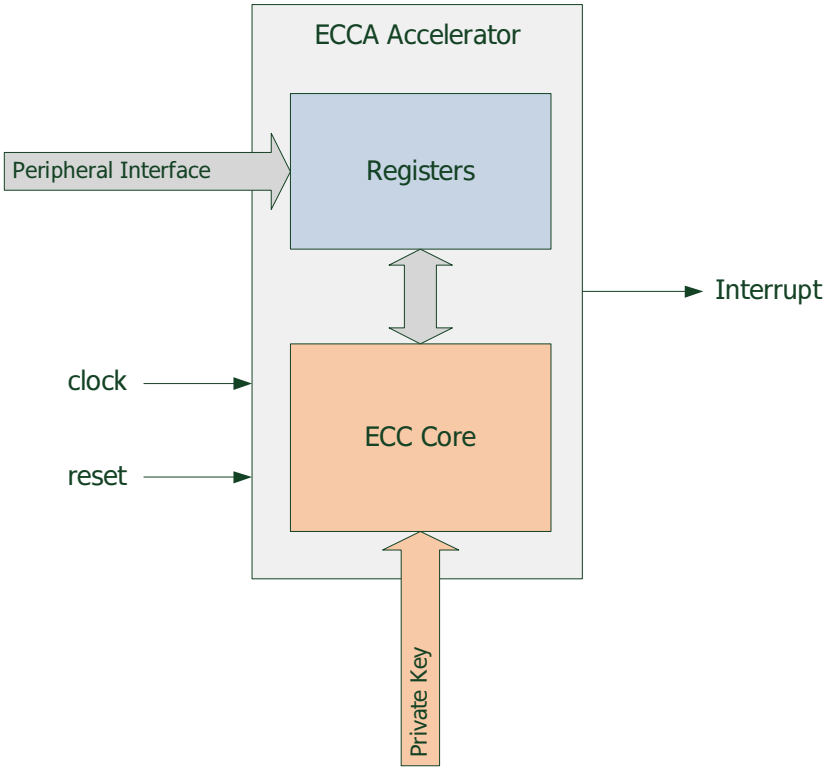
- Configurable bit width and modulus
- Operation over any prime field GF(p) within the configured bit width
- EC point arithmetic operations over any prime curve
- ECDSA/EdDSA sign and verify and ECDH
- Built-in side channel attack (SCA) countermeasures for resistance against timing attacks, doubling attacks and power analysis (SPA/SEMA and DPA/DEMA)
- Configured via a memory mapped register interface, AXI options available
- Optionally, a private hardware key may be wired to the IP, not readable via the register interface
- Our flexible micro sequencer allows for extensive customisation and new feature support if required
- Suitable for both FPGA and ASIC implementation
- Various size versus performance options available upon request

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

Product overview

IP Overview

The Cerberus Elliptic Curve Cryptography (ECC) accelerator is a configurable hardware IP core capable of delivering high speed elliptic curve point arithmetic over any prime field. It is thus compatible with all NIST prime curves as well as any other prime field alternative. Examples are Ed25519, SM2 and the Brainpool family of curves. It may be used for encryption, decryption, signing and verification operations and in the implementation of common standards such as ECDSA, EdDSA and ECDH.



ECC Accelerator IP

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.

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

Product overview

Contact details

Email: sales@cerb-labs.com

Phone: +44(0)117 214 1405

Web : https://cerberus-laboratories.com