

Public Key Crypto Engine

○ Description

- The BA414E is a scalable Public Key Crypto Engine developed, validated & licensed by Barco Silex. Based on the concept of "Smart Engine", it does not require any assistance from the main CPU to handle the complete processing

○ Portability

- ASIC, Actel, Altera, Xilinx

○ Key Features

- High-level of scalability
- Supports all arithmetic operations in both fields $F(p)$ & $F(2^m)$,
 - Modular or normal Addition/Subtraction
 - Modular Multiplication/Division/Inversion
- Supports arbitrary data/key sizes up to 4096 bits
- Supports all standard PK crypto primitives:
 - Modular Exponentiation (RSA)
 - Point Doubling/Addition/Multiplication for ECC- $F(p)$ & $F(2^m)$
- Supports high-level PK Algorithms:
 - RSA & RSA-CRT, Key Generation (Primality Test Procedure)
 - Elliptic Curve Cryptography (ECC – NIST Curves)
 - Digital Signature Algorithm (DSA) & Elliptic Curve DSA (ECDSA)
- Pre- & post-processing automatically executed by the core

○ Interfaces

- Control Interface: APB-compliant / AXI4-lite
- Data Interface: Generic Memory Interface with internal DMA

○ Independent Technology Figures

| Number of Operations / sec (@ 100MHz) (*) | | | | | |
|---|------------------------------------|---|-------|--------|------------|
| Size | Operation | HW Configuration - Number of Xers or DSP Blocks | | | |
| | | 4 | 16 | 64 | 256 |
| 256-bit | ECDSA - Sign | 84 | 223 | 476 | - |
| | ECDSA - Verify | 42 | 111 | 238 | - |
| 1024-bit | RSA - Sign Full Exp | 33 | 116 | 377 | On request |
| | RSA - Verify $\text{Exp}=2^{16}+1$ | 1,200 | 4,200 | 13,300 | On request |
| | RSA Sign with CRT | 108 | 349 | 1,008 | On request |
| 2048-bit | RSA - Sign Full Exp | 4 | 17 | 59 | On request |
| | RSA - Verify $\text{Exp}=2^{16}+1$ | 317 | 1,200 | 4,200 | On request |
| | RSA Sign with CRT | 16 | 56 | 183 | On request |

(*) Pre- & post-processing included

○ Performance – Size

Refer to DS for more results

- ASIC 90nm (Tiny): < 30kgates, up to 500 1024-bit CRT op/sec
- ASIC 90nm (Fast): Max Freq=500MHz, up to 5,000 1024-bit CRT op/sec
- High-end FPGA: Max Freq=250MHz
- Low-end FPGA: Max Freq=80MHz

○ Benefits

- 100% CPU Offload, no need of extra SW
- Easy-to-use & small footprint solutions
- Off-the-shelf & silicon-proven solution

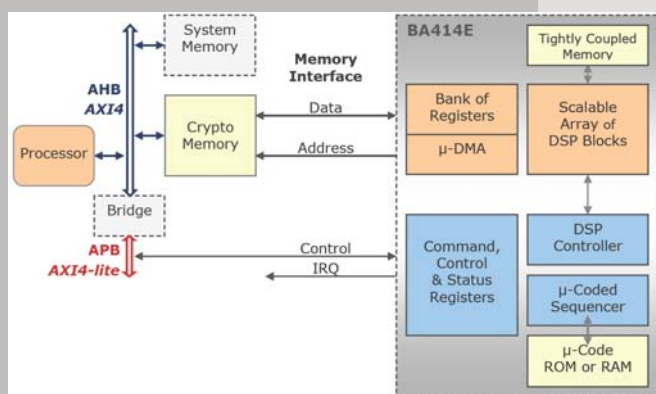
○ Deliverables

- RTL or netlist
- Scripts for synthesis
- Self-checking Testbench based on FIPS vectors

For more information contact:

e-mail: barco-silex@barco.com
www.barco-silex.com

International : + 32 (0)10 454 904
 France : + 33 (0)1 47 38 30 89



BA414E - Typical Configuration using the BA414E Crypto Engine