RSA5X Core

RSA/Elliptic Curve Accelerator Core

General Description

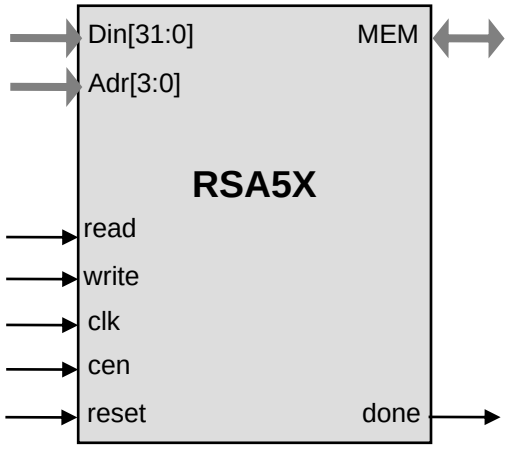
Rivest-Shamir-Adelman (RSA) is a public-key cryptographic technology that uses the mathematics of so called “finite field exponentiation”. The operations necessary for the RSA cannot be efficiently implemented on an embedded CPU, typically requiring many seconds of the CPU time for signature verification. RSA5X implements by far the most time-consuming operation of the RSA cryptography: so called “exponentiation” to enable low-power operation high-speed operation.

RSA5X-4096-32-3 is targeted toward mid-performance applications (hundreds of RSA operations per second at typical clock rates).

RSA5X also supports finite programmable field arithmetic for both prime (GF(p)) and, optionally, binary (GF(2^m)) Galois fields of sizes from 96 bits to 576 bits to support the elliptic curve cryptography (ECC) calculations.

The design is fully synchronous and uses microprocessor-friendly interface.

Symbol



Key Features

Small size: RSA5X starts from less than 100K ASIC gates (size depends on the core configuration)

Implements a modular RSA exponentiation engine; CPU assistance is only required for programming parameters and reading the results.

Implements a microprogram-driven interface for the finite field arithmetic. Microprograms consist of three-address operations, are stored in the external memory, and can be invoked by the CPU. CPU assistance is only required for writing the microprograms into memory programming parameters and reading the results.

32 bit-wide microprocessor-friendly register-based interface. **done** output can be connected to the interrupt pin of the CPU.

Self-contained, except for the external single-port memory

Test bench provided

Applications

- Secure communications systems
- Digital Rights Management (DRM) for battery powered electronics
- Digital Signature using Reversible Public Key (rDSA) standard ANSI X9.31
- Digital Signature Standard (DSS) FIPS-186
- PKCS RSA cryptography per RFC 2347
- High performance RSA accelerators
- Elliptic curve cryptography per FIPS 186-3, NIST SP800-56A, SEC 1 and SEC 2 standards

Pin Description

Name	Type	Description
clk	Input	Core clock signal
reset	Input	HIGH level asynchronously resets the core
Din[ ]	Input	Core input data
Dout[ ]	Output	Core output data
A[ ]	Input	Address for the core memory or on-chip registers
read	Input	Core read request
write	Input	Core write request
MEM	I/O	Memory interface
done	Output	HIGH level indicates a completion of computation

Function Description

The core implements the exponentiation operation of the RSA cryptography $Q = P^k$. The operands for the exponentiation: k and P as well as the modulus are programmed into the memory and the calculation is started. Once the operation is complete, the result Q can be read through the interface.

Elliptic curve support via microprograms stored in the internal memory. SDK provides microprograms for the popular curve types, including all NIST and SECP curves.

Export Permits

The core is subject to the US export regulations. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and licensing details.

Deliverables

- Synthesizable Verilog RTL source code
- Software SDK for complete RSA, CRT, DH, ECDH, DSA, and ECDSA implementation
- Verilog testbench (self-checking)
- Test harness and simulator for software modules
- Vectors for testbench and test harness
- Expected results
- User Documentation

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com