

Public Key Crypto Engine

BA414PKE

Key Features

- 1 • Hardware execution of complex arithmetic operations for Public Key algorithms;
- 2 • Flexible synthesizable core optimized for low cost FPGA families and ASIC solutions, allowing customers to get the best possible trade-off between performance and area;
- 3 • Dual Field Arithmetic Unit including:
 - 4 - one Modular Montgomery Multiplier (MMM) based on a flexible array of 16x16-bit Multipliers;
 - 5 - one removable very efficient 256 or 512-bit Unified Modular Divider (UMD);
- 6 • μ Code Driven State Machine with pre-defined algorithms (several are available; extensions possible);
- 7 • Internal scatter/gather DMA to interface with the external crypto memory;
- 8 • Very simple host interface & handshake mechanism;
- 9 • Size of operands, parameters & types of elliptic curves configurable by software;

Host/Memory Interface

- Very simple 16-bit Host Interface;
- Classical handshake mechanism;
- All parameters, control & command signals programmable on the fly;
- Requires maximum 128-kbit external memory for storage of operands and transient results;
- 64-bit Memory Interface with internal DMA;

PK Features

- Dual Field $GF(p)$ & $GF(2^m)$ Arithmetic Unit;
- Supports arbitrary Data/Key Size (up to 4096 bits);
- Supports all operations for RSA & Elliptic Curve;
- Supports all types of recommended elliptic curve equations (NIST);
- Gives assistance for other useful complex operations;
- Automatic precomputation of initial parameters;
- All long numbers stored in external memory;

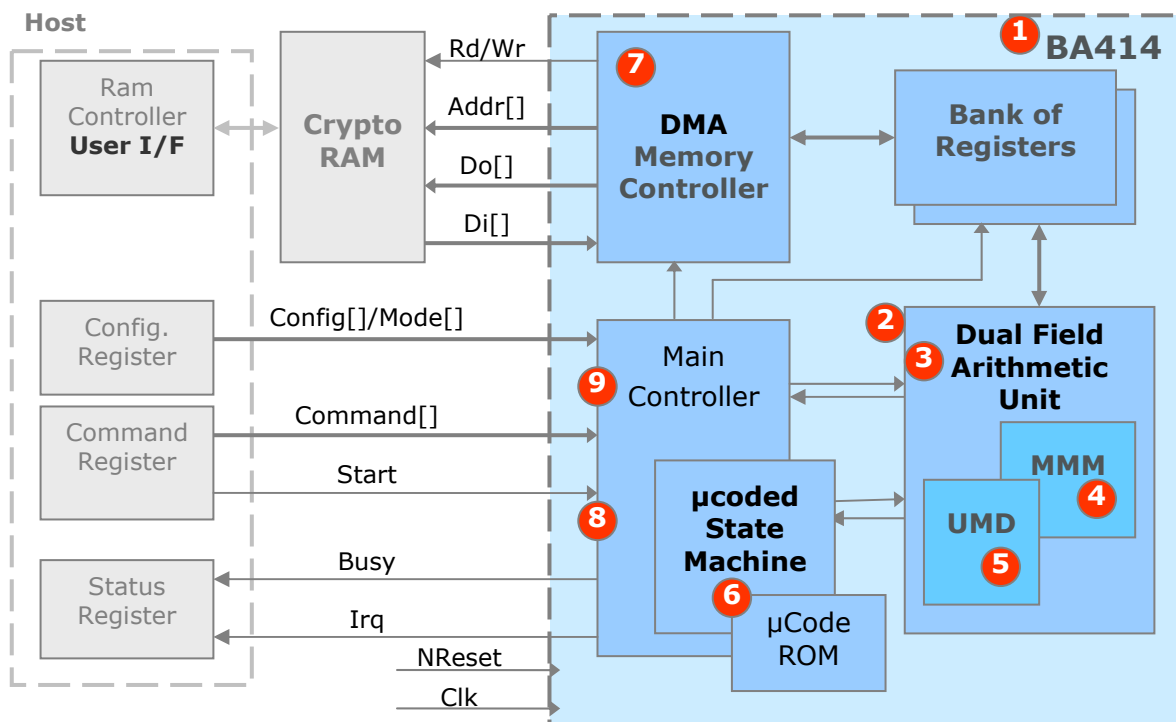


Figure 1 - Typical System Configuration using the BA414 Crypto Engine

General description

The BA414 is a flexible and high performant Public Key Crypto Engine developed, validated & licensed by BARCO-Silex. All features & complex arithmetic operations needed for the execution of both RSA & ECC algorithms are supported.

Dual Field Arithmetic Unit

The BA414 includes fast hardware required for the execution of arithmetic operations in both fields $GF(p)$ & $GF(2^m)$ on very large numbers (up to 4096 bits):

- one Modular Montgomery Multiplier(MMM) based on a flexible array of 8, 16, 32 or 64 multipliers;
- one removable very efficient 256 or 512-bit Unified Modular Divider (UMD);

Control Unit

As shown in figure 1, the BA414 includes a scatter/gather DMA and a μ Code driven State Machine with the targets to offload the processor from all control tasks and to make the integration in your design very easy:

- The internal DMA is used to collect all needed input data from the external crypto memory and write back the data upon completion of cryptographic operations;
- μ Code driven architecture offers the possibility to implement high-level & customizable algorithms;
- Very simple interface to the host processor with classical handshake solutions;

Applications

- PKI, RSA, Diffie-Hellman, ...
- Digital Signature
- Secure Electronic Transactions (e-banking, e-commerce)
- IPS (Internet Protocol Security), SSL (Secure Sockets Layer), TLS (Transport Layer Security) protocol implementations

Technical description

Supported Functions & Algorithms

Supported Functions			
	Function	Description	Max. Size Operands
✓	ADD/SUB	Modular or Regular Addition/Subtraction	4096
✓	MMM/MEXP	Modular Montgomery Multiplication/Exponentiation	4096
✓	MUL	Multiplication	2048
✓	MDIV	Fast Modular Division	512
✓	MINV	Modular Inversion	4096
✓	ECCADD	Point Addition $ECC\ GF(p) / GF(2^m)$	512
✓	ECCDBL	Point Doubling $ECC\ GF(p) / GF(2^m)$	512
✓	ECCMUL	Point Multiplication $ECC\ GF(p) / GF(2^m)$	512
✓	Verification	Input/Output point on curve, at infinity for ECC- $GF(p) / GF(2^m)$...	512
✓	Others	Pre-calculation of initial parameters(*) Modular Reduction Any custom complex arithmetic function (CRT, ...)	Any

(*) $RSq=R^2 \bmod N$ or $N0p.N = -1 \bmod 2^w$ in $GF(p)$ or $1 \bmod x^w$ in $GF(2^m)$

Table 1 – Supported Functions & Algorithms

Configurable Parameters

✓	Type of Operation, Field GF(p) or GF(2 ^m), Size of operands, ...	Config[], Mode[], Cmd[]
✓	Parameters of elliptic curves, use of Affine or Projective coordinates,...	from µCode

Table 2 - Configurable Parameters

Generic Parameters

The BA414_PKE can be tailored to get the best possible trade-off between performance and area:

Generic Parameters	
Parameter	Description
MMMConfig	Number of 16x16-bit Multipliers used: 8, 16, 32 or 64
UMDConfig	Size of UMD Core: 0 (not implemented), 256 or 512 bits

Table 3 - Generic Parameters

Some examples of possible HW Configurations

HW Configurations (1)			
Config	MMM	UMD	Comment
1	32 x 16-bit MUL	512-bit	High-performance solution for RSA-4096 & ECC-512
2	16 x 16-bit MUL	256-bit	Low cost solution for RSA-4096 & ECC-256
3	64 x 16-bit MUL	None	Very High-performance solution for RSA (up to 4096) (2)
4	16 x 16-bit MUL	None	Low cost solution for RSA (up to 4096) (2)

(1) Any other configuration is possible

(2) Possibility to implement ECC functions with projective coordinates

Table 4 – HW Configurations

Performances

Performances – Config 2				
Function	Description	Size Operands	Cycles/Op	Op/s @100MHz
MEXP	Modular Montgomery Exponentiation	1024-bit Full Expo	860k	116
		4096-bit Full Expo	48M	2.1
MDIV	Fast Modular Division	256-bit	512	195k
ECCMUL	Point Multiplication for ECC	256-bit	450k	222

Table 5 – Performances – Config. 2

FPGA Implementation

Device	Slices	BRAM (ucode)	MULT	Fmax (MHz)	Config
XC3S5000-5	15k (45%)	8	32	66	1 High-performance RSA & ECC
	11k (33%)	8	16	66	2 Low cost RSA & ECC
	9k (27%)	4	64	66	3 Very High-performance RSA
	7k (20%)	4	16	66	4 Low cost RSA

The external crypto Ram is not included

Table 6 – FPGA Implementation

ASIC Implementation

Technology	Gates	RAM/ROM (ucode)	MULT	Fmax (MHz)	Config
0.13µm	230k	16 kbytes	Included	100	1 High-performance RSA & ECC
	125k	16 kbytes	in	100	2 Low cost RSA & ECC
	270k	8 kbytes	Gate	100	3 Very High-performance RSA
	85k	8 kbytes	Count	100	4 Low cost RSA

The external crypto Ram is not included

Table 7 – ASIC Implementation

Maturity/Silicon-proven

- All features fully validated on FPGA (Spartan3 XC3S5000-5)

Deliverables

- Compiled model available on request for evaluation;
- RTL/VHDL/Synchronous Design;
- TestBench;
- Documentation;

Signals description

Refer to the datasheet document for a more detailed description.

Barco Silex overview

Barco Silex is a micro-electronic design house located in Belgium and France belonging to the Belgian Barco group.

Barco Silex offers a complete portfolio of high-end design services, from ASIC/FPGA design to advanced SoC/SoPC based system development, IP-core design and board design in the fields of:

- image processing
- communications
- consumer electronics
- industrial electronics.

Barco Silex IP products

Barco Silex design expertise is also made available through a wide portfolio of IP products, with a strong focus on high performance, standardized image processing and encryption functions.

All these IP cores have been designed and fully validated by Barco Silex and are hardware proven, which guarantees high IP quality as well as best support during your integration phase.

Deliverables include:

- RTL Code or netlist (depending on license type)
- Functional simulation testbench
- Synthesis script
- Full documentation

For some of them, we can also provide you with simulation models and a design kit.

These "off the shelf", high quality IP cores provide you with the fastest and most efficient way of integrating complex functionalities on FPGAs or ASICs, while meeting short time to market constraints.

More information

Order-reference: **BA414PKE**

For additional information and other IP products contact:

Barco – Silex

e-mail: barco-silex@barco.com

<http://www.barco-silex.com>

or the local Barco Silex design centers:

Belgium

Scientific Park
Rue du Bosquet 7
1348 Louvain-la Neuve
+32(0)10/45.49.04

France

ZI Peynier- Rousset
Route de Trets Imm CCE
13790 Peynier
+33(0)44/216.41.06