SILEX INSIGHT

Product sheet
BA414EP

FIPS COMPLIANT 140-2

PUBLIC KEY CRYPTO ENGINE

The Public Key Crypto Engine is a versatile IP core for hardware offloading of all asymmetric cryptographic operations. It enables any SoC, ASIC and FPGA to support efficient execution of RSA, ECC-based algorithms and more. The IP core is ready for all ASIC and FPGA technologies.

Complete asymmetric cryptography support

Elliptic Curve Cryptography (ECC) operations

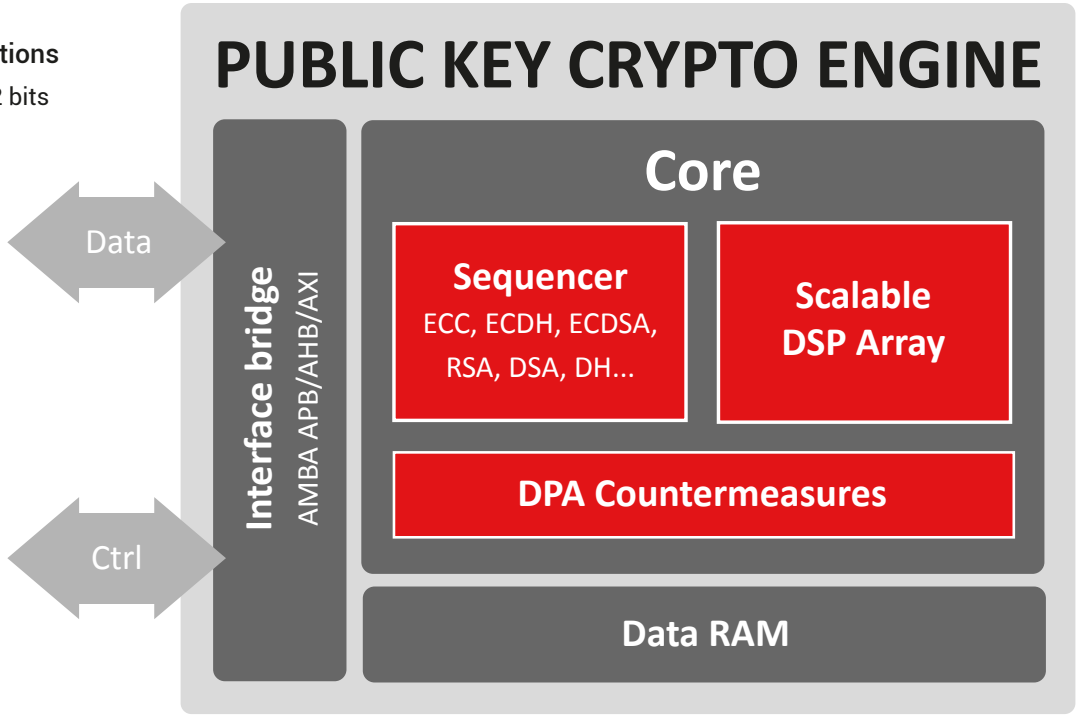
- ECC operations up to 571 bits in F(p) and F(2^m)
- ECDSA and ECDH support
- NIST, Brainpool, Koblitz curves, Montgomery, Edwards, Twisted-Edwards, SM2 and other curves

Other operations

- Curve25519/Curve448, EdDSA/Ed448, SRP and others
- Special operations: J-PAKE, ECMQV, ECIES, ECKCDSA
- Rabin-Miller (primality check)
- PQC

Modular Exponentiation operations

- RSA and RSA-CRT up to 8192 bits
- DSA and Diffie-Hellman (DH)



Features

- ASIC & FPGA (Xilinx, Intel, Microchip, Lattice...)
- RSA, ECC and more
  - ECDH, ECDSA
  - DSA, DH
  - SM2, SM9
- 100% CPU offload
- DPA countermeasures
- Very small footprint & high performance

Applications

- MPU/MCU Crypto acceleration
- Hardware Security Module (HSM)
  - Car-to-X
  - Banking
  - Government
  - Enterprise VPN
- Industrial communications
- Networking security
  - TLS/SSL
  - IPsec
  - Diffie-Hellman

100% CPU offload asymmetric cryptography

The Public Key IP core is the perfect companion to your processor or microcontroller. It executes high level operations (ECDSA, Diffie-Hellman…) completely stand-alone. The host controller does not need to interact with the Public Key IP core except for configuring the operation and reading out the result.

Scalable architecture matching any application

The core processing unit is scalable in performance and resource allowing both very high performance and very small configurations. The granularity of these configurations guarantees the best trade-off between technology, performance and area.

DPA and Timing attack resistance

By construction, the IP is protected against timing attacks. DPA countermeasures are available for both ECC and RSA operations. With DPA countermeasures, the cryptographic operations are strongly protected against side channel attacks.

Low resource usage and high performance

Thanks to its scalable architecture, the Public Key IP core can have a very low gate count delivering the most power efficient way to execute ECC/RSA algorithms in ASIC.

In terms of FPGA resources, it fits into the smallest FPGAs. Latest FPGA devices such as the Intel Arria 10/Stratix 10, Xilinx UltraScale+ and others enable extremely low execution time.

Custom operations possible on request

The flexibility of the architecture enables us to implement custom algorithms and schemes. For more information, please contact us.

Software Interfacing

To easily interface the IP core with your software application, several solutions are possible. A Linux Kernel Module (LKM) and OpenSSL engine are available. An OS-Independent software library is also available for small MCU and bare-metal software integration.

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking test-bench based on FIPS vectors
- Documentation

The Public Key Cryptography IP core is available in our **eSecure Root-Of-Trust** (BA470), **Crypto Coprocessor** (BA450) and **TLS Handshake Accelerator/Blockchain accelerator** (BA452).

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