Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security

Xu Guo[1], Junfeng Fan[2], Patrick Schaumont[1], Ingrid Verbauwhede[2]

[1] Bradley Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg, VA 24061, USA

[2] ESAT/SCD-COSIC, Katholieke Universiteit Leuven and IBBT
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

Overview

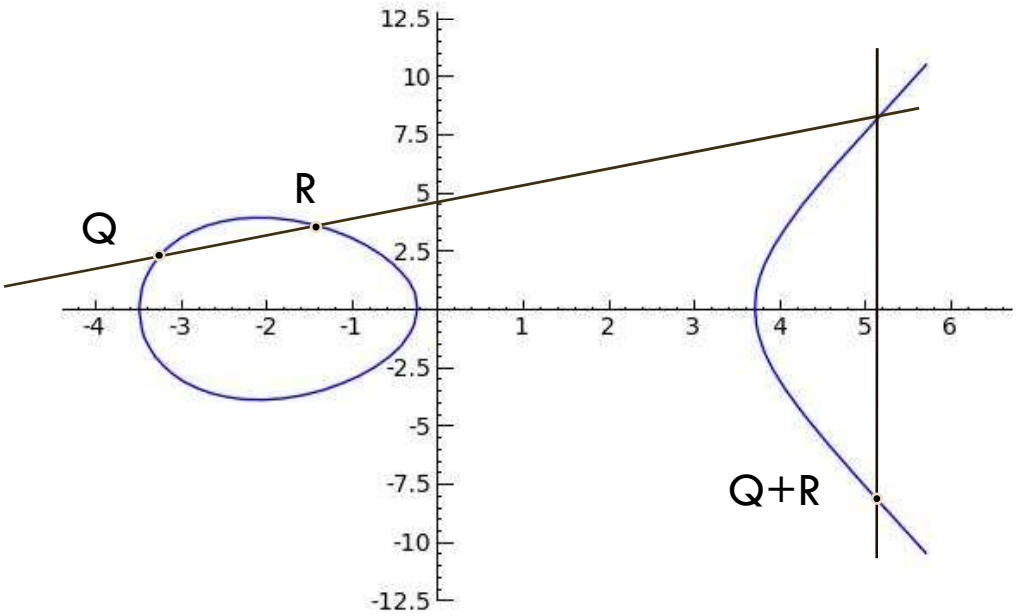
- Background
- Side-channel attacks on ECC
  - Power analysis on ECC
  - Fault analysis on ECC
- Countermeasure selection
- Architecture
- Conclusions

Elliptic Curve Cryptography (ECC)

- Definition:

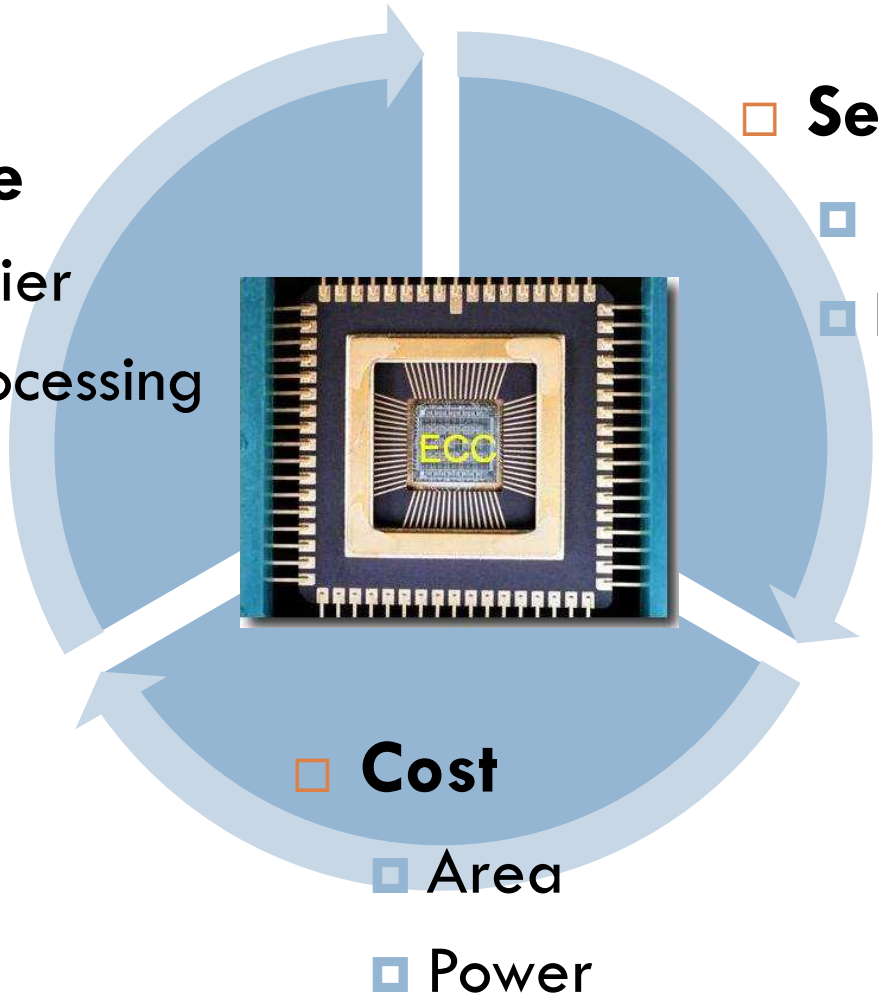
  E: $y^2 + a_1xy + a_3\,y = x^3 + a_2\,x^2 + a_4x + a_6$

- Group operation
- Point multiplication
  - $Q = k \cdot P$
- Applications
  - ECDSA
  - ECDH
  - Pairing
  - …



Trade-offs

- **Performance**
  - Fast multiplier
  - Parallel processing
  - NAF



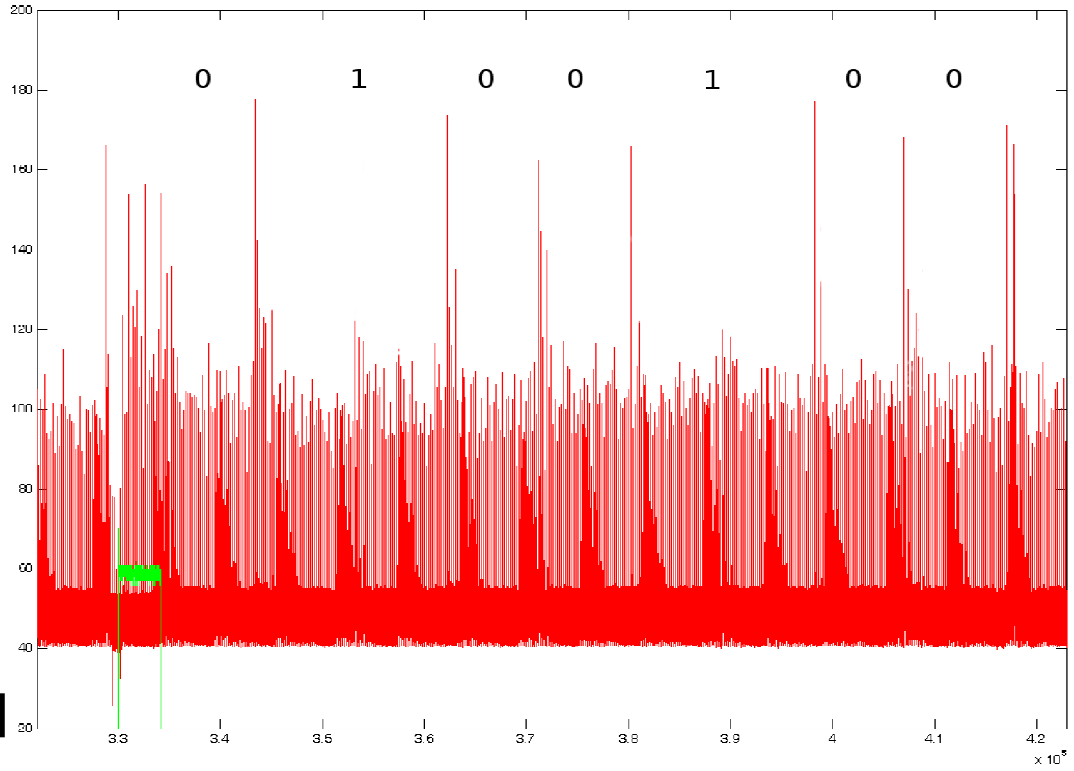
- **Security**
  - Power analysis
  - Fault analysis

- **Cost**
  - Area
  - Power

Simple Power Analysis (SPA)

- Unprotected method

```
for i=n-1 to 0
    Q← 2Q
    if k_i=1
        Q ← Q+P
end for
```



- Countermeasure
  - Unified PA/PD
  - Window method
  - Double-and-add-always
  - Montgomery ladder

Differential Power Analysis

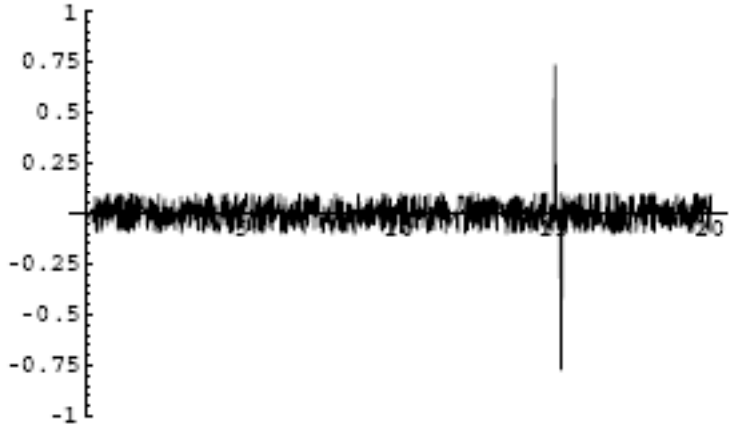
- Countermeasures
  - Random scalar:

    $k' = k + r \#E$
  - Base point blinding:

    $P' = P + R$
  - Random projective coordinates:

    $(X, Y, Z) \rightarrow (rX, rY, rZ)$
  - Random key split [Ciet+03]

    $k=k1 + k2$

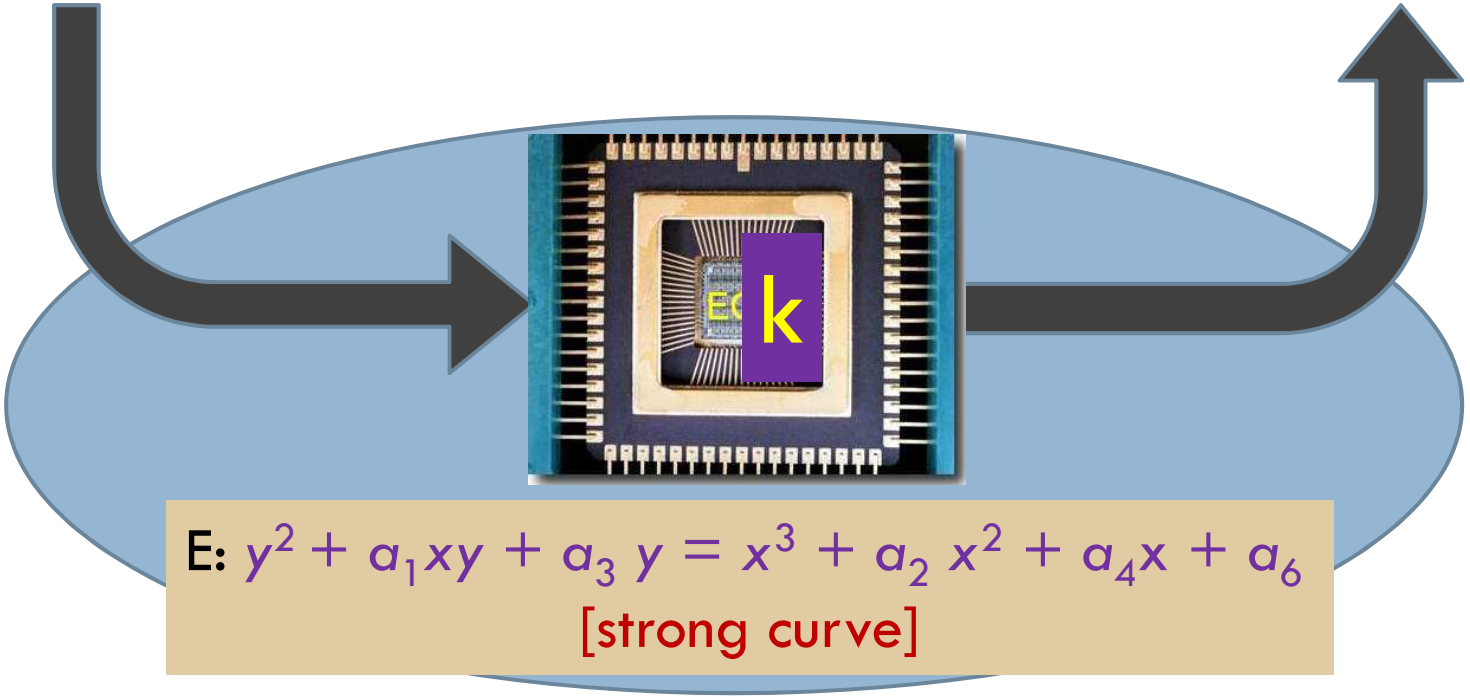


[Coron'99]

Fault Analysis

P(x, y)

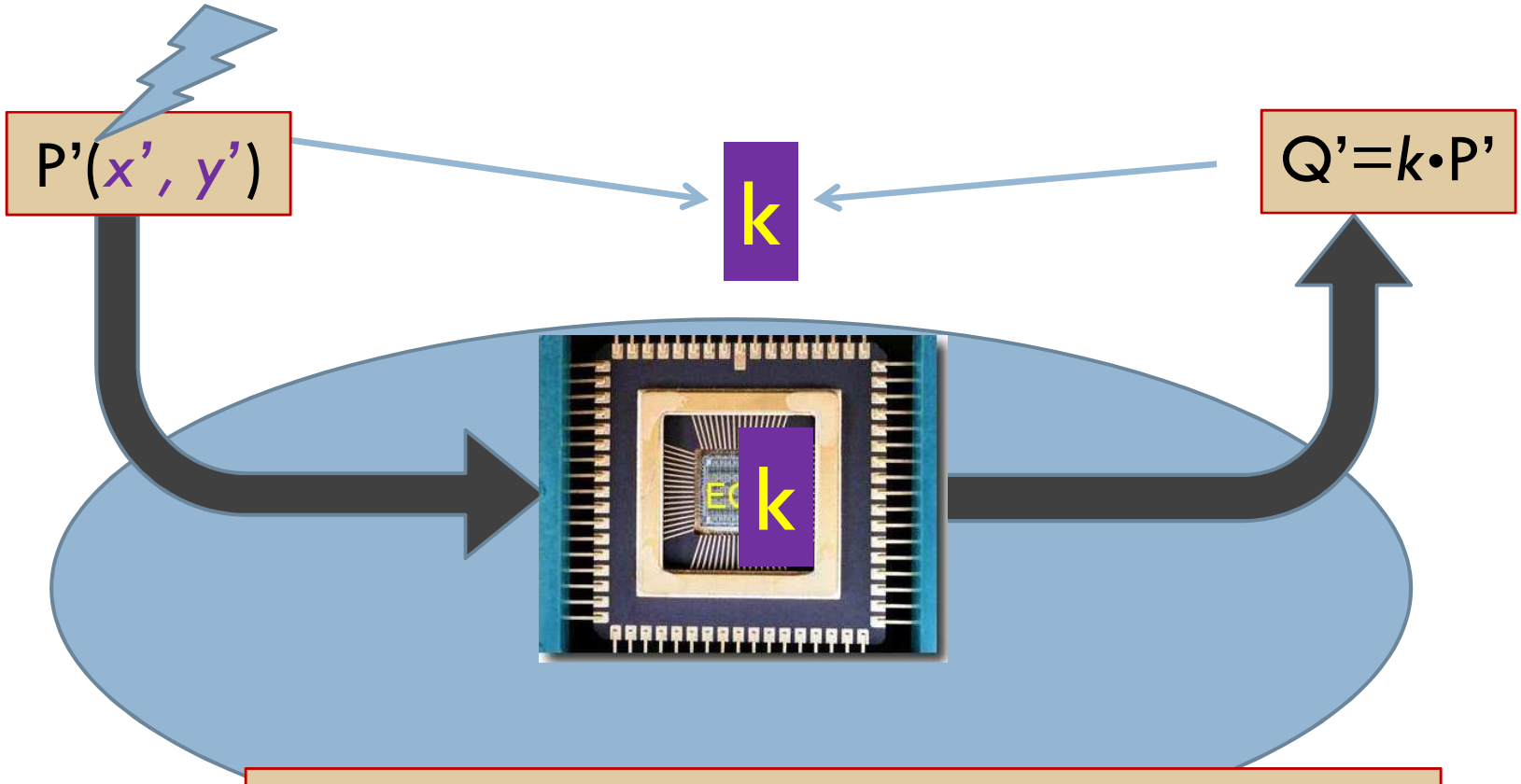
Q=k•P



E: $y^2 + a_1xy + a_3\,y = x^3 + a_2\,x^2 + a_4x + a_6$

[strong curve]

Fault Analysis



E': $y^2 + a_1xy + a_3 y = x^3 + a_2 x^2 + a_4x + a'_6$

[weak curve]

Fault Analysis

Fault Analysis on ECC

Type A: Go to weak curves E'

1, Faults in base point [Biehl+00]
2, Faults in underlying field [Ciet+05]
3, Faults in curve parameters [Ciet+05]
4, Twist-curve based attack [Fouque+08]

Type B: Might stay on curve E

1, Differential fault attack [Biehl+00]
2, Sign-change attack [Blomer+06]
3, M safe-error [Yen+00]
4, C safe-error [Yen+02]

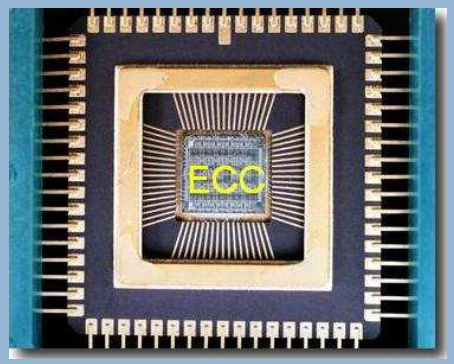
Choice of Adversaries

Simple power analysis

Doubling Attack

Twist curve based analysis

Differential power analysis



Safe-error analysis

Refined power analysis

…

Invalid curve analysis

Choice of Adversaries

Simple power analysis

Doubling Attack

Twist curve based analysis

Need only a single successful attack to win.

analysis

Safe-error analysis

Refined power analysis

…

Invalid curve analysis

Attacks vs. countermeasures

√ : Effective -- : Not related

× : Attacked H : helps the attack

* : Depends on the implementation

Attacks vs. countermeasures

√ : Effective -- : Not related

× : Attacked H : helps the attack

* : Depends on the implementation

	SPA SEMA								

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA								
Double-add-always	√								
Balanced PA/PD	√								
Montgomery Ladder	√								

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA							
Double-add-always	√	--							
Balanced PA/PD	√	--							
Montgomery Ladder	√	--							
Randomized splitting key	--	√							
Scalar randomization	--	√							
Base point blinding	--	√							
Randomized proj. coord.	--	√							

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack						
Double-add-always	√	--	--						
Balanced PA/PD	√	--	--						
Montgomery Ladder	√	--	--						
Randomized splitting key	--	√	√						
Scalar randomization	--	√	×						
Base point blinding	--	√	×						
Randomized proj. coord.	--	√	√						

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack	Refined PA					
Double-add-always	√	--	--	--					
Balanced PA/PD	√	--	--	--					
Montgomery Ladder	√	--	--	--					
Randomized splitting key	--	√	√	√					
Scalar randomization	--	√	×	--					
Base point blinding	--	√	×	--					
Randomized proj. coord.	--	√	√	×					

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack	Refined PA	Safe error				
Double-add-always	√	--	--	--	×H				
Balanced PA/PD	√	--	--	--	*H				
Montgomery Ladder	√	--	--	--	√*				
Randomized splitting key	--	√	√	√	--?				
Scalar randomization	--	√	×	--	--?				
Base point blinding	--	√	×	--	--				
Randomized proj. coord.	--	√	√	×	--				

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack	Refined PA	Safe error	Invalid Point			
Double-add-always	√	--	--	--	×H	--			
Balanced PA/PD	√	--	--	--	*H	--			
Montgomery Ladder	√	--	--	--	√*	--			
Randomized splitting key	--	√	√	√	--?	--			
Scalar randomization	--	√	×	--	--?	--			
Base point blinding	--	√	×	--	--	*?			
Randomized proj. coord.	--	√	√	×	--	--			
Point validity check	--	--	--	--	*H	√			

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack	Refined PA	Safe error	Invalid Point	Invalid curve		
Double-add-always	√	--	--	--	×H	--	--		
Balanced PA/PD	√	--	--	--	*H	--	--		
Montgomery Ladder	√	--	--	--	√*	--	--		
Randomized splitting key	--	√	√	√	--?	--	--		
Scalar randomization	--	√	×	--	--?	--	--		
Base point blinding	--	√	×	--	--	*?	*?		
Randomized proj. coord.	--	√	√	×	--	--	--		
Point validity check	--	--	--	--	*H	√	×		
Curve integrity check	--	--	--	--	--	--?	√		

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack	Refined PA	Safe error	Invalid Point	Invalid curve	Sign change	
Double-add-always	√	--	--	--	×H	--	--	*	
Balanced PA/PD	√	--	--	--	*H	--	--	*	
Montgomery Ladder	√	--	--	--	√*	--	--	√*	
Randomized splitting key	--	√	√	√	--?	--	--	--?	
Scalar randomization	--	√	×	--	--?	--	--	--?	
Base point blinding	--	√	×	--	--	*?	*?	--	
Randomized proj. coord.	--	√	√	×	--	--	--	--	
Point validity check	--	--	--	--	*H	√	×	×H	
Curve integrity check	--	--	--	--	--	--?	√	--	

Attacks vs. countermeasures

√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack	Refined PA	Safe error	Invalid Point	Invalid curve	Sign change	Twist curve
Double-add-always	√	--	--	--	×H	--	--	*	--
Balanced PA/PD	√	--	--	--	*H	--	--	*	--
Montgomery Ladder	√	--	--	--	√*	--	--	√*	×H
Randomized splitting key	--	√	√	√	--?	--	--	--?	√
Scalar randomization	--	√	×	--	--?	--	--	--?	--
Base point blinding	--	√	×	--	--	*?	*?	--	--
Randomized proj. coord.	--	√	√	×	--	--	--	--	--
Point validity check	--	--	--	--	*H	√	×	×H	√*
Curve integrity check	--	--	--	--	--	--?	√	--	--
Coherence check	--	--	--	--	--	--	--?	√*	--

Attacks vs. countermeasures

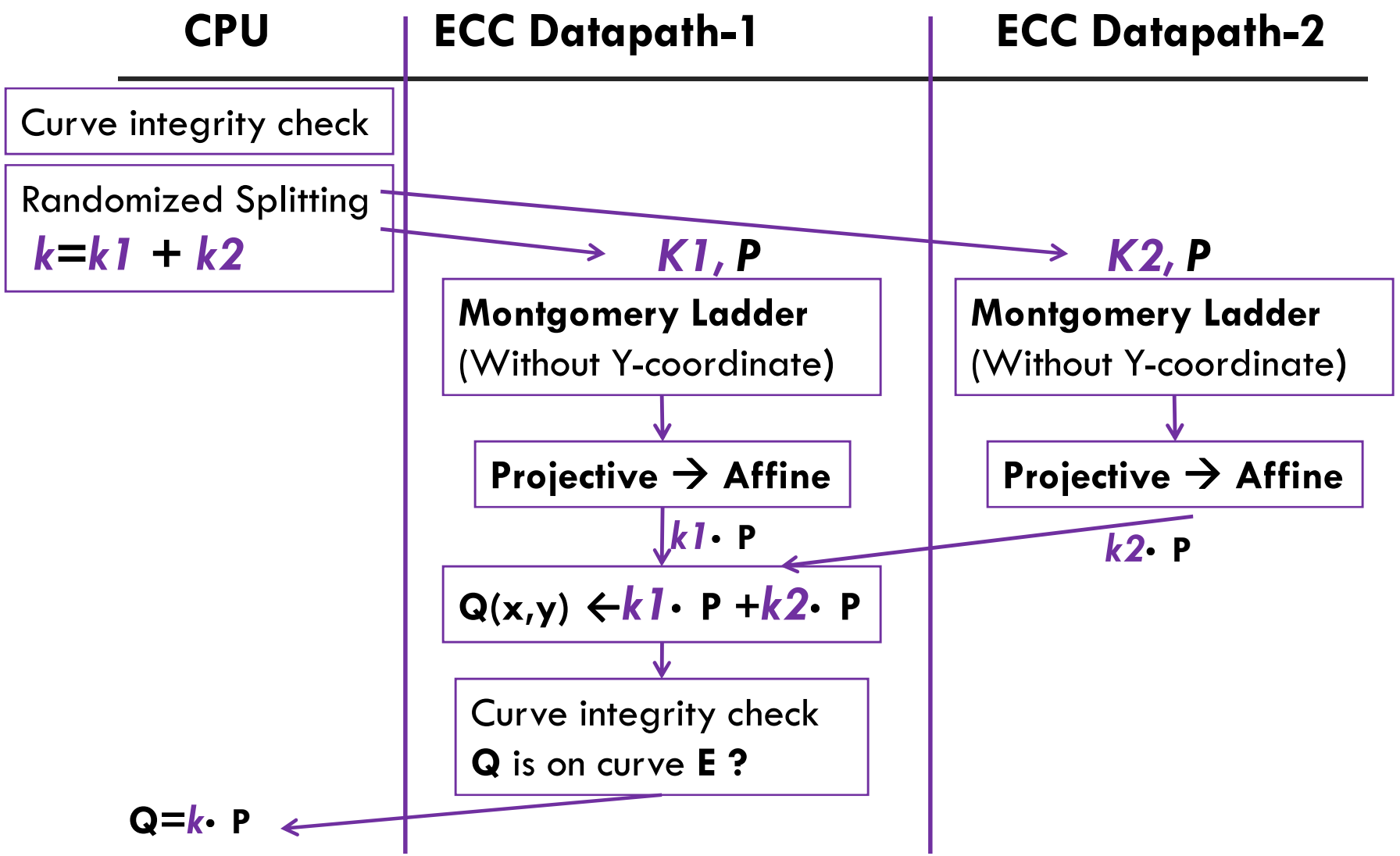
√ : Effective -- : Not related
× : Attacked H : helps the attack
* : Depends on the implementation

	SPA SEMA	DPA DEMA	Doubling Attack	Refined PA	Safe error	Invalid Point	Invalid curve	Sign change	Twist curve
Double-add-always	√	--	--	--	×H	--	--	*	--
Balanced PA/PD	√	--	--	--	*H	--	--	*	--
Montgomery Ladder	√	--	--	--	√*	--	--	√*	×H
Randomized splitting key	--	√	√	√	--?	--	--	--?	√
Scalar randomization	--	√	×	--	--?	--	--	--?	--
Base point blinding	--	√	×	--	--	*?	*?	--	--
Randomized proj. coord.	--	√	√	×	--	--	--	--	--
Point validity check	--	--	--	--	*H	√	×	×H	√*
Curve integrity check	--	--	--	--	--	--?	√	--	--
Coherence check	--	--	--	--	--	--	--?	√*	--
Combined	√	√	√	√	√*	√	√	√*	√*

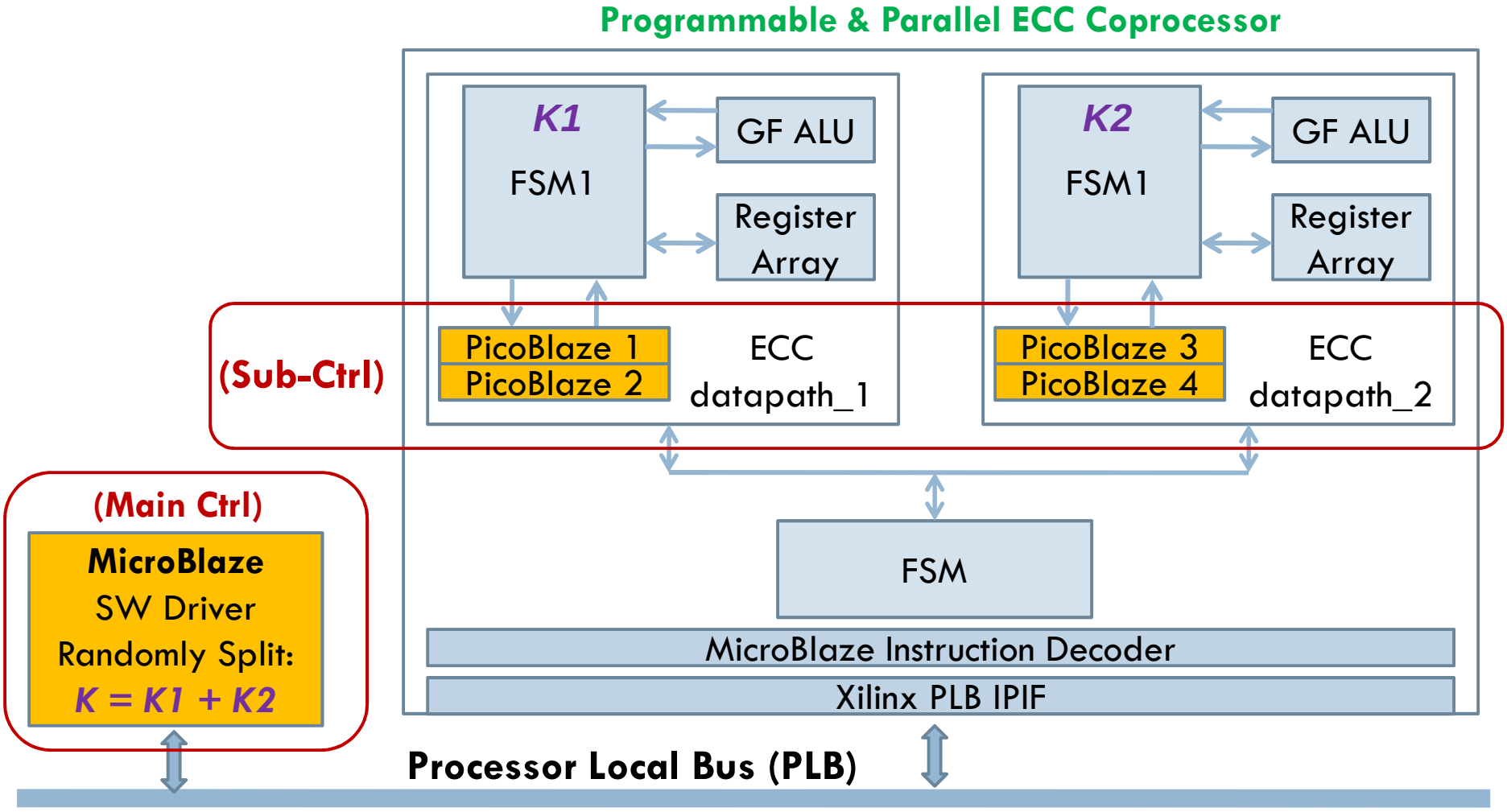
Suggestion

- Combine
  - Curve integrity check
  - Randomized splitting key
  - Montgomery ladder
  - Point validity check

Using the suggested countermeasures



Map to FPGA


Programmable & Parallel ECC Coprocessor
K1
FSM1
GF ALU
Register Array
K2
FSM1
GF ALU
Register Array
(Sub-Ctrl)
PicoBlaze 1
PicoBlaze 2
ECC datapath_1
PicoBlaze 3
PicoBlaze 4
ECC datapath_2
(Main Ctrl)
MicroBlaze
SW Driver
Randomly Split:
K = K1 + K2
FSM
MicroBlaze Instruction Decoder
Xilinx PLB IPIF
Processor Local Bus (PLB)

Conclusions

- A set of countermeasures against multiple attacks
  - Curve integrity check
  - Randomized splitting key
  - Montgomery ladder
  - Point validity check
- A parallel architecture for ECC processor
- An actual implementation on FPGA

Thanks for your attention!

Table of attacks and countermeasures is updated at
http://homes.esat.kuleuven.be/~jfan/eccaac.html