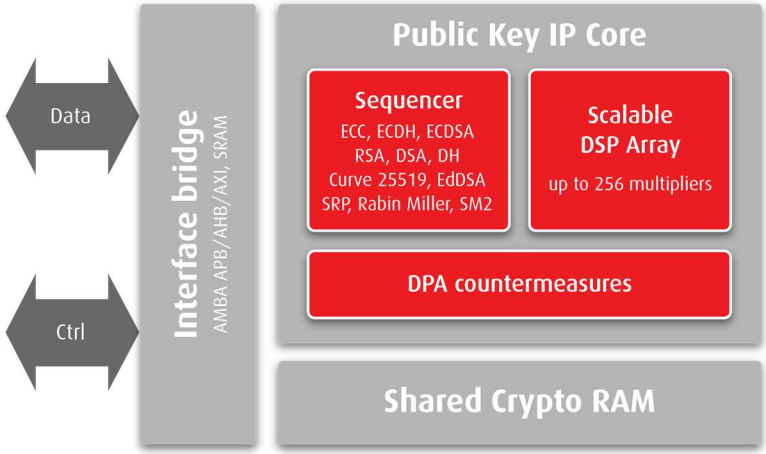
Public Key Cryptography IP core

BA414EP
Product sheet

The Public Key Cryptography IP core is a versatile IP core for 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(2m)
- ECDSA and ECDH support
- NIST, Brainpool, Koblitz curves, Montgomery, Edwards, Twisted-Edwards, SM2 and other curves

Modular Exponentiation operations

- RSA and RSA-CRT up to 4096 bits
- DSA and Diffie-Hellman (DH)

Other operations

- Apple HomeKit support (Curve25519, EdDSA/Ed25519, SRP)
- Special operations: J-PAKE, ECMQV, ECIES, ECKCDSA
- Rabin-Miller (primality check)

Custom operations possible on request

The flexibility of the architecture enables us to implement custom algorithms and schemes. For more information, don't hesitate to contact us.

100% CPU offload asymmetric cryptography

The Public Key IP core is the perfect companion to your processor or

Features

- RSA, ECC and more
  - ECDH, ECDSA
  - DSA, DH
  - Apple HomeKit
  - SM2
- Very small footprint in ASIC and FPGA
- High performance on low-end FPGA
- 100% CPU offload
- DPA countermeasures
- FPGA and ASIC

Applications

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

microcontroller. It executes operations completely stand-alone. The host controller doesn't need to interact with the Public Key IP core except for configuring the operation and reading out the result. This is also true for higher level operations such as ECDSA and Diffie-Hellman.

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. Silex Insight is part of the Rambus-CRI developer ecosystem.

Low resource usage and high performance

Thanks to its scalable architecture, the Public Key IP core can have a gate count as low as 17k gates delivering the most power efficient way to execute ECC/RSA algorithms in ASIC.

In terms of FPGA resources, it fits into the smallest FPGAs families (Altera, Xilinx and Microsemi). Latest FPGA devices such as the Altera Arria 10 and Xilinx Ultrascale enable extremely low execution time:

- 145µs for one ECDSA-256 verification with NIST P-256 curve
- 110µs for one RSA-1024 CRT operation

Software integration

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