ECC7

Elliptic Curve Processor for Prime NIST Curves

General Description

Elliptic Curve Cryptography (ECC) is a public-key cryptographic technology that uses the mathematics of so called “elliptic curves” and it is a part of the “Suite B” of cryptographic algorithms approved by the NSA.

The design is fully synchronous, with the exception of the seed part, and available in both source and netlist form.

The core is supplied as portable Verilog (VHDL version available) thus allowing customers to carry out an internal code review to ensure its security.

Key Features

ECC7 implementation is unencumbered by any patents

Support for NIST and NIST-like curves. For generic curves, see ECC8 family. Each core in the family is specialized for a single NIST curve (e.g., ECC7-P256 for P-256) or switchable between few curves.

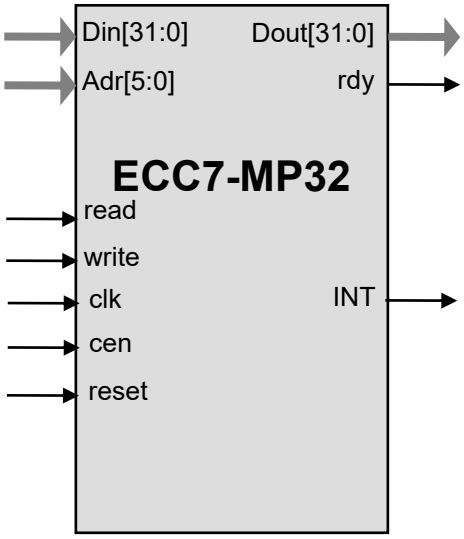
High throughput for long life battery powered applications: more than 1,000 point multiplications per second at 100 MHz clock

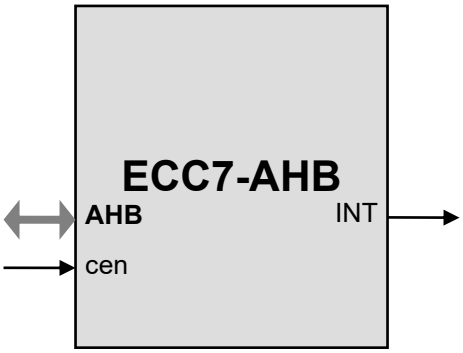
Support for NIST prime curves P-192, P-224, P-256, P-384, or P-521

Microprocessor-friendly interface. AHB wrapper available.

Test bench provided

Symbols





Applications

- Secure communications systems
- RFID
- Implantable medical devices
- Digital Rights Management (DRM) for battery powered electronics
- Elliptic Curve Diffie-Hellman (EC-DH) standard ANSI X9.63
- Blockchain processing
- Elliptic Curve Digital Signature Algorithm (EC-DSA) standard ANSI X9.62
- Digital Signature Standard (DSS) FIPS-186
- IEEE P1363
- TLS implementations per RFC 4492
- Cryptographic messaging per RFC 3278
- Windows Digital Right Management
- HDCP 2.x

Pin Description

Name	Type	Description
CPU interface		
Adr[5:0]	Input	Address
Din[31:0]	Input	Write data
Dout[31:0]	Output	Read data
read	Input	When HIGH, read operation
write	Input	When HIGH, write operation
rdy	Output	Ready bit for microprocessor. Deasserted when data is not available for reading.
INT	Output	HIGH when data processing is completed or an exception occurs
Generic		
clk	Input	Core clock signal
reset	Input	Asynchronous core reset signal
cen	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
AHB Bus		
Hsel	Input	HSELx
Haddr[12:0]	Input	HADDR
Hwrite	Input	HWRITE
Htrans[1:0]	Input	HTRANS
Hsize [2:0]	Input	HSIZE. The core only accepts the size value of 010 (32 bits)
HwData [31:0]	Input	HWDATA
HRESETn	Input	HRESETn
clk	Input	HCLK
HreadyIn	Input	HREADY input signal

Name	Type	Description
HreadyOut	Output	HREADY output signal
Hresp [1:0]	Output	HRESP. The core does not use the 10 (RETRY) and 11 (SPLIT) responses.
HrData[31:0]	Output	HRDATA
		HBURST[2:0]. Ignored (do not even need the pins)
		HPROT[3:0]. Ignored (do not even need the pins)

Function Description

The core implements either a point multiplication operation and the point verification operations, or (optionally) a complete digital signature operation (signing or signature verification).

For the point multiplication version, the operands for the multiplication (k, P_x, P_y) are pushed into the core before the start of operation. Once the operation is completed, the result, Q_x, Q_y can be read from the core.

For the ECDSA version, for signing the input parameters (z, d, k) are pushed into the core and there (r,s) result can be read. For signature verification (z, Q_x, Q_y, r, s) are the input parameters. Here z is the hashed message, d is the private key, k is the nonce, r and s constitute the signature, Q_x, Q_y constitute the public key. A wrapper integrating multiple ECC7 cores with the hash cores and random number generators is available.

The curve and digital signature selections are fixed for the particular version of the core, for example the ECC7-P256-ECDSA-V core works with the NIST binary curve P-256 and implements the signature verification for the ECDSA algorithm.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the ECC cores. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Verilog self-checking test bench
- Test vectors and expected results as text files
- Software SDK
- 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