

Elliptic Curve Cryptography (ECC) relies upon the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) and was proposed by Miller and Koblitz in 1985. The advantages of ECC over classical cryptosystems like RSA/Diffie-Hellman (D-H) include higher speed, lower power consumption, less bandwidth, and less storage requirements. The CLP-17 offloads the computationally difficult aspects of Elliptic Curve calculation and can be tailored to the application with build options that span low power hand-held requirements to high-performance designs for Ethernet passive optical networking (EPON) systems.

Key Features:

- Offloads the computationally intensive parts of ECC public key cryptography
- Options for various ECC key/field sizes: 163, 191, 233, 283, 409 & 571
- Build options for different performance levels – e.g. for 163 bit key/field size:
 - 1,900 ECC-DH/s in 45K ASIC gates
 - 12,700 ECC-DH/s in 115K ASIC gates
 - 33,000 ECC-DH/s in 240K ASIC gates
- Acts as a processor peripheral
- Support for NIST EC B and K curves (163, 233, 283, 409, 571)
- Support for IEEE P1363 for curves in $GF(2^m)$

Applications:

- IPsec and SSL Consumer Gateways and VPN products
- Low Power Portable Web Clients (PDA, Cell Phones)
- Portable Media Devices (DRM component)
- Smart Cards
- Ethernet passive optical systems (EPON)
- Government and military communications systems

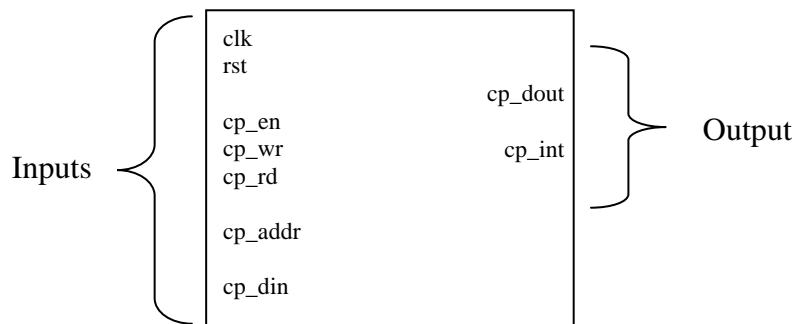


Figure 1 CLP-17 Block Diagram

Pin Description

Signal Name	Width (Bits)	Direction	Description
<i>System Pins</i>			
clk	1	input	System clock. All inputs are sampled on the rising edge of the clock.
rst	1	input	Asynchronous reset. All internal state returns to default value upon assertion (active high) of this signal.
<i>Control Interface</i>			
cp_en	1	input	Enable pin for the interface. All other inputs are ignored unless this pin is asserted.
cp_addr	10	input	Address to perform a read or write. This bus must be valid any time cp_wr or cp_rd (qualified with cp_en) are asserted.
cp_wr	1	input	Write signal for the data on cp_din and address on cp_addr.
cp_rd	1	input	Read signal for the address on cp_addr.
cp_din	32	input	Data to write. This bus must be valid any time cp_wr (qualified with cp_en) is asserted.
cp_dout	32	output	Result of a read.
cp_int	1	output	Core ready interrupt. Indicates that the last calculation has ended and the core is idle.

Table 1 CLP-17 Pin Description

General Description

The Elliptic Curve Cryptosystem (ECC) is a method based on the Discrete Logarithm Problem over points on an Elliptic curve. ECC has so far shown no weakness and as such several algorithms have been created primarily in asymmetric or public-key cryptography for key exchange and digital signature applications. The most common algorithms are:

- Public Key - Elliptic Curve Diffie Hellman Key Exchange (EC-DHKE)
- Public Key - Elliptic Curve ElGamal (EC-ElGamal)
- Digital Signature - Elliptic Curve Digital Signature (EC-DSA)

The primary advantage of the ECC algorithm over the comparable RSA public key algorithms is reduced key size (and relative increase in speed of processing). A comparison between the ECC/D-H and RSA/D-H algorithms is presented in the following table.

ECC –DH Key/Field Size (bits)	Equivalent Security with RSA/D-H (bits)	Ratio
163	1024	1:6
256	3072	1:12
512	15360	1:30

Table 2 ECC/D-H Key Size and Equivalent Security RSA/D-H Key Sizes

The underlying equation in Elliptic curve mathematics is specified as:

$$y^2 + xy = x^3 + ax^2 + b \quad (\text{non-supersingular curve of characteristic 2}).$$

The primary operation involved in the ECC algorithm and protocols is Elliptic Curve Point Multiplication; the CLP-17 core provides hardware acceleration and processor offload for this complex operation. The CLP-17 core is customized for a specific m as in $GF(2^m)$ and the curve can be modified using the a and b parameters. The parameter m indicates the key/field size of the ECC implementation.

Core Usage:

The CLP-17 block diagram is shown in Figure 2. The core acts as a processor peripheral and is controlled by manipulating control registers and by writing ECC parameters into

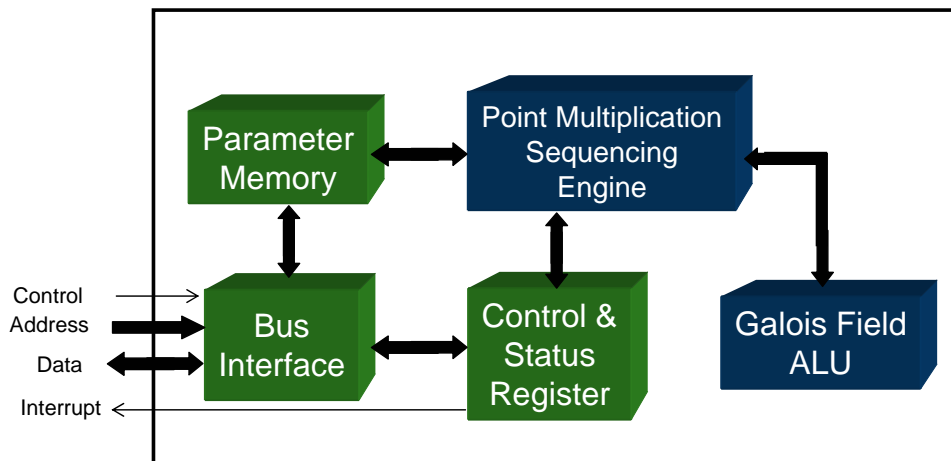


Figure 2 CLP-17 Block Diagram

the core memory through the bus interface. The results of the calculation are also stored in the parameter memory and can be accessed through the bus interface.

In general, the Elliptic Curve coefficients a and b are fixed for a specific application and as such are entered into the core once and remain unchanged thereafter. For each Point Multiplication Operation: $Q(x_{res}, y_{res}) = k P(x, y)$, the processor must provide the following parameters by writing the internal memory of the core:

- k - m -bit integer ($k = 1, n-1$; where n is the order of point P)
- x - m -bit x affine coordinate
- y - m -bit y affine coordinate.

The results - coordinates (x_{res}, y_{res}) , are stored back into x, y memory locations and can be accessed by the processor through read operations.

The resulting sequence of operation of the core is:

1. The processor reads the core status register to determine if the core is busy
2. The processor optionally writes parameters a and b into core memory
3. The processor writes parameters k, x and y into core memory
4. The processor asserts the go parameter in the core control register
5. The processor then either polls the busy parameter in the core status register or waits for a core interrupt to indicate that the computation is complete
6. When the core is finished the computation, the processor can then retrieve x_{res} and y_{res} in the core memory location where x and y were originally written

Performance and Core Sizes:

The following table indicates a subset of the performance options for the CLP-17.

ECC Key Size (m in $GF(2^m)$)	ECC-DH (operations/s)	Gate Count (K Gates)	Clock Rate (MHz)
163	250	35	200
163	1,900	45	200
163	12,700	115	200
163	33,000	240	200
191	180	40	200
191	1,400	50	200
191	10,900	135	200
191	29,000	325	200

Table 3 Core Size versus Performance

The core performance scales approximately linearly with clock speed – please contact Elliptic Semiconductor for precise details of the performance for different clock speeds and key field sizes.

Elliptic offers supporting software and drivers for the CLP-17 in C source code for Linux, embedded Linux and VxWorks. The software is constructed to be easily portable to other environments.

The CLP-17 is available in soft IP form, either as a netlist or HDL Source. The deliverables available are:

Netlist Licenses:

- Post synthesis EDIF netlist
- Testbench
- Sample simulation script
- Documentation

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load can be made available under license or through the Elliptic evaluation card – the EVAL-01 for evaluation purposes. For more information on pricing and a full data sheet, please contact:

Elliptic Semiconductor Inc.
62 Steacie Drive, Suite 201
Ottawa, ON, K2K 2A9

Phone: +1 613 254-5456
Fax: +1 613 254-7260
Email: info@ellipticsemi.com