Les FPGA pour des applications à très hautes performances

CETIC: groupe de discussion sur la technologie FPGA

Thierry Watteyne, Jean-Marie Cloquet

le 5 décembre 2012

BarcoSilex

BARCO

Visibly yours

Barco Silex: Profile

- Barco Silex is a micro-electronic design house
- We have design offices in Belgium and France
- Barco Silex belongs to the Barco group
- History:
  - **1991: Foundation in Louvain-La-Neuve**
  - **1995: Acquired by Barco**
  - **2001: Creation of Barco Silex France**
  - **2006: First JPEG 2000 IP sales**
  - **2010: First Public Key crypto IP**
  - **2012: Start design team in Ghent**
- Revenues 2011: € 6.3 Mio
- Total people count: 39
- ISO9001-2008

Barco Silex: Main activities / products

- Electronic design services
  - **Highly integrated embedded systems development**
  - **Custom component development**
  - **Specialized in high performance digital signal processing hardware design**
    - ASIC/SoC Design
    - Complex FPGA design
    - PCB level development and PCBA prototyping
- Custom component solutions
  - **“System on a Chip” (SoC) IC development service**
  - **Old obsolete ASIC retargeting solutions**
  - **Sales of resulting IC product, thanks to partnership with silicon manufacturers**
- IPs or Intellectual Property blocks: Firmware for programming, defining custom chips (ASIC, FPGA)
  - **Image compression (JPEG, JPEG 2000)**
  - **Crypto & Security (AES, Public Key, …)**
  - **Memory Controllers**

Barco Silex: Main competence areas

- ASIC/SoC Design
  - **Historical strong Silex competence since 1991**
  - **SoC expertise mostly based on ARM architectures**
    - Fom ARM7 to ARM11 and Cortex families
- Complex FPGA/PLD Design
  - **Strong partnership with Xilinx, Altera & Actel for many years**
  - **Experience with “complex” and “High speed” latest devices**
    - Stratix-4-5, Virtex-7, high speed serial links
- DO-254 compliant design methodology
  - **Strong track record of ASIC and FPGA designs following DO254 with major Avionics players in France (Sagem, Airbus)**
  - **Active member of DO-254 User group (together with Barco D&A)**
- Crypto & Security
  - **Expertise in data encryption derived from many projects done in EPOS applications (Atos, Ingenico)**
  - **Knowledge and IP for all major standard encryption algorithms**
    - AES, Hashing, Public Key, ….
- Video Compression & processing
  - **Strong knowledge of most of image compression standards**
    - JPEG, JPEG 2000, MPEG2, MPEG4, H264
  - **Very advanced products based on JPEG 2000 (IP cores)**
  - **Video over IP reference design**

Barco Silex markets

- Our technologies and competences are applicable in multiple applications and markets.

- Our main markets:
  - **Communications**
  - **Industrial**
  - **Defense & Aerospace**
  - **Broadcast**
  - **Digital Cinema**

BarcoSilex France
+33 4 42 16 41 06

BarcoSilex Belgium
+32 10 45 49 04

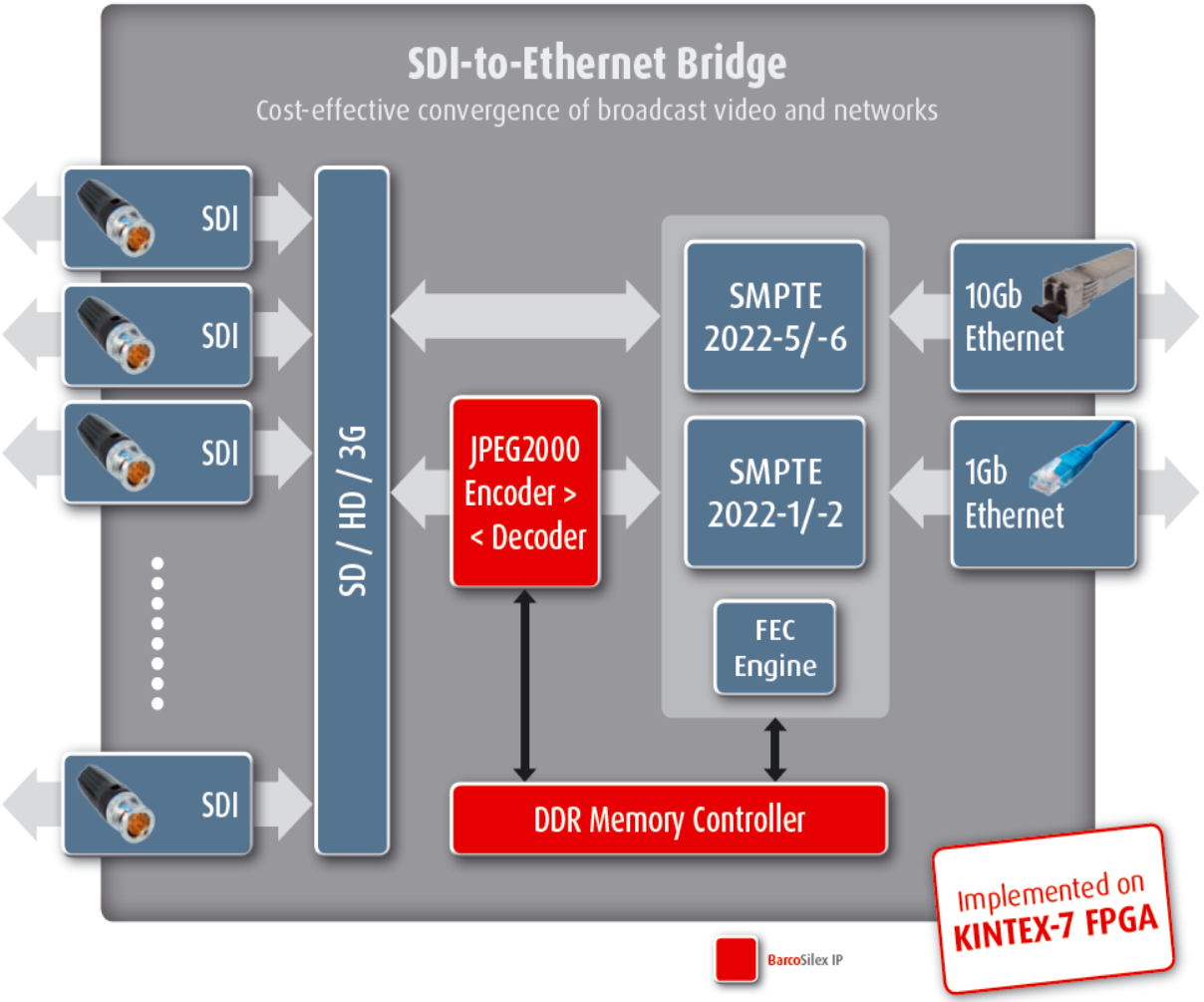
Video over IP solutions

Flexible

Performance and power of **programmability** let FPGAs uniquely bridge between **SDI** and **Ethernet** worlds

Uncompressed or JPEG2000

- **High resolution:** up to HD 1080i and 1080p.
- **High speed**
- **Flexible solutions:** multi-channel support, low latency, low resource usage



Maximizes interoperability

Support for the emerging industry standard **SMPTE 2022-1,2,5,6**

Multiple Channels

Support of **SD/HD/3G-SDI**

Accelerated Productivity

BarcoSilex XILINX

Video over IP reference design: Main features

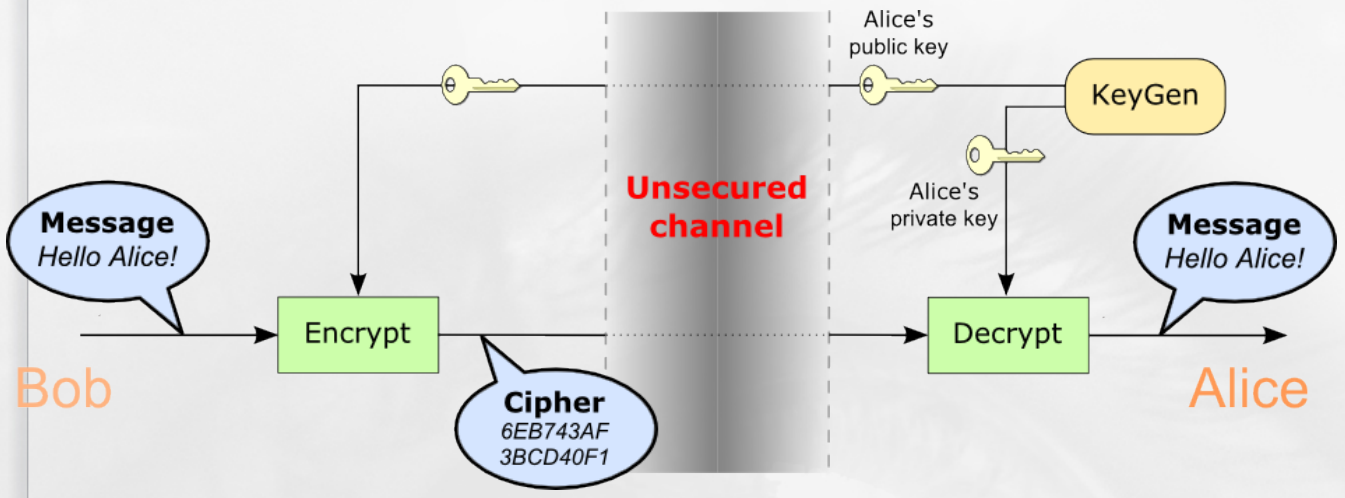
- Multiple SDI video inputs:
  - **Input bandwidth up to 3 Gbps per channel**
  - **Clock frequency = 148,5 Mhz**
- JPEG2000 compression:
  - **Intra compression for very high quality applications**
  - **Complex algorithms, data management…**
  - **Clock frequency = 160 Mhz**
- SMPTE-2022 transport:
  - **Media transport over IP networks with FEC**
  - **Clock frequency = 200 Mhz**
- Ethernet (1Gb & 10Gb):
  - **Copper or optical network interface**
  - **Clock frequency = 156 Mhz**
- DDR memory controller:
  - **Memory controller for high efficiency accesses**
  - **Bandwidth up to 50 Gbps with 'random' accesses**
  - **DDR clock frequency = 800 Mhz**

Why FPGA versus other solutions ?

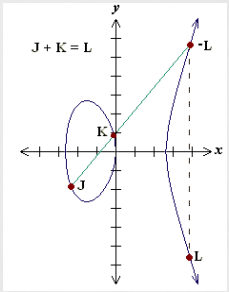
- FPGA vs SW: much higher performances with FPGA
- FPGA vs standard ICs: much more flexible to use and to update:
  - **Can be tuned to customer needs**
  - **SMPTE standard is not finalized but solutions can already be built**
- FPGA vs GPU: higher performance with FPGA with less power consumption
- FPGA vs DSP: higher data rates not suited for DSP

The main FPGA drawback is the development complexity

Smart engine for Public Key
Asymmetric cryptography



A lot of complex arithmetic operations on large numbers and a lot of data transfers



ECC - Point doubling

$c = (3x_1^2+a)/2y_1,$

$x3 = c^2 - 2x_1,$

$y3 = c(x_1-x_3) - y_1,$

ECC - Point addition

$c = (y_2-y_1)/(x_2-x_1),$

$x_3 = c^2 - x_1 - x_2,$

$y_3 = c(x_1-x_3) - y_1,$

→ Public key algorithms (ECC, RSA, ...) are time consuming

2048-bit RSA exponentiation

requires 84.000.000 of 16x16-bit multiplications

Smart engine for Public Key
BA414E

Algorithms (RSA, ECDSA, ...)

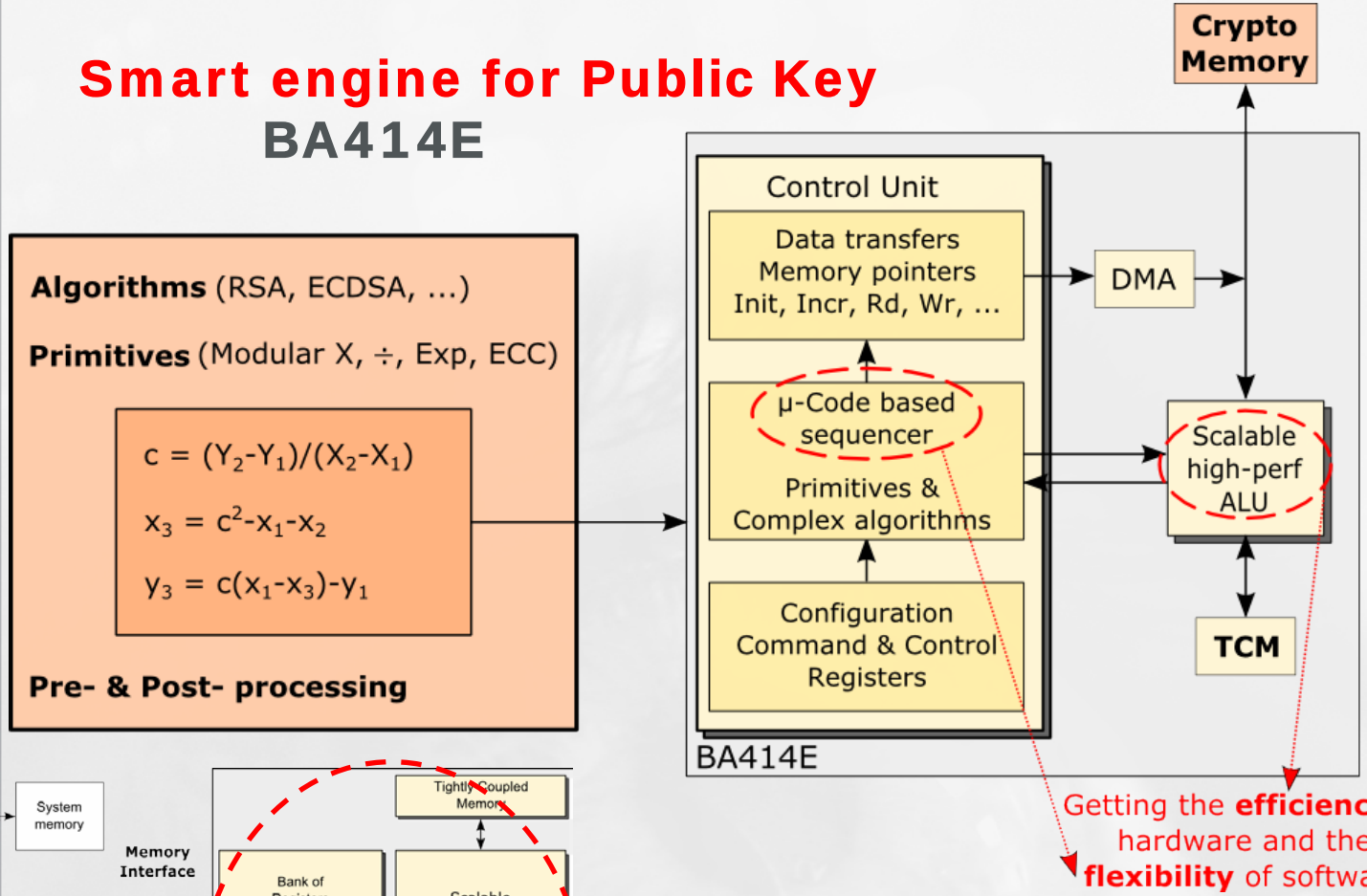
Primitives (Modular X, ÷, Exp, ECC)

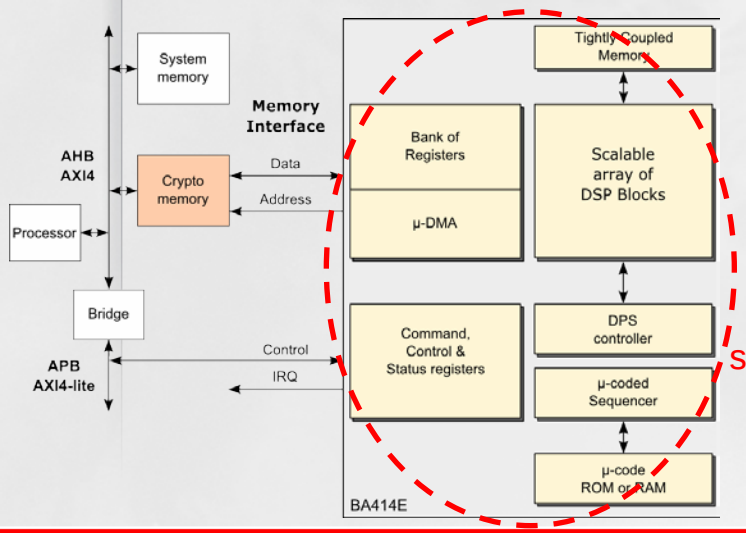
$c = (Y_2-Y_1)/(X_2-X_1)$

$x_3 = c^2-x_1-x_2$

$y_3 = c(x_1-x_3)-y_1$

Pre- & Post- processing





Public Key solution with **less than 33 kgates**

BARCO Visibly yours

Smart engine for Public Key

- 100% CPU offload
  - → **No need of high performance CPU**
  - → **Easy to reach high performance requirements**

- Handles and optimize all memory transfer
  - → **Easier to use**
  - → **Reduce power**

- Higher performance
  - → **Full processing power from hardware solution**
  - → **For instance with 256 multipliers in Stratix4 @ 300 Mhz:**
    - → 1024 b RSA – Full Expon.: -> **3.000 op/sec!**
    - → 256 b ECC – Point Mult..: -> **1.900 op/sec!**
  - → **For comparison, a ARM Cortex A8 @1GHz provides:**
    - → 1024 b RSA: -> **56 op/sec**

Design methodology

- Controlled development flow:
  - **Planning with controlled milestones**
  - **Version control**
  - **Bug tracking system**
  - **Templates, guides,…**
- Focus on validation:
  - **Module and top level simulations with code coverage**
  - **Use XML for CPU register map and generates VHDL, C header and HTML**
  - **Build environment to use same test files for simulation and board testing**
    - **Set of validation scripts in python or C**
    - **C to sim for testbench in simulation**
    - **Build regression tests**

Some concluding considerations about FPGA

- FPGA have become almost unavoidable in embedded systems that require:
  - **High throuput DSP content (high performance real time video, high bandwith communication,….) meaning dedicated hardwired logic.**
  - **Design flexibility (spec evolution, re-programmability, re-configurability,….)**

- Athough they are « relatively expensive » components, they often bring an interesting tradeoff between:
  - **Performance**
  - **Power consumption**
  - **Flexibility**
  - **System integration**

- Developping complex FPGA is a complicated and difficult process that requires stringent and advanced verification methods (Times of « code and try » approach are gone!!)

- Today, we are moving from « FPGA in Embedded Systems » to « Embedded system in FPGA », which is becoming a programmable system:
  - **Xilinx Zynq with embedded dual Cortex A9**
  - **Altera Arria5 or Cyclone5 with embedded dual Cortex A9**