RSA1-E Core

RSA Exponentiation Accelerator Core

General Description

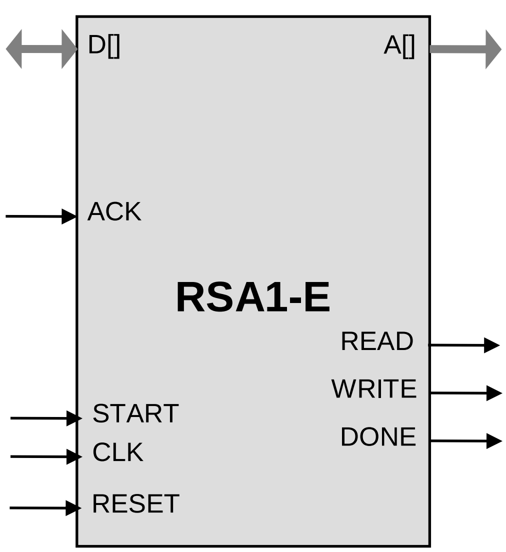
Rivest-Shamir-Adelman (RSA) is a public-key cryptographic technology that uses the mathematics of so called “finite field exponentiation”.

The operations necessary for the RSA cannot be efficiently implemented on an embedded CPU, however, typically requiring many seconds of the CPU time for signature verification.

RSA1-E implements by far the most time-consuming operation of the RSA cryptography: so called “exponentiation” to enable low-power operation of the battery-powered devices.

The design is fully synchronous and available in multiple configurations varying in bus widths, set of finite fields supported and throughput.

Symbol



Key Features

Small size: RSA1-E starts from less than 5K ASIC gates (size depends on the core configuration)

Implements the computationally demanding parts of RSA public key cryptography for long life battery powered applications

Support for RSA binary fields of configurable bit sizes up to 3072

Microprocessor-friendly interface

Test bench provided

Applications

- Secure communications systems
- RFID
- Implantable medical devices
- 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

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
START	Input	When HIGH, starts a Point Multiply or Point Verify operation
RESET	Input	HIGH level asynchronously resets the core
READ	Output	Read request for the memory
WRITE	Output	Write request for the memory
DONE	Output	HIGH level indicates a completion of computation
D[ ]	I/O	Memory data bus
A[ ]	Output	Address for the memory
ACK	Input	Read/write acknowledgement from the memory

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 through the microprocessor interface and the calculation is started. Once the operation is complete, the result Q can be read through the interface.

Design of RSA1 allows sharing of the arbitrated CPU memory to store the arguments and results of operations. This feature both helps to save the silicon resource in the extremely compact implementations (smart cards) and simplify the data transfer between the CPU and the ECC1 core. If sharing memory is not desirable, an optional dedicated memory can be used.

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

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Software modules for a complete RSA implementation (optional)
- Verilog testbench (self-checking)
- Software modules test harness
- Vectors for testbench and harness
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbench
- Expected results

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