technology
from seed

AES and EC Cryptographic Processor with Runtime Configuration

Leonel Sousa

Technical University of Lisbon/INESC-ID, Lisbon, Portugal

16th December, 2009

Motivation

- **Most electronic devices require security**
  - Applications and devices have to be secure
  - Security/computation in the same device
  - Both asymmetric and symmetric cryptography required

- ***Advanced Encryption Standard* (AES) widely used in symmetric cryptography**
  - Symmetric block cipher, standardized by the NIST (US)

- **EC cryptosystem used in asymmetric cryptography**
  - More security per key bit than RSA (e.g. 163 EC ↔ 1024 RSA)
  - Therefore, smaller keys to be computed, transmitted and stored

Motivation

- **Exploiting TOGETHER reconfigurability …**
  - Design an architecture based on processing modules
  - These modules are independent and autonomous
  - Allow for runtime adaptation to the host requests

- **… and programmability**
  - Control the dedicated hardware with microcode (centralized memory)
  - Support different algorithms (production of keys, signing)
  - Fast and easy to design based on microcode

- **Last but nost the least: “Good” random number generators (RNG)**
  - For private keys generation
  - By integrating in a single device avoids communication of private data
  - Compact random number generation with good statistical properties

Outline

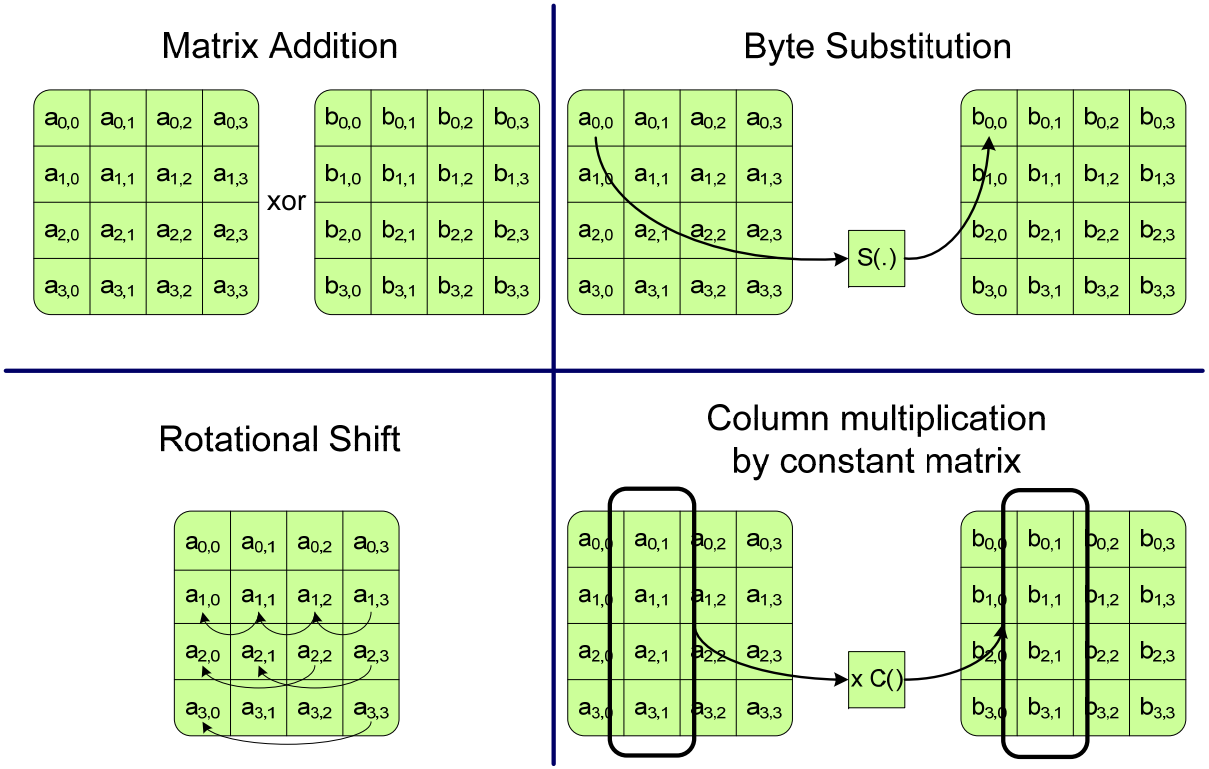
technology
from seed

inesc id lisboa

- Motivation
- **AES and Elliptic Curve (EC) overview**
- Processor design
- Reconfiguration
- Results
- Conclusions

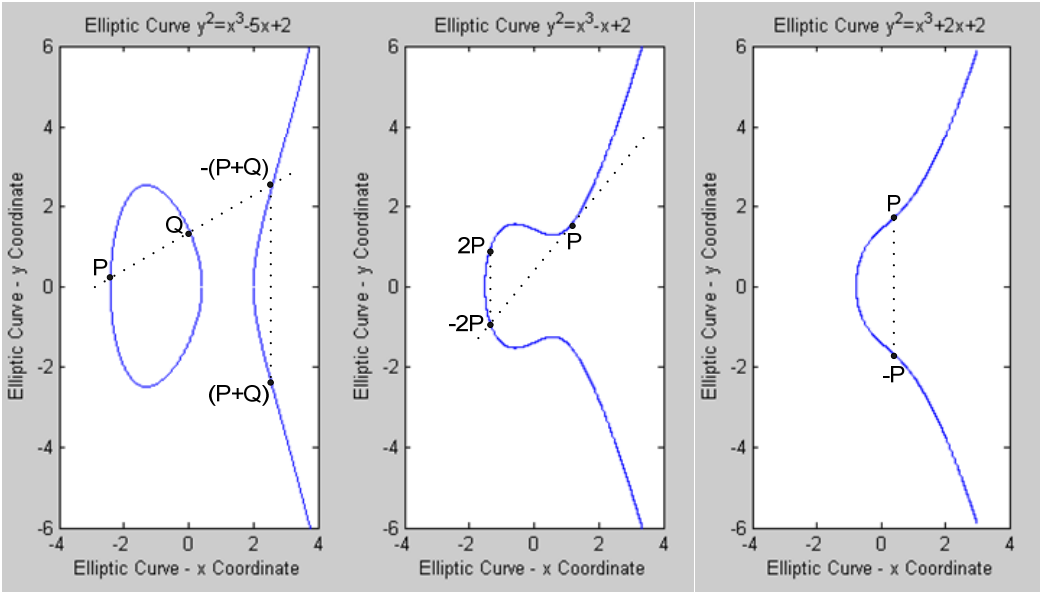
AES and EC Overview

- **AES** is performed over GF(2^8) (8-bit words)
- Data organized in 4x4 matrices
- Simpler and faster than asymmetric cryptography



AES and EC Overview

- **EC** geometrical interpretation

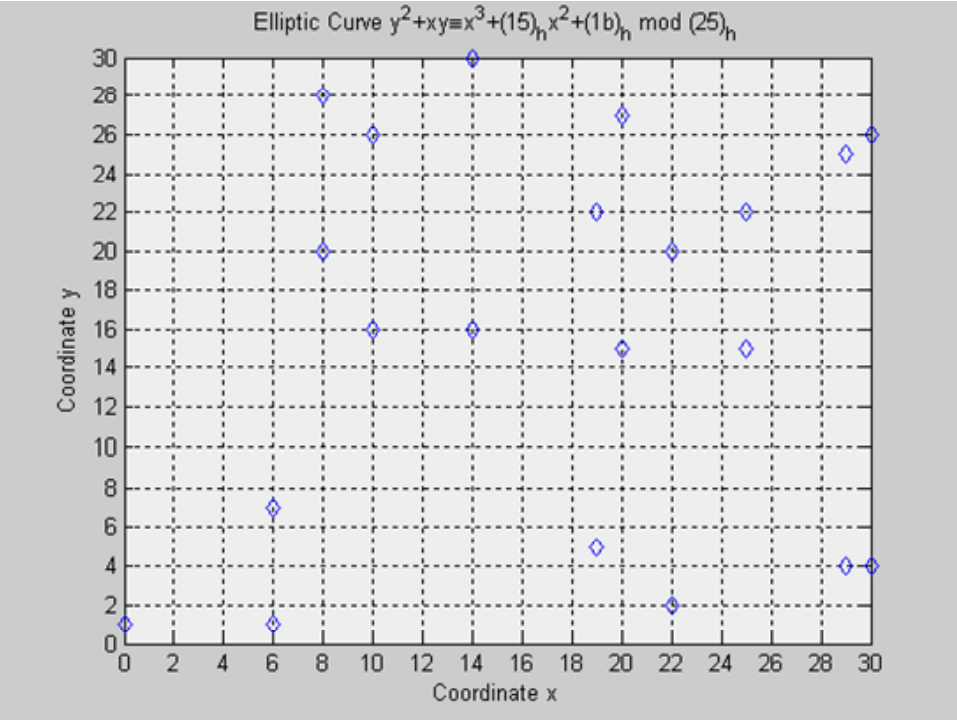


$$Q = kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}$$

EC discrete logarithm problem: it is hard to compute k knowing Q and P

AES and EC Overview

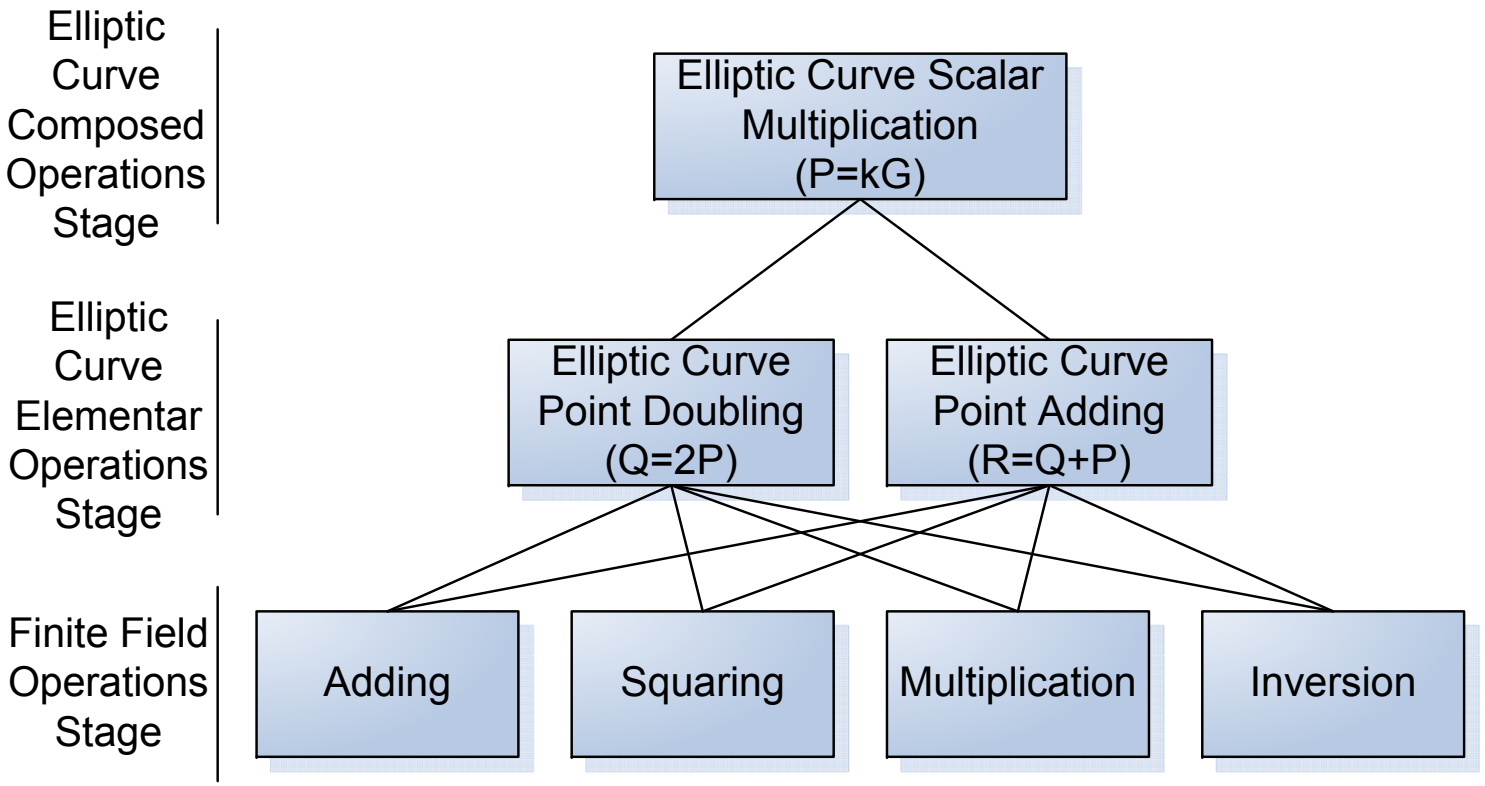
- **EC** over a finite field GF(2^m)



- Extension of a binary field
- Suitable to hardware implementations
- Additions are XOR
- Operations modulo an irreducible polynomial
- Polynomial Basis

AES and EC Overview

- **EC** operations hierarchy



AES and EC Overview

AES + EC: challenges for putting together

- Different datapath width:
  - AES operates over 8 bit elements
  - EC operates over from 163-bit up to 571-bit elements
- Different security scalability:
  - + Secure AES = More rounds in the algorithm over the same data type
  - + Secure EC = Increase the underlying field size (larger elements)
- Different reduction methods
  - AES implementation can avoid reduction methods by table look-ups
  - EC involves direct computation of reduction methods

Processor design

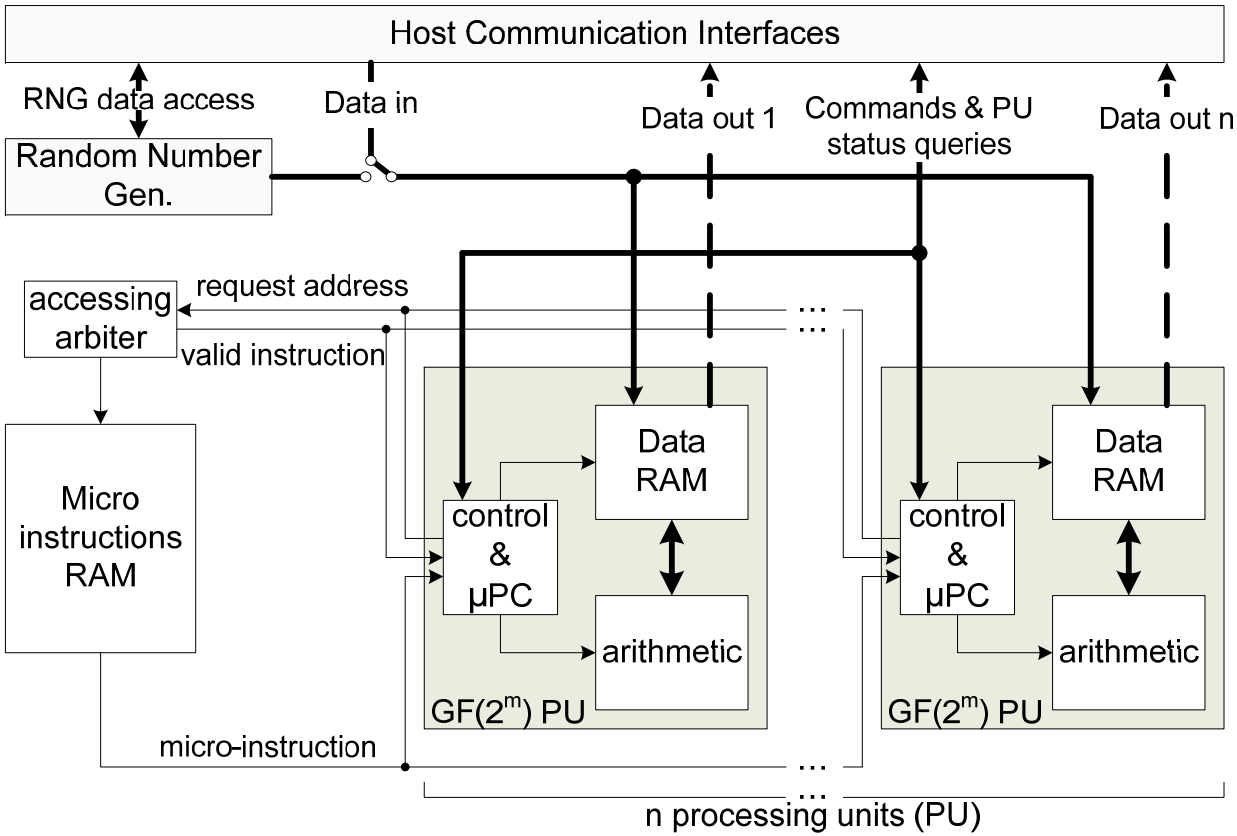
- Motivation
- AES and Elliptic Curve (EC) overview
- **Processor design**
- Reconfiguration
- Results
- Conclusions

Processor Design

- Modular system: PU contains arithmetic units for basic field operations
- Centralized control: single shared instruction memory for all PUs
- Arbiter to solve memory access conflicts
  - PUs operate with multi-cycle instructions
- Architecture allows to easily detach or attach PUs
  - AES PUs and/or EC PUs
  - Adapt to runtime requirements
- Random Number Generator (RNG)
  - Avoiding external communication of private data

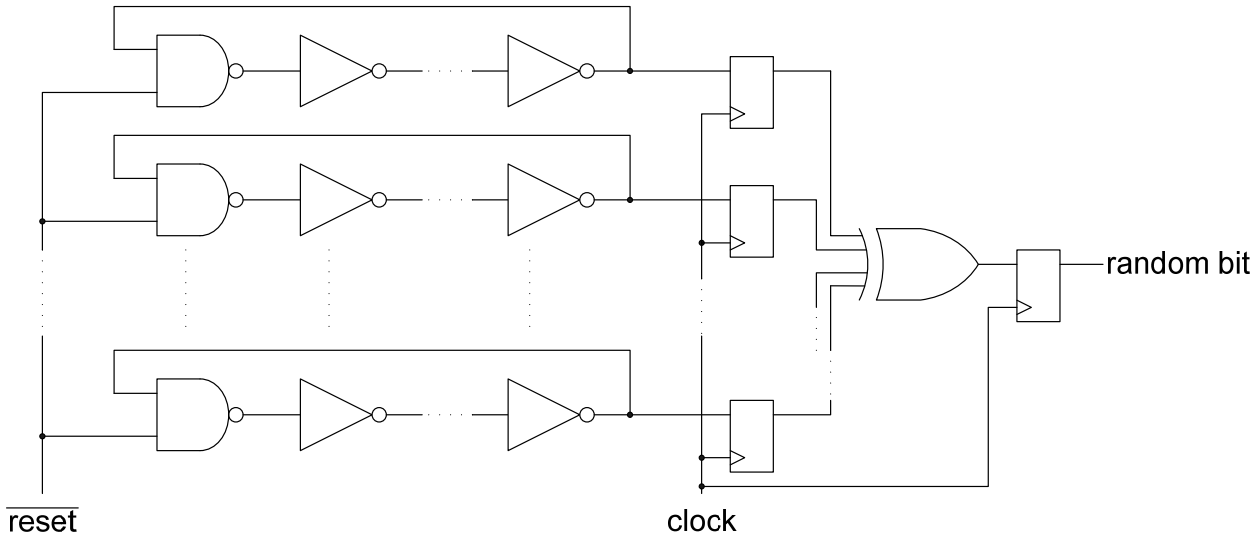
Processor Design

- Different processing units (PUs) sharing a single RAM with microcode



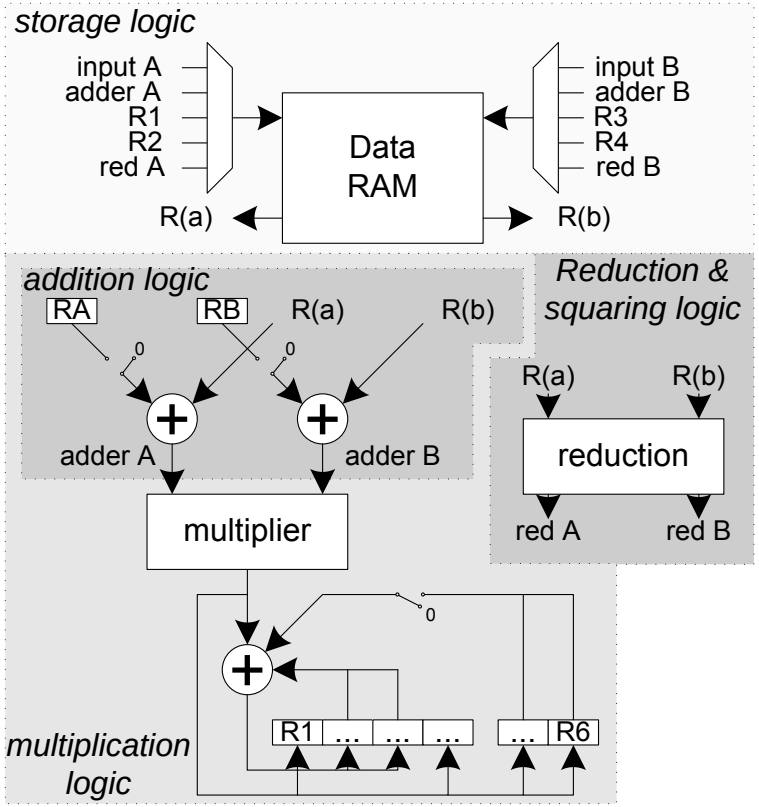
Processor Design

- Random Number Generator (RNG)
  - Use internal jitter noise as randomness source (+oscilators = +randomness)
  - Host can order to write random words to the PUs local memory without accessing them
  - Avoiding external communication of private data increases security
  - RNG can be switched off by asserting a reset signal



Processor Design

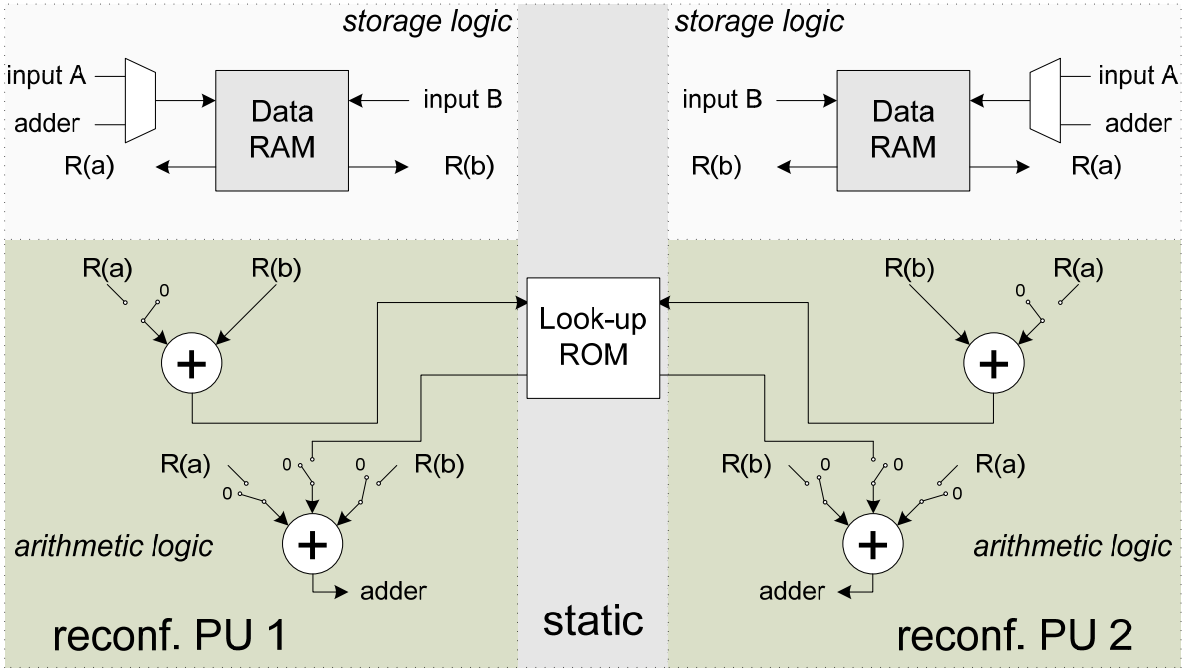
- EC processing unit



- Each field element is decomposed in several words stored in the RAM
- Take advantage of dual port RAMs
- Operations supported:
  - 2-word addition
  - 2-word multiplication (Karatsuba)
  - Field addition
  - Squaring
  - Reduction
  - Conditional jump (key register)
  - Customized field operation

Processor Design

- AES processing unit
  - XOR operation
  - Shared look-up ROM
  - ROM contains the substitution function and constants
  - Jump instructions supported



- Operations Supported (L(.) is a look-up)
  - R(c)=R(a)+R(b)
  - R(c)=R(a)+ L(R(b))
  - R(c)=L(R(a)+ R(b))
  - R(c)=L(R(b))

Reconfiguration

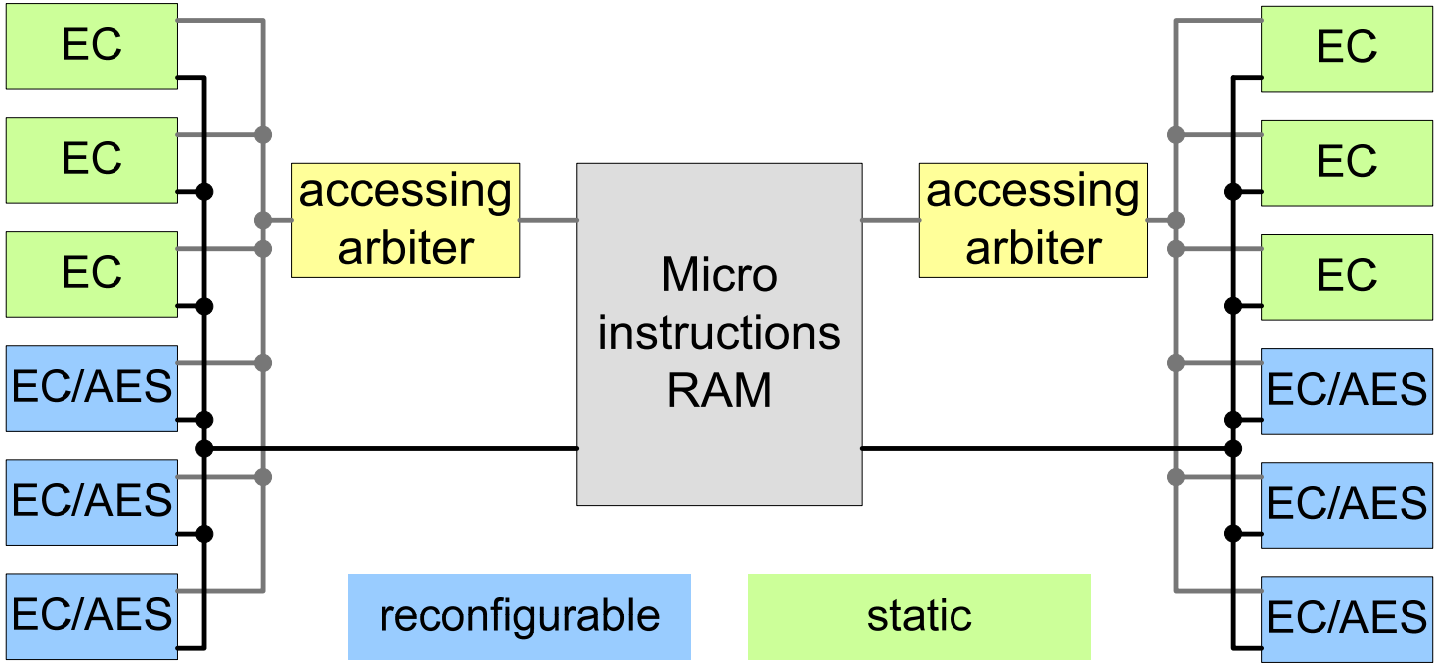
- Motivation
- AES and Elliptic Curve (EC) overview
- Processor design
- **Reconfiguration**
- Results
- Conclusions

Reconfiguration

- Communication logic redirect input data to ICAP while reconfiguring
  (ICAP – Internal Configuration Access Port)
- Support different runtime requirements – trade AES by EC PUs
- Number of PUs limited by the maximum number of AES PUs
  - Number of cycles per instruction in the AES unit (3 cycles)
- Resources to support a PU (reconfiguration zone) limited by EC PUs
  - EC PUs require more resources
  - More complex datapath
- Signals crossing the reconfiguration zone boundaries directly routed
  - 20 bus macros of 8 bit each required

Reconfiguration

- Maximum 3 AES PUs per arbiter = 3 reconfigurable zones per arbiter
- Several static EC PUs (more PUs = more conflicts)
- Compromise of up to 6 operating PUs attached to the same arbiter



Results

technology
from seed

inesc id lisboa

- Motivation
- AES and Elliptic Curve (EC) Overview
- Processor design
- Reconfiguration
- **Results**
- Conclusions

Results

technology
from seed

inesc id lisboa

- Prototyped on a Xilinx Virtex 4 (XC4VSX35-10) device
- Operating frequency: 100 MHz
- Resources:
  - RNG 20 oscillators: 20 CLB (passed statistical tests)
  - Static logic: 8,446 slices, 11 BRAM
    - 6 EC PUs
    - 2 arbiter
    - 1 RNG
    - Communication logic
  - Reconfigurable PUs: 1 BRAM - 157±2 slices (AES) - 943±7 slices (EC)
    - Oscillation in the resources usage – different reconfigurable zones

Results

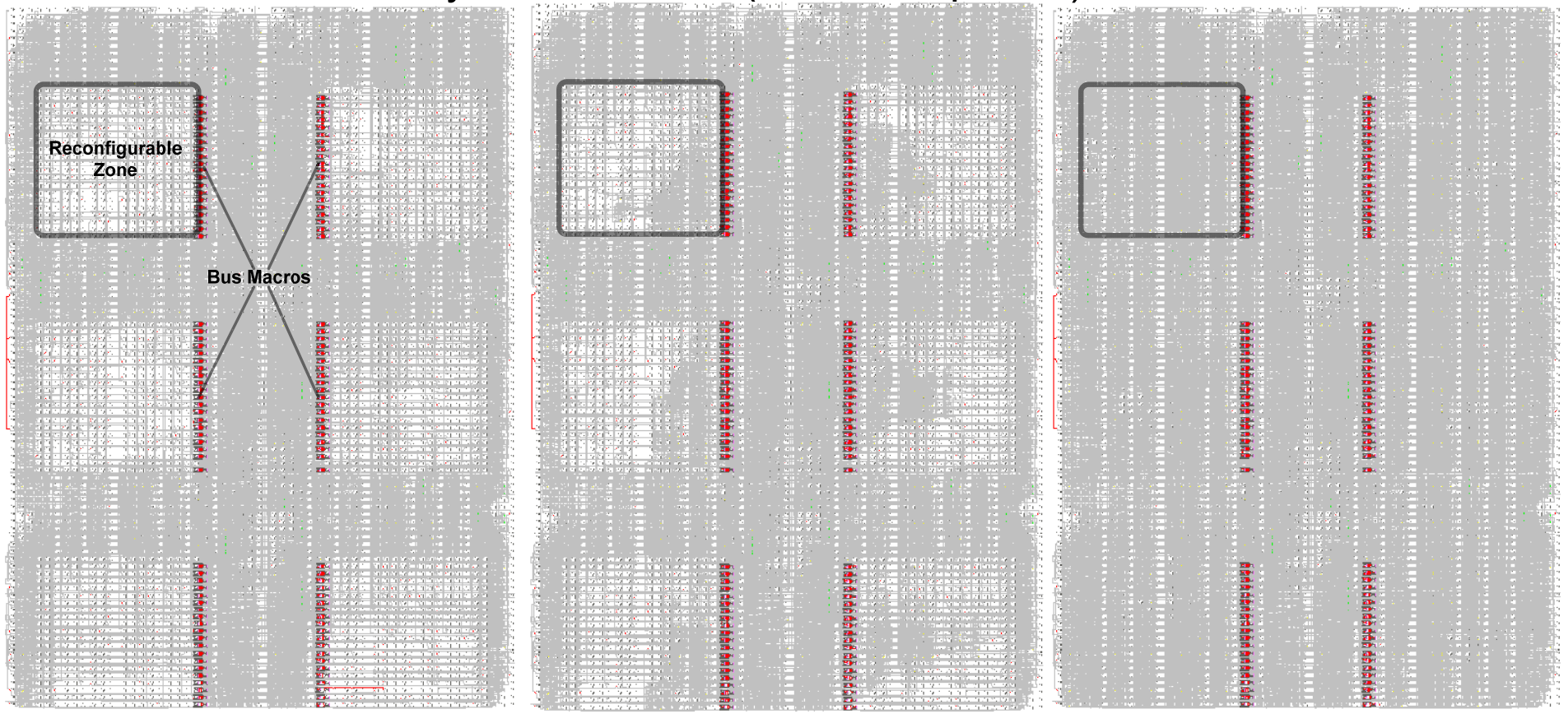
- 13 x 21 CLB reconfigurable zones (1092 slices)
  - 14% usage by AES unit
  - 86% usage by EC unit
  - Resource margin allowing to ease the routing task
- 26 reconfiguration frames per reconfigurable zone
  - Different reconfiguration frames for the different reconfiguration zones
  - Compressed bitstream used to runtime reconfiguration
  - Bitstream size:
    - 29500 x 32-bit words – AES
    - 31067 x 32-bit words – EC
  - PU reconfiguration time (limited by communication): 941µs
    - 310 µs if maximum ICAP frequency used

Results

technology
from seed

inesc id lisboa

- Processor layout after P&R (98% occupation)



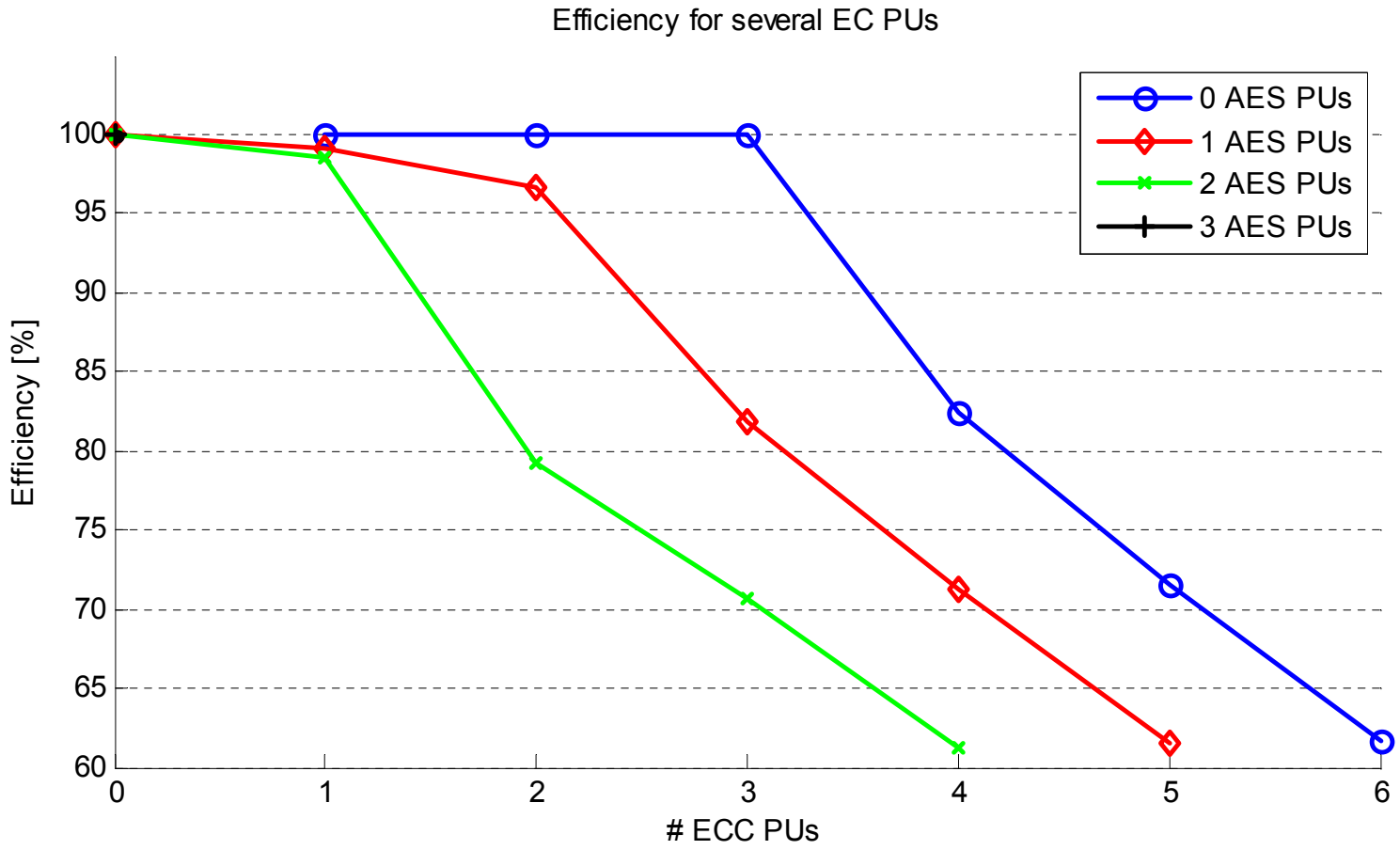
No PUs | AES PUs only | EC PUs only

Results

- Prototype tested with
  - EC arithmetic over GF(2^{163})
  - AES 128-bit key
- Instructions' time
  - AES: 3 clock cycles
  - EC: from 3 to 14 clock cycles
- AES key expansion (610 cc), ciphering/deciphering (2,290 cc)
  - total 253 instructions
- EC point addition (4,796 cc) and point multiplication (201,661 cc)
  - total 401 instructions

Results

- Conflicts solved by an arbiter



Results

- Related art comparison
  - Our performance figures per arbiter (AES cipher. and EC point mult.):
    - Single AES PU throughput: **5.59 Mbit/s**
    - Maximum AES PU throughput: **16.67 Mbit/s (x 2 ports = 33.34Mb/s)**
    - Single EC PU throughput: **496 OP/s**
    - Maximum EC PU throughput: **1536 Op/s (x 2 ports = 3072 Op/s)**
  - Lim et. al. (Xilinx Virtex – 41 MHz)
    - SIMD for EC and SISD for AES
    - Does not support simultaneous EC and AES computation
    - **Our design is 1.4 and 2.65 faster** for AES and EC (considering only one PU)
    - **Our design is 2.1 times more compact**

Results

- Related art comparison (cont.)
  - Wang et. al. (0.18µm ASIC -100 MHz)
    - Share multipliers and register for AES and EC
    - **AES faster but does not support simultaneous AES+EC**
    - **Our design is 1.4 times faster for EC**
  - Good et. al. (Xilinx Spartan 2 – 67 MHz)
    - Compact AES solution
    - Multiply-accumulate and byte substitution unit
    - **124 slices (vs. 157 slices in our AES PU)**
    - **Our throughput is 2.5 times higher (for 1 single PU)**

Conclusions

technology
from seed

inesc id lisboa

- Motivation
- AES and Elliptic Curve (EC) Overview
- Processor design
- Reconfiguration
- Results
- **Conclusions**

Conclusions

- EC + AES processor composed of several PUs sharing a common instruction memory
- Reconfigurability and programmability enhance the flexibility of the processor for different algorithms and protocols
- Architecture allows to easily reconfigure the PUs
  - Runtime reconfiguration allows to adapt the system to the runtime needs
- RNG allows to the internal generation of secrets, enhancing security
- PU's reconfiguration time smaller than EC point multiplication
  - Reduced overhead for the adaptability
- Processor provides competitive performance figures regarding the related art

Related publications

technology
from seed

inesc id lisboa

- Samuel Freitas Antão, Ricardo Chaves and Leonel Sousa, “Compact and Flexible Microcoded Elliptic Curve processor for Reconfigurable Devices”, In the 17th IEEE *Symposium on Field-Programmable Custom Computing Machines* (FCCM), 2009 [***HiPEAC paper award***]
- Ricardo Chaves, Georgi Kuzmanov, Stamatis Vassiliadis and Leonel Sousa, “Reconfigurable Memory based AES Co-processor”, In IPDPS, 13th *Reconfigurable Architectures Workshop* (RAW), 2006.

Questions

technology
from seed

inesc id lisboa

Questions?

Contact person: Leonel Sousa

las@inesc-id.pt