Introduction to Physical Attacks

Arnaud Tisserand

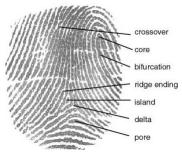
CNRS, Lab-STICC

25th October 2018

Summary

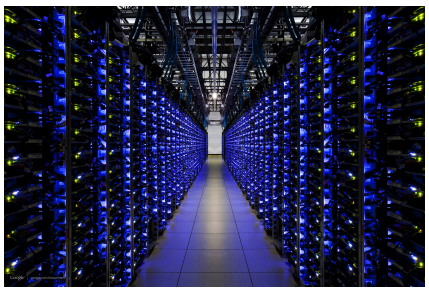
- Introduction
- Side Channel Attacks
- Fault Injection Attacks
- Conclusion and References

Applications with Security Needs







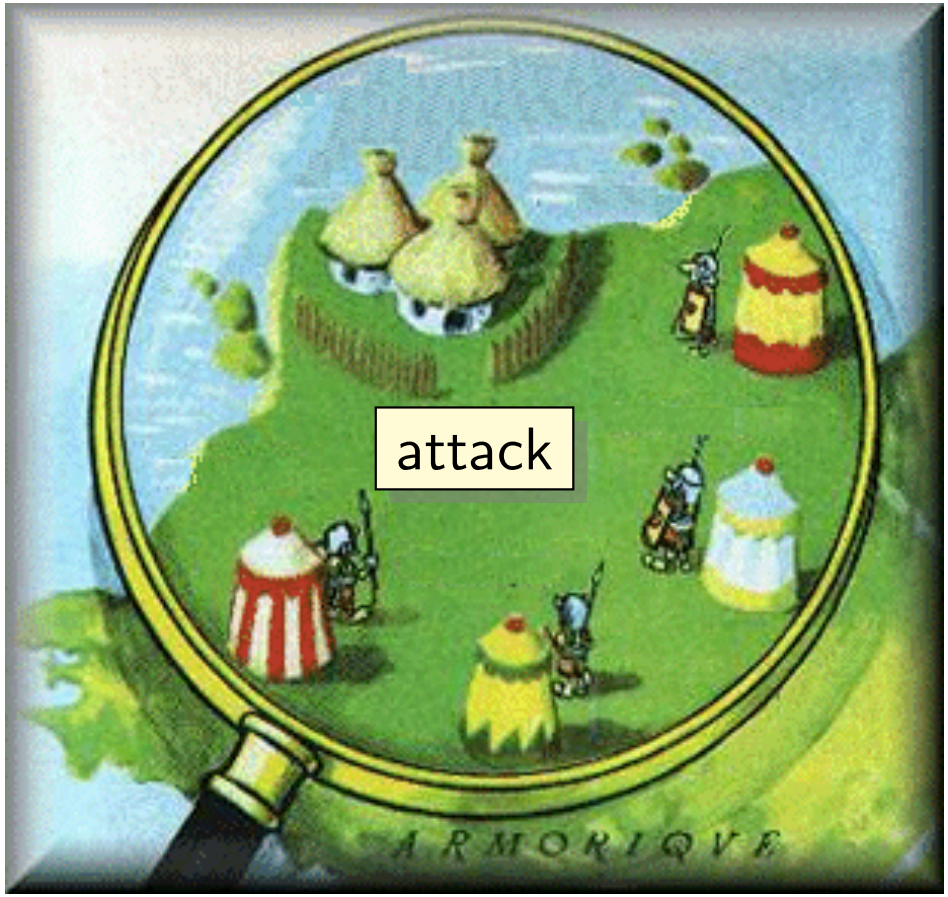




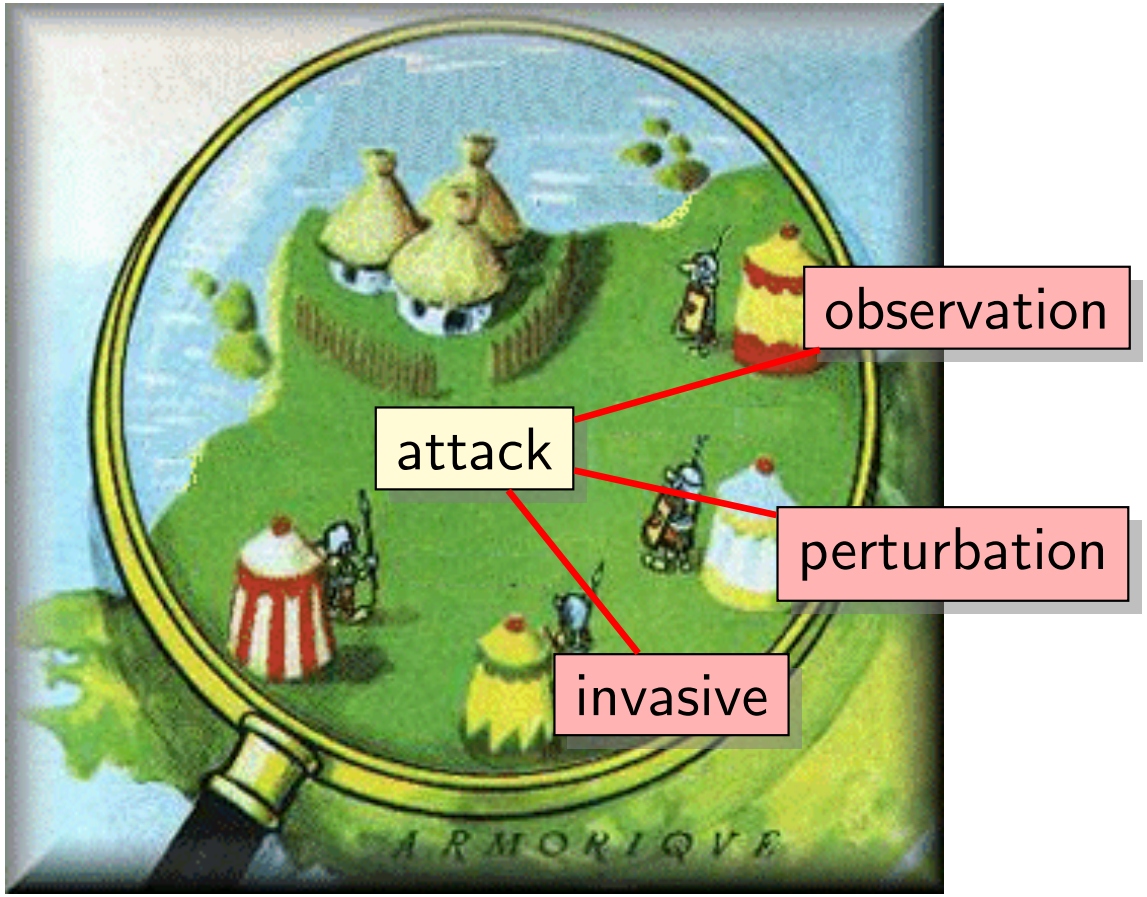



Applications: smart cards, computers, Internet, telecommunications, set-top boxes, data storage, RFID tags, WSN, smart grids...

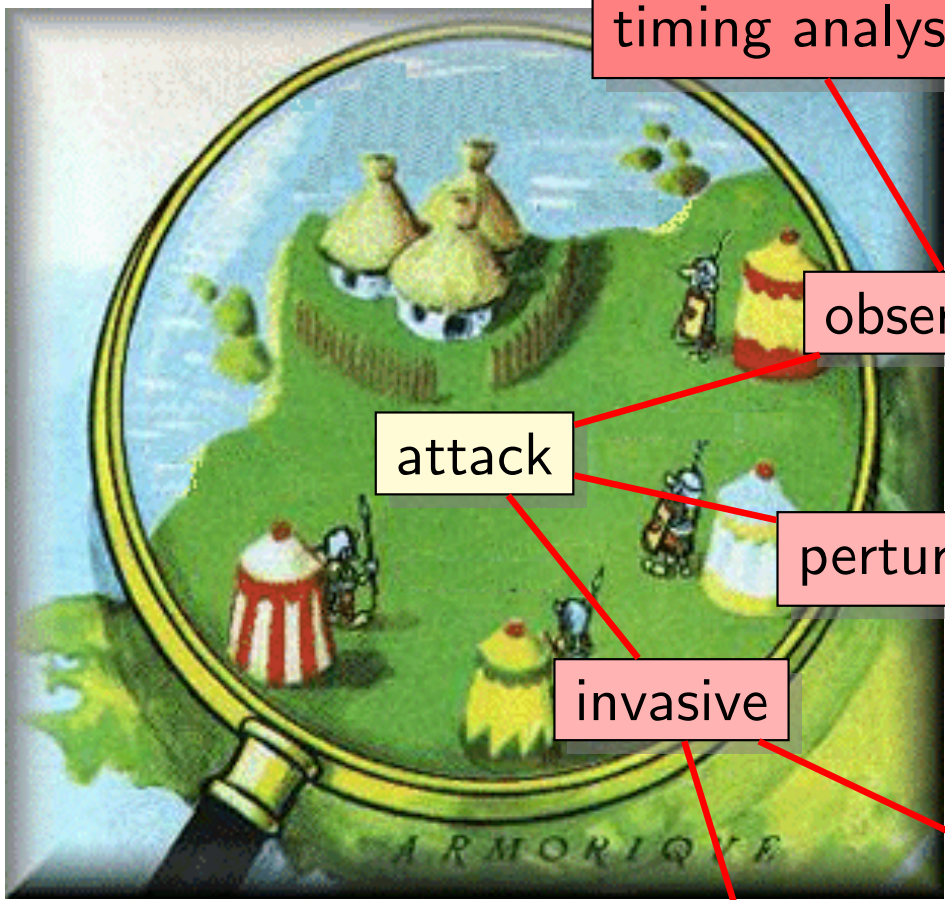
Attacks



Attacks



Attacks



timing analysis

power analysis

EMR analysis

observation

attack

perturbation

fault injection

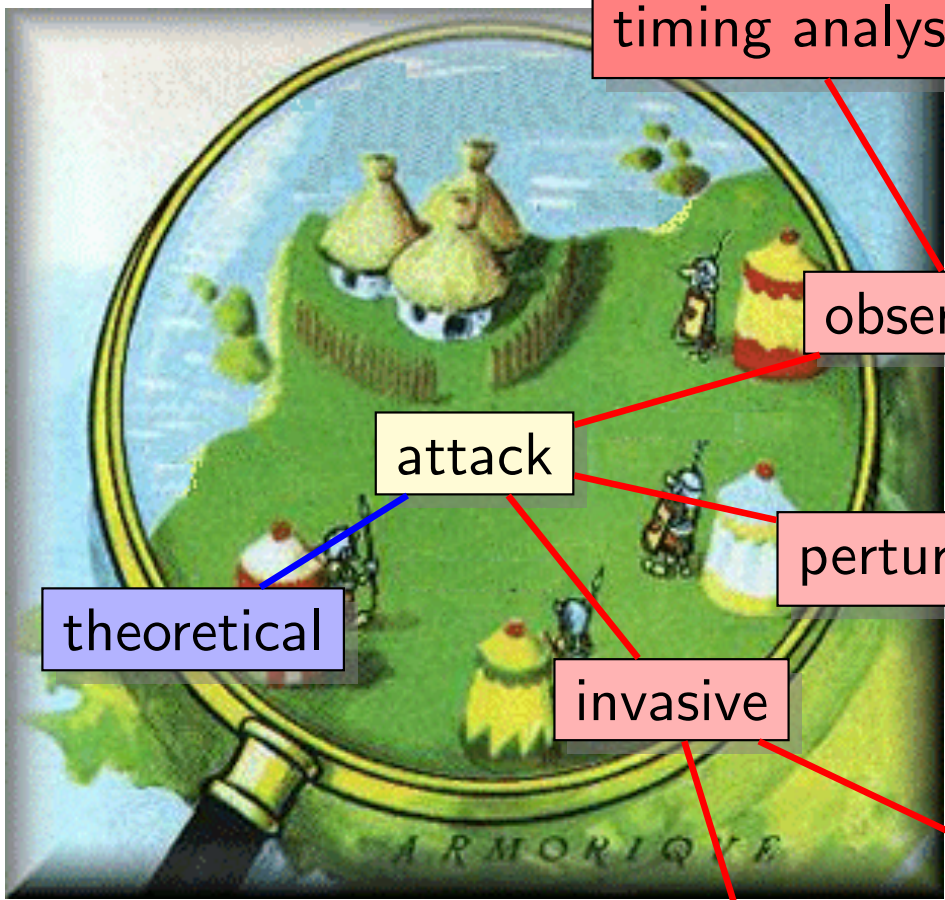
invasive

probing

reverse engineering

EMR = Electromagnetic radiation

Attacks



timing analysis

power analysis

EMR analysis

observation

attack

perturbation

theoretical

invasive

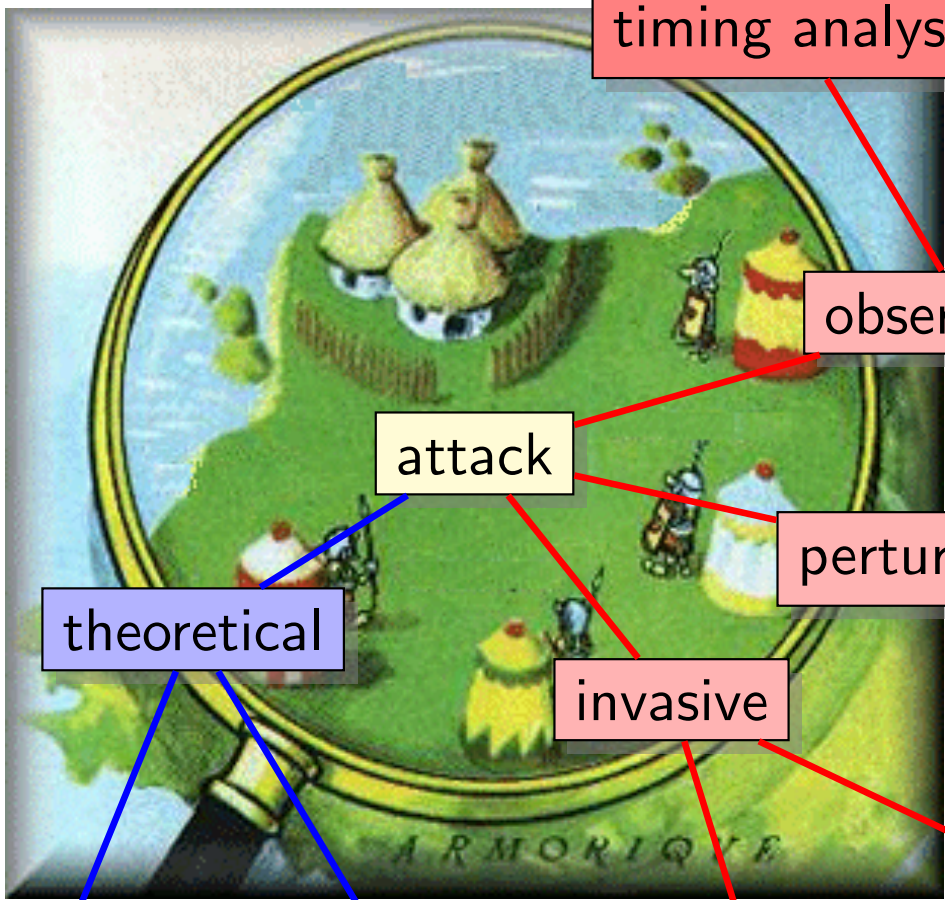
fault injection

probing

reverse engineering

EMR = Electromagnetic radiation

Attacks



timing analysis

power analysis

EMR analysis

observation

attack

perturbation

theoretical

invasive

fault injection

advanced algorithms

probing

reverse engineering

optimized programming

EMR = Electromagnetic radiation

Side Channel Attacks (SCAs) (1/2)

Attack: attempt to find, without any knowledge about the secret:

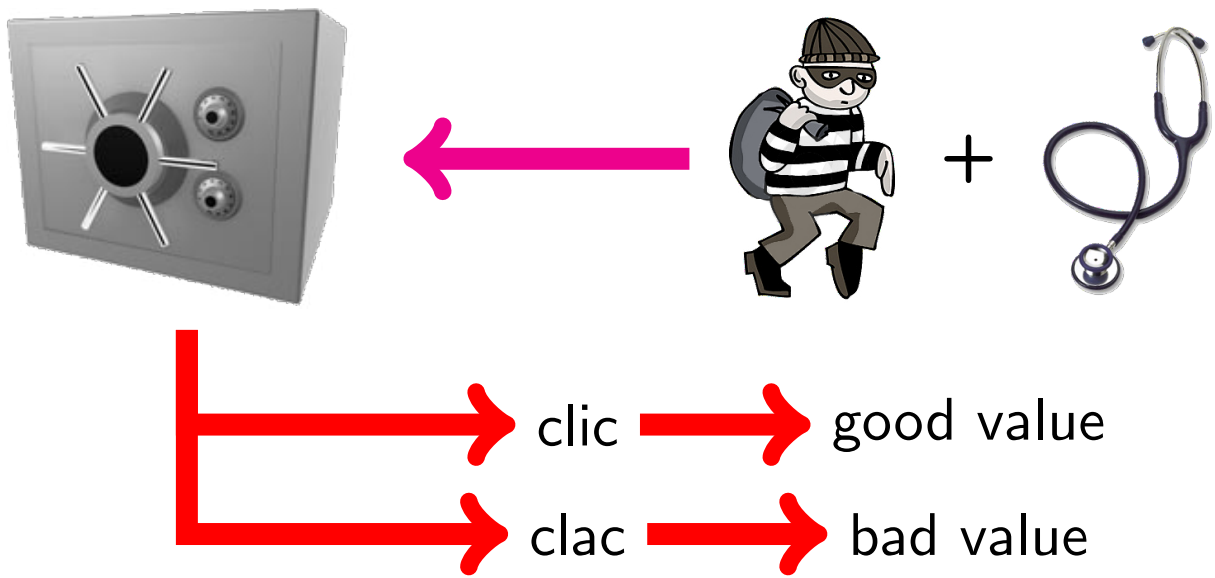
- the message (or parts of the message)
- informations on the message
- the secret (or parts of the secret)

Side Channel Attacks (SCAs) (1/2)

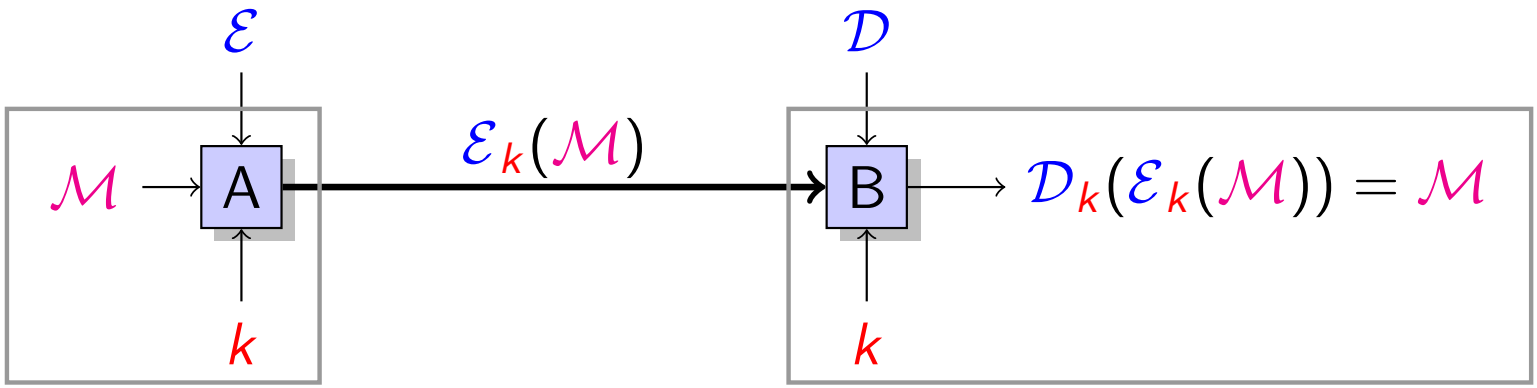
Attack: attempt to find, without any knowledge about the secret:

- the message (or parts of the message)
- informations on the message
- the secret (or parts of the secret)

"Old style" side channel attacks:

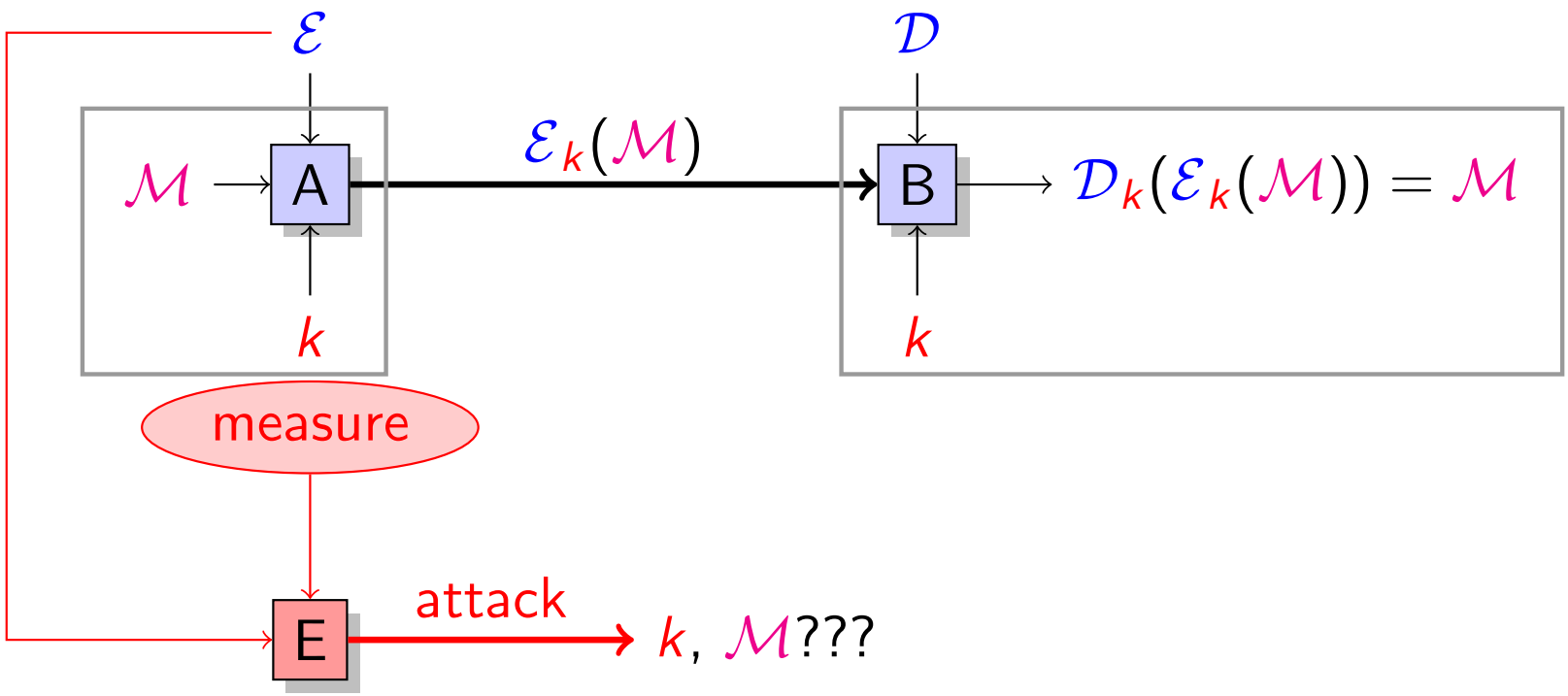


Side Channel Attacks (SCAs) (2/2)



General principle: measure external parameter(s) on running device in order to deduce internal informations

Side Channel Attacks (SCAs) (2/2)



General principle: measure external parameter(s) on running device in order to deduce internal informations

What Should be Measured?

Answer: everything that can "enter" and/or "get out" in/from the device

- power consumption
- electromagnetic radiation
- temperature
- sound
- computation time
- number of cache misses
- number and type of error messages
- ...

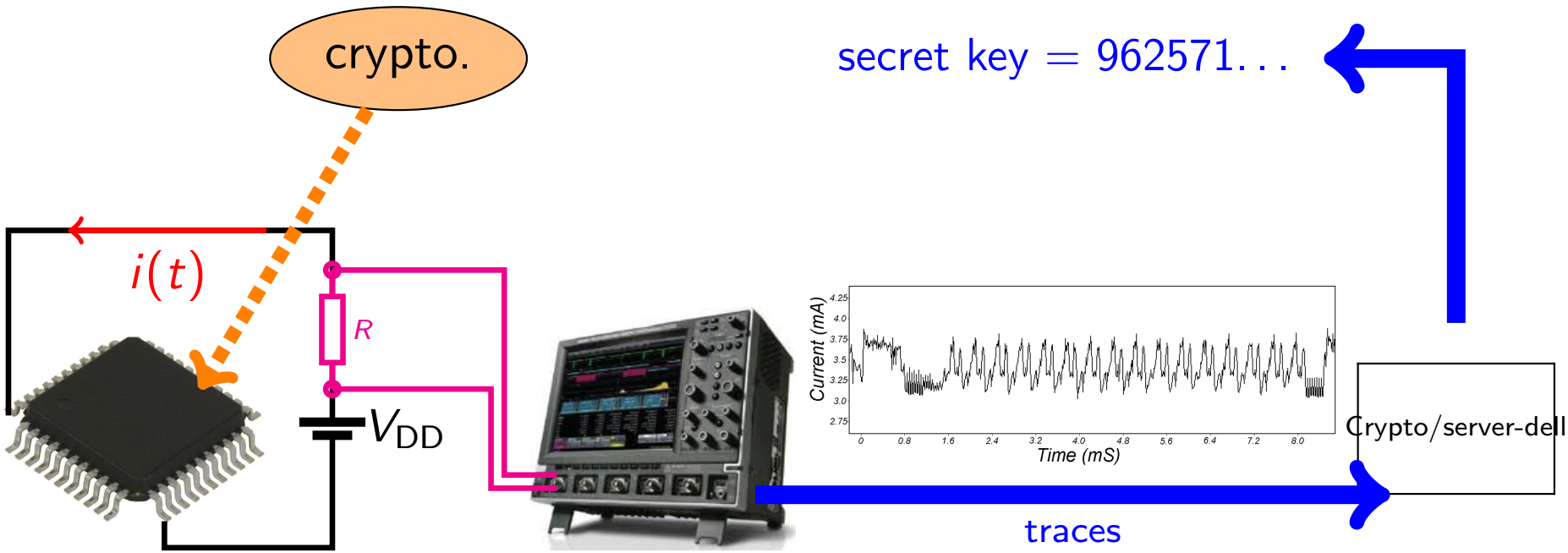
The measured parameters may provide informations on:

- global behavior (temperature, power, sound...)
- local behavior (EMR, # cache misses...)

Power Consumption Analysis

General principle:

1. measure the current $i(t)$ in the cryptosystem
2. use those measurements to "deduce" secret informations



Differences & External Signature

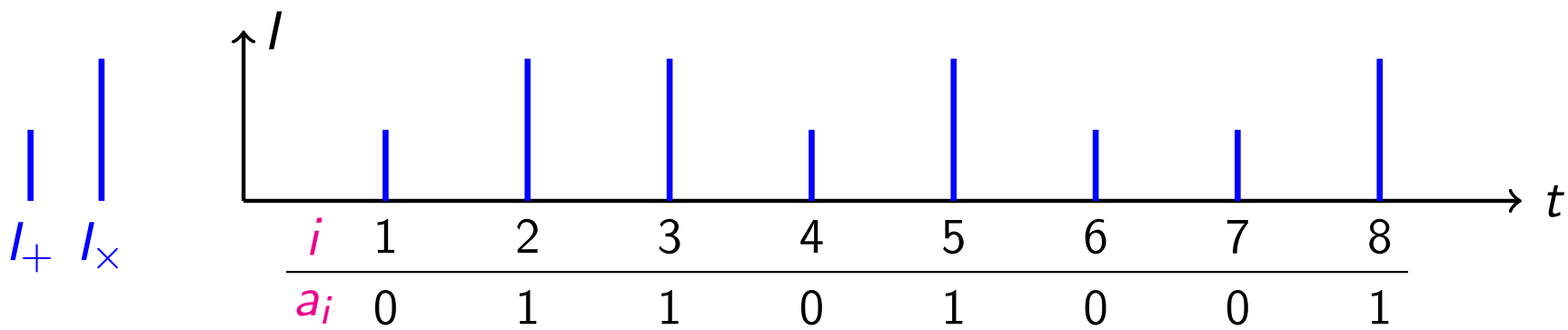
An algorithm :

```
r = c0
for i from 1 to n do
    if a_i = 0 then
        r = r + c1
    else
        r = r × c2
```

Differences & External Signature

An algorithm has a current signature :

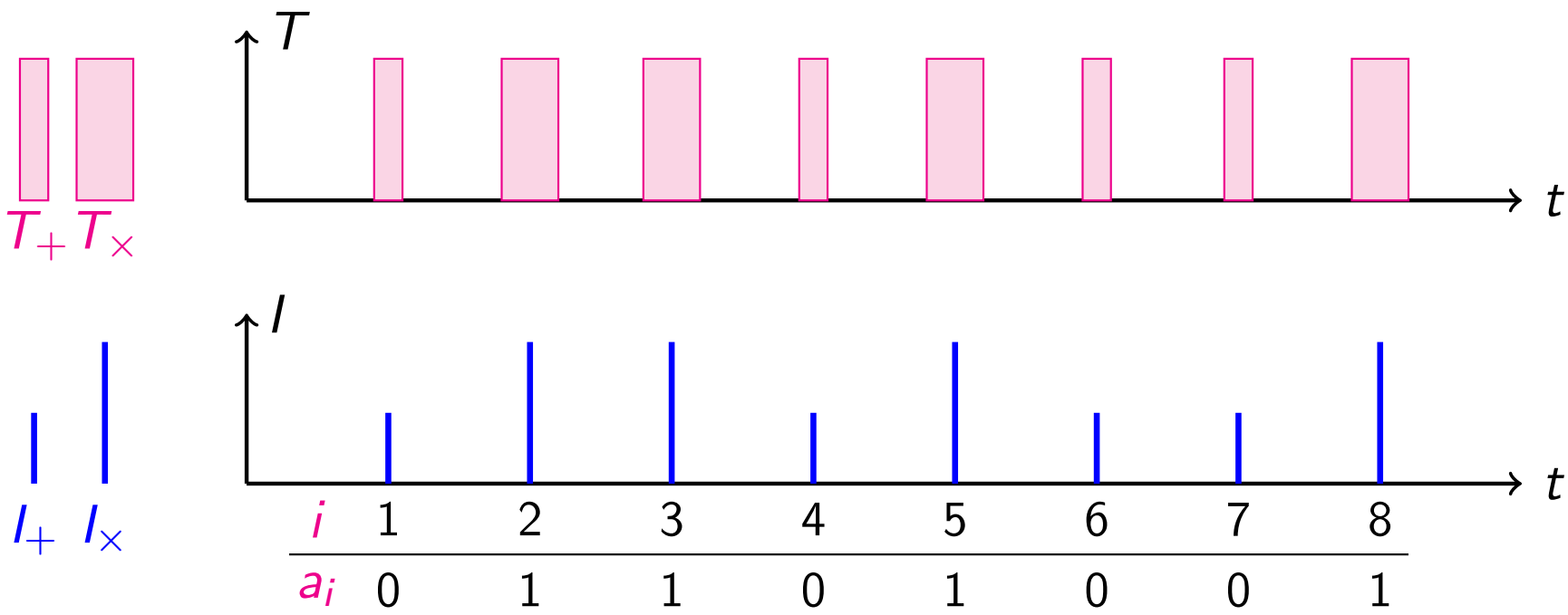
$r = c_0$
`for` i `from 1 to` n `do`
  `if` $a_i = 0$ `then`
    $r = r + c_1$
  `else`
    $r = r \times c_2$



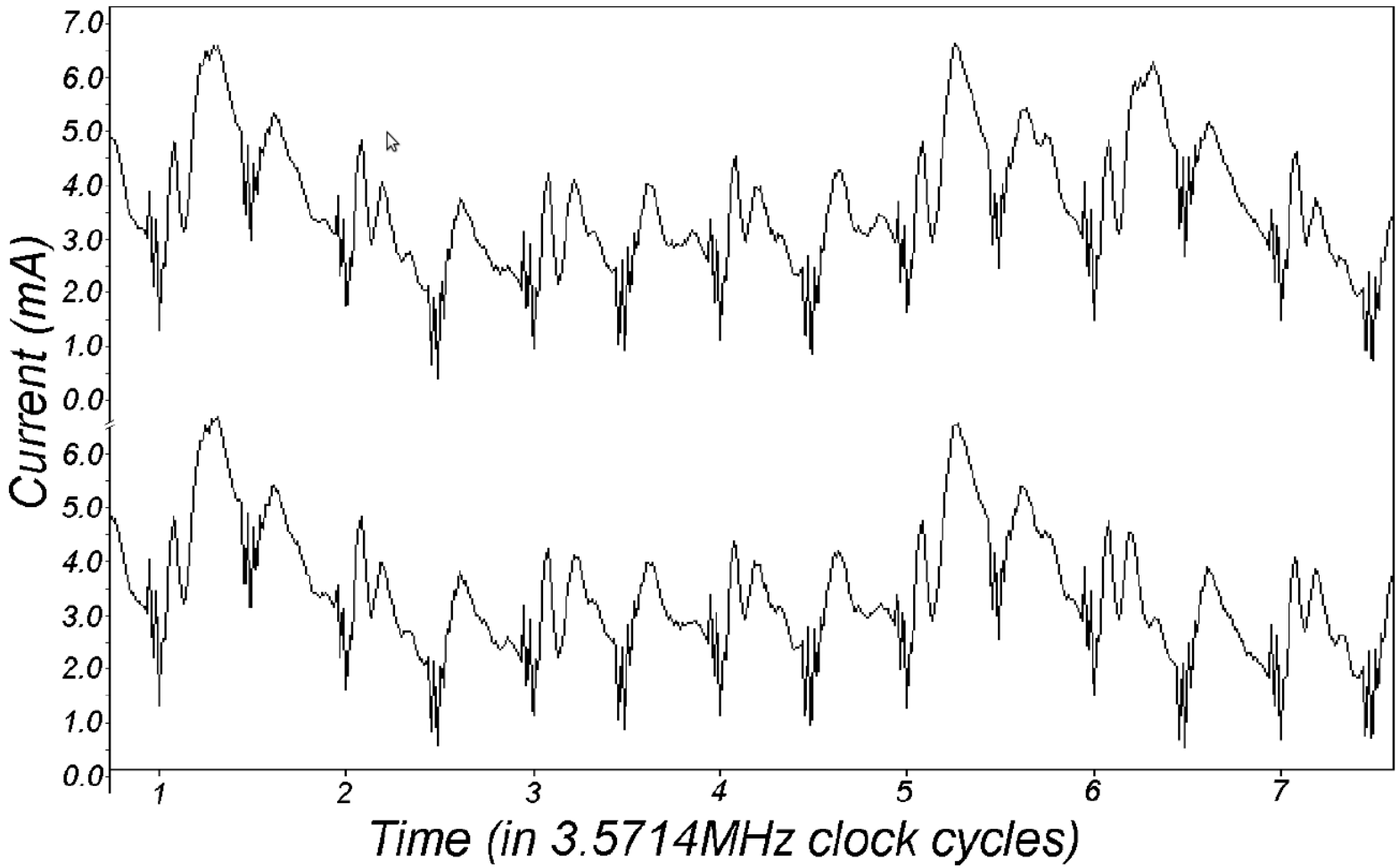
Differences & External Signature

An algorithm has a current signature and a time signature:

```
r = c0
for i from 1 to n do
    if ai = 0 then
        r = r + c1
    else
        r = r × c2
```

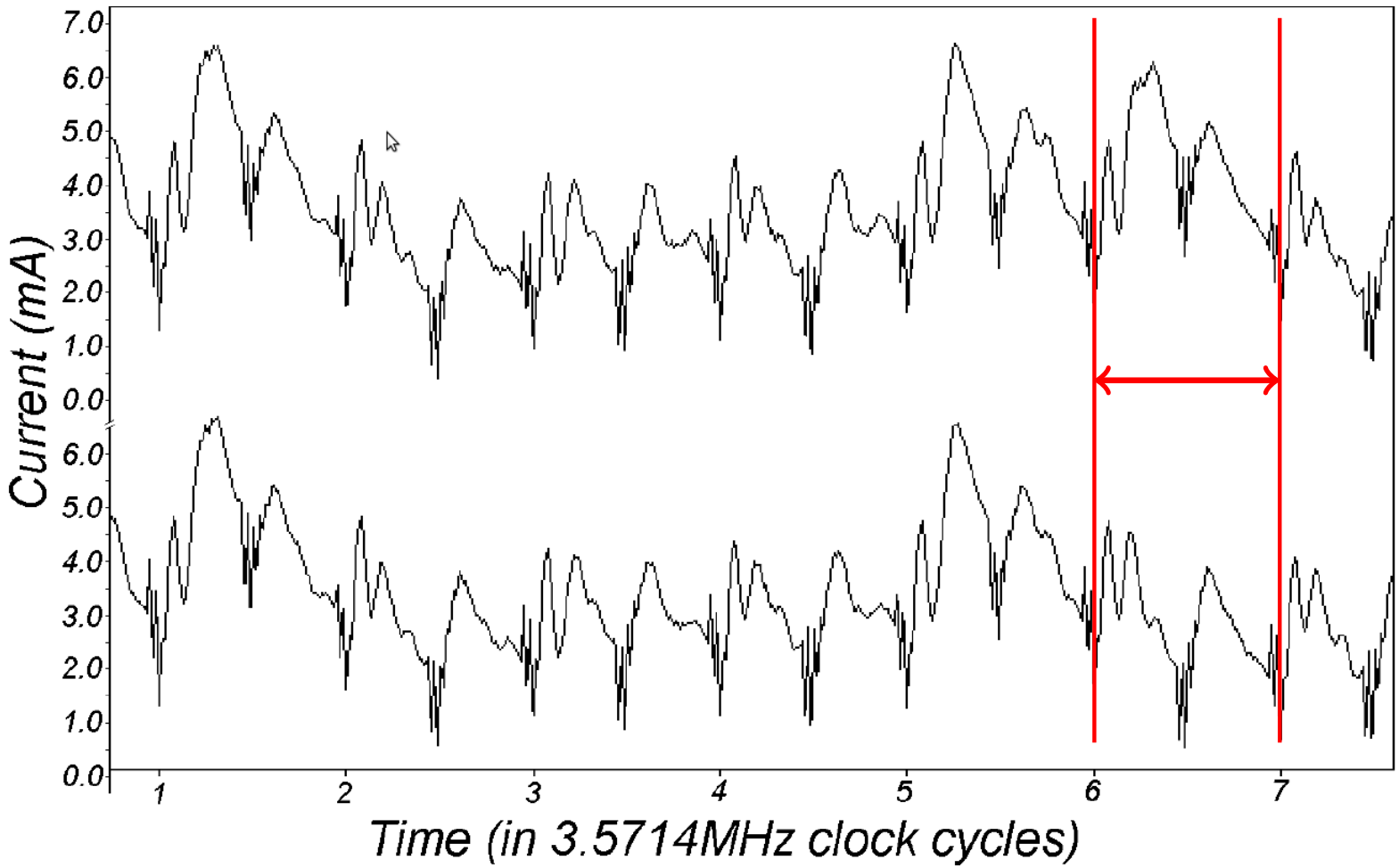


Simple Power Analysis (SPA)



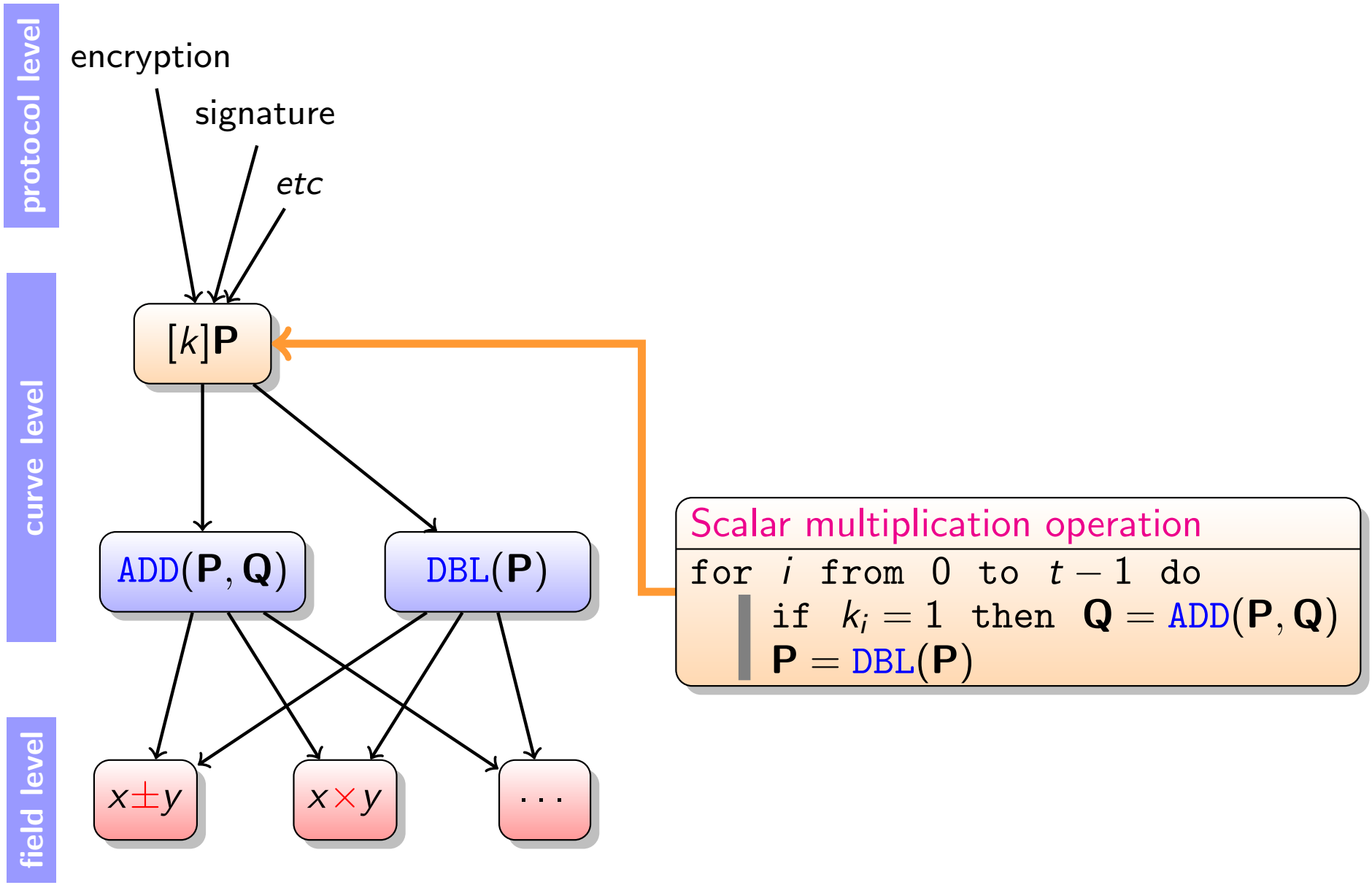
Source: [2]

Simple Power Analysis (SPA)



Source: [2]

SPA on ECC


protocol level
curve level
field level
encryption
signature
etc
[k]P
ADD(P, Q)
DBL(P)
x±y
x×y
...
Scalar multiplication operation
for i from 0 to t − 1 do
if k_i = 1 then Q = ADD(P, Q)
P = DBL(P)

SPA on ECC

protocol level

curve level

field level

encryption

signature

etc

$[k]\mathbf{P}$

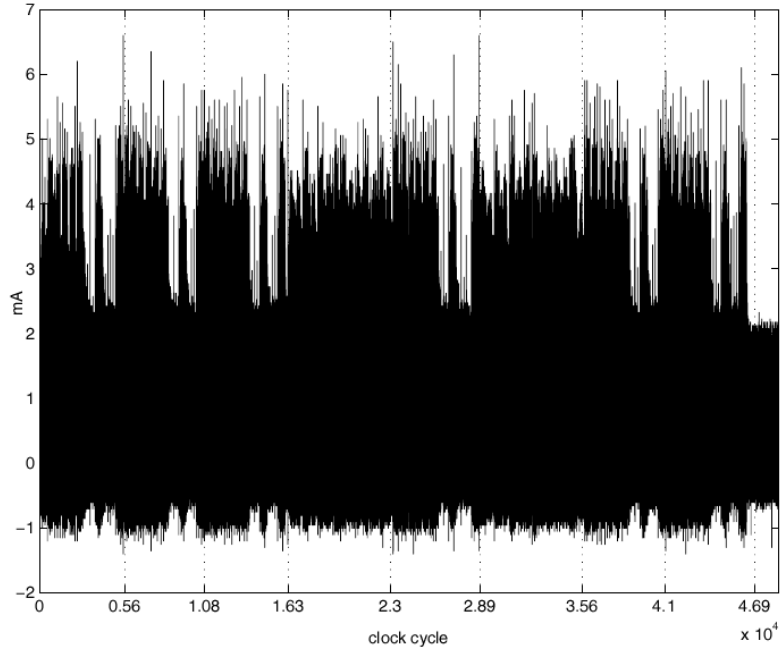
$\mathtt{ADD}(\mathbf{P},\mathbf{Q})$

$\mathtt{DBL}(\mathbf{P})$

$x \pm y$

$x \times y$

$\ldots$



Scalar multiplication operation

```
for i from 0 to t − 1 do
    if k_i = 1 then Q = ADD(P, Q)
    P = DBL(P)
```

SPA on ECC

protocol level

curve level

field level

encryption

signature

etc

$[k]\mathbf{P}$

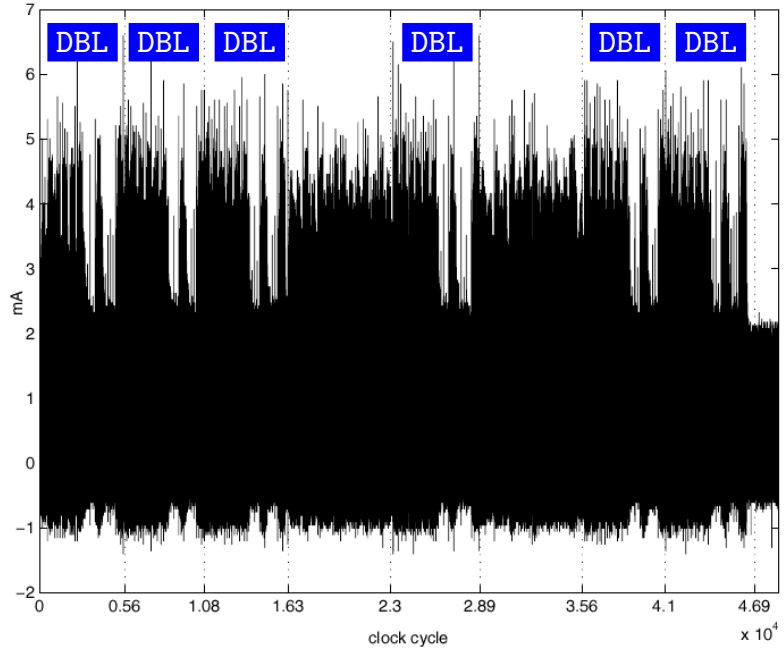
$\mathtt{ADD}(\mathbf{P},\mathbf{Q})$

$\mathtt{DBL}(\mathbf{P})$

$x \pm y$

$x \times y$

$\ldots$



Scalar multiplication operation

```
for i from 0 to t − 1 do
    if k_i = 1 then Q = ADD(P, Q)
    P = DBL(P)
```

SPA on ECC

protocol level

curve level

field level

encryption

signature

etc

$[k]\mathbf{P}$

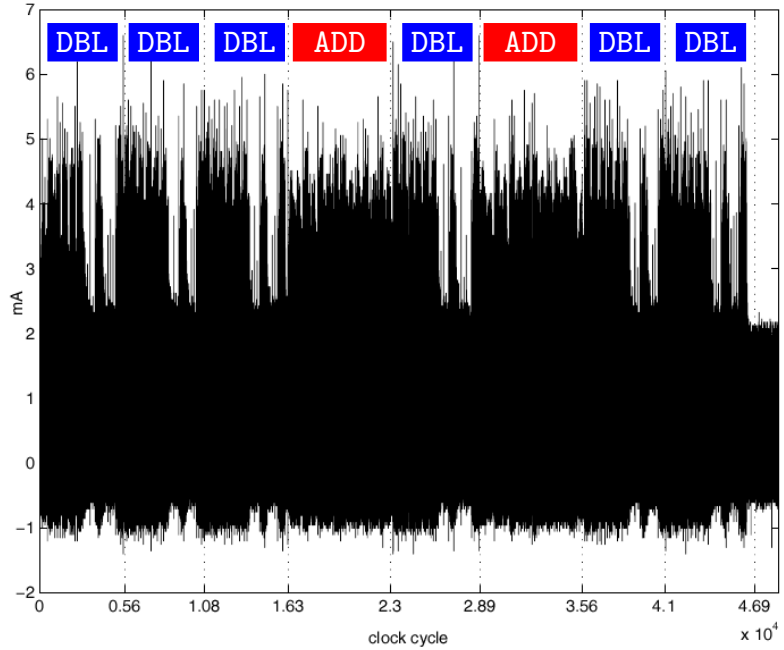
$\mathtt{ADD}(\mathbf{P},\mathbf{Q})$

$\mathtt{DBL}(\mathbf{P})$

$x \pm y$

$x \times y$

$\ldots$



Scalar multiplication operation

```
for i from 0 to t − 1 do
    if k_i = 1 then Q = ADD(P, Q)
    P = DBL(P)
```

SPA on ECC

protocol level

curve level

field level

encryption

signature

etc

$[k]\mathbf{P}$

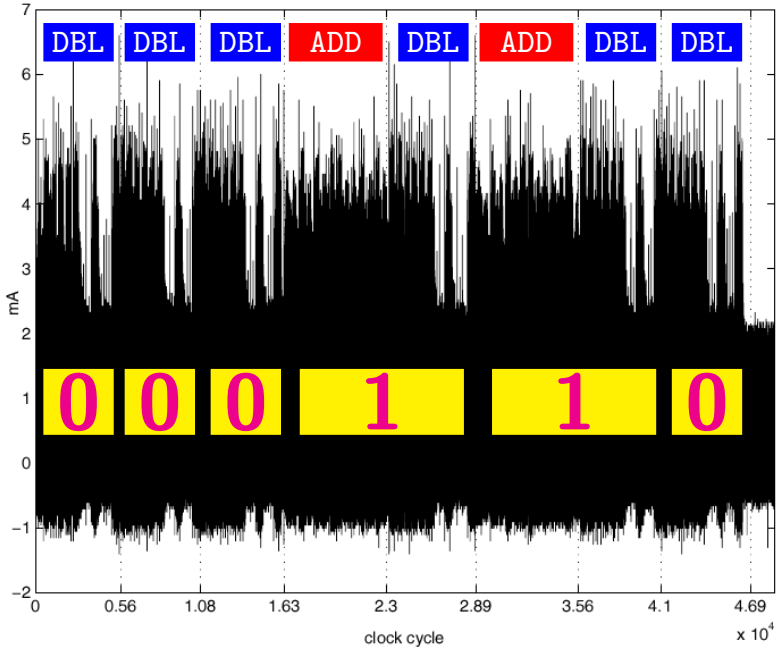
$\mathtt{ADD}(\mathbf{P},\mathbf{Q})$

$\mathtt{DBL}(\mathbf{P})$

$x \pm y$

$x \times y$

$\ldots$

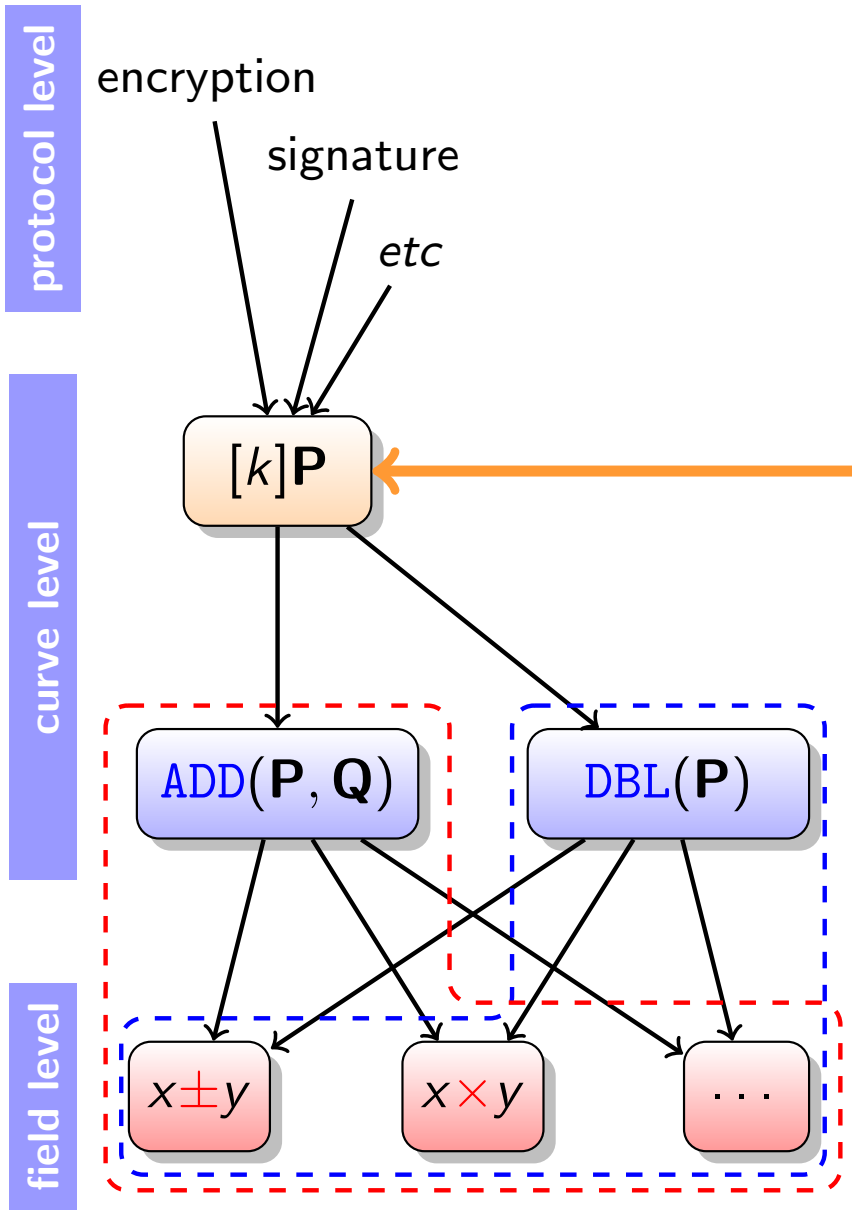


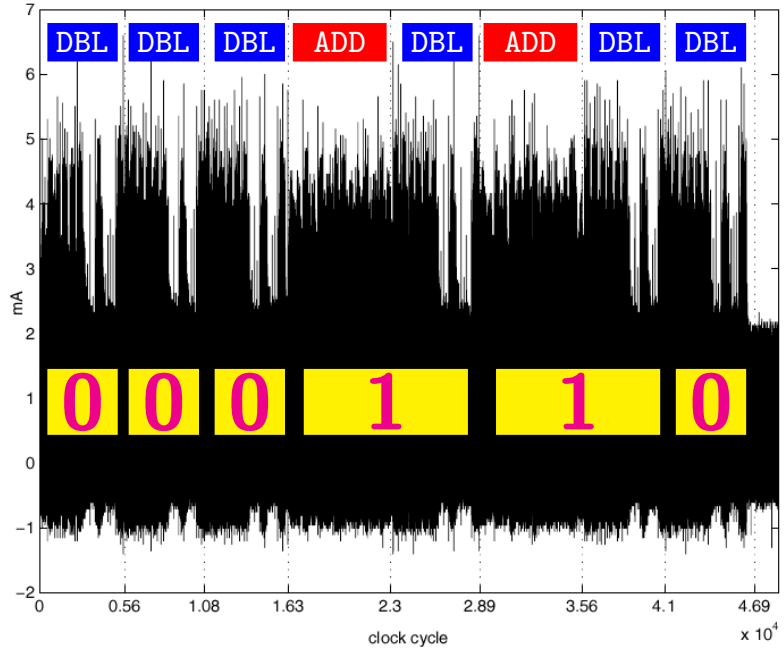
Scalar multiplication operation

```
for i from 0 to t − 1 do
    if k_i = 1 then Q = ADD(P, Q)
    P = DBL(P)
```

- simple power analysis (& variants)

SPA on ECC





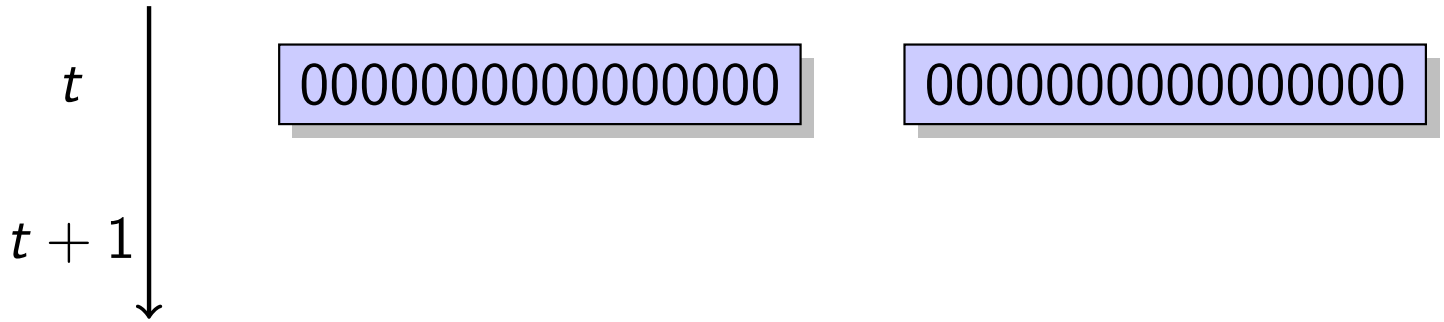
Scalar multiplication operation

```
for i from 0 to t − 1 do
    if k_i = 1 then Q = ADD(P, Q)
    P = DBL(P)
```

- simple power analysis (& variants)
- differential power analysis (& variants)
- horizontal/vertical/templates/... attacks

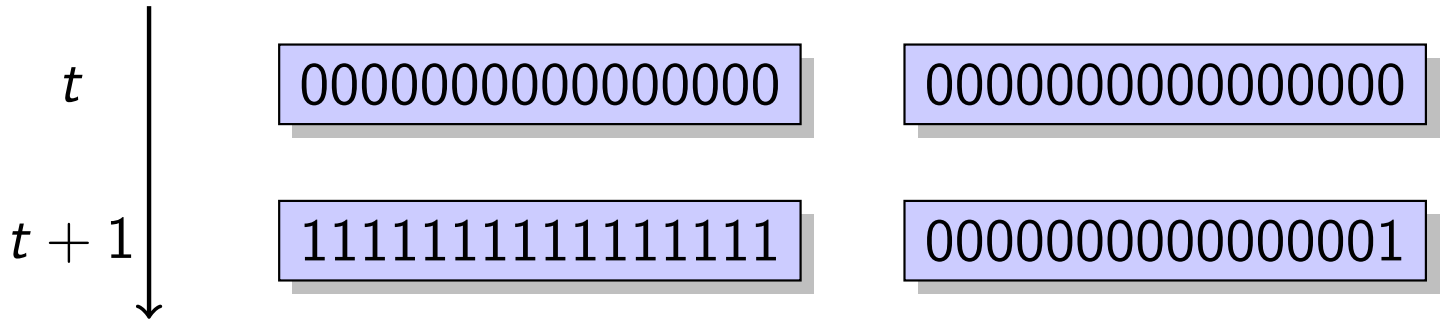
Limits of the SPA

Example of behavior difference: (activity into a register)



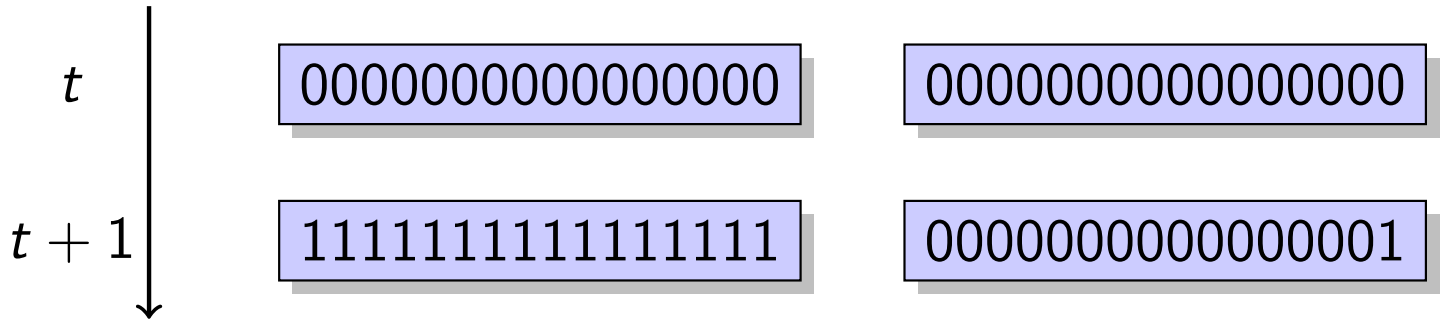
Limits of the SPA

Example of behavior difference: (activity into a register)



Limits of the SPA

Example of behavior difference: (activity into a register)

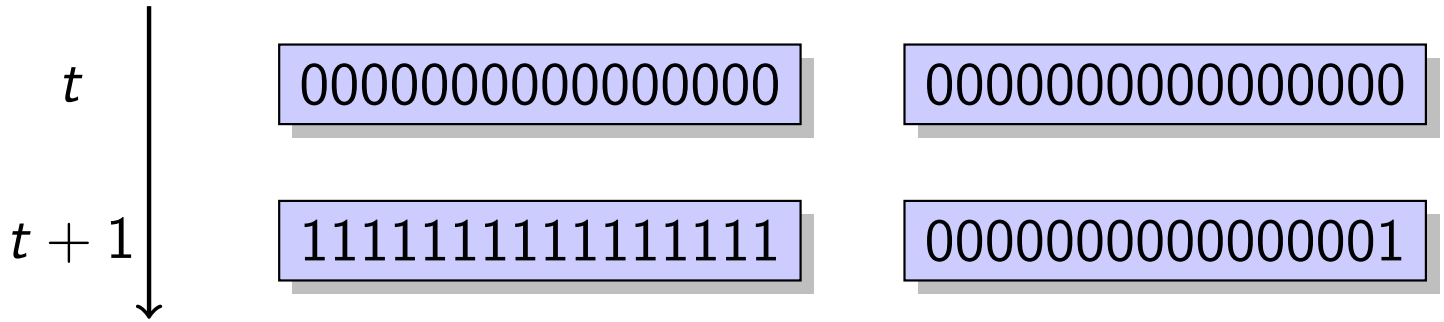


Important: a small difference may be evaluated has a noise during the measurement → traces cannot be distinguished

Question: what can be done when differences are too small?

Limits of the SPA

Example of behavior difference: (activity into a register)



Important: a small difference may be evaluated has a noise during the measurement → traces cannot be distinguished

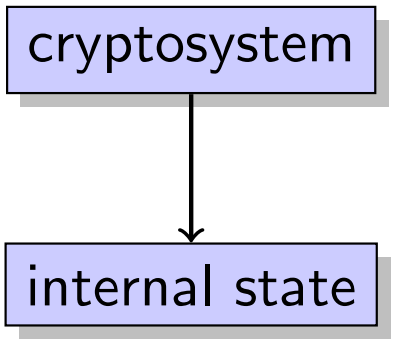
Question: what can be done when differences are too small?

Answer: use statistics over several traces

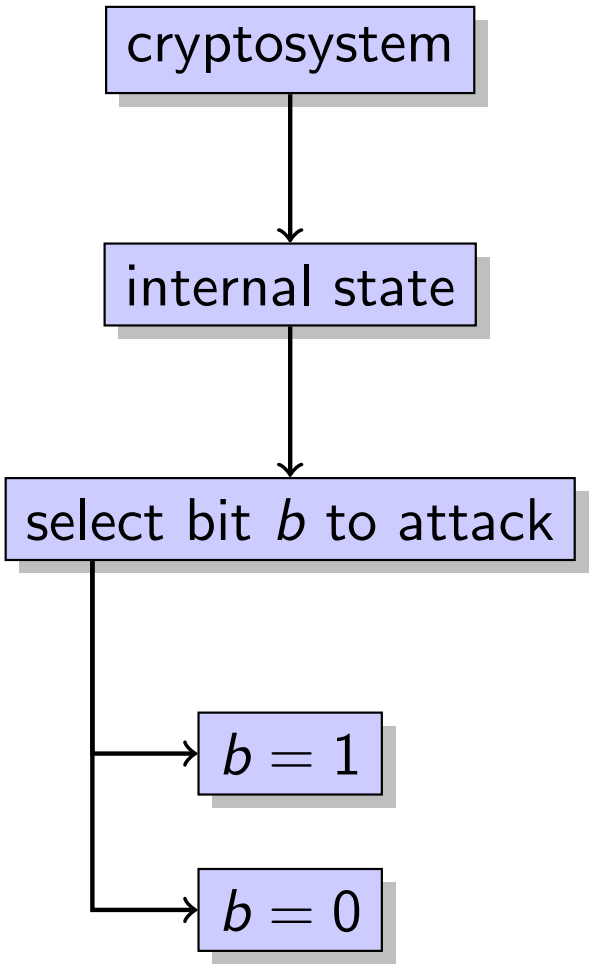
Differential Power Analysis (DPA)

cryptosystem

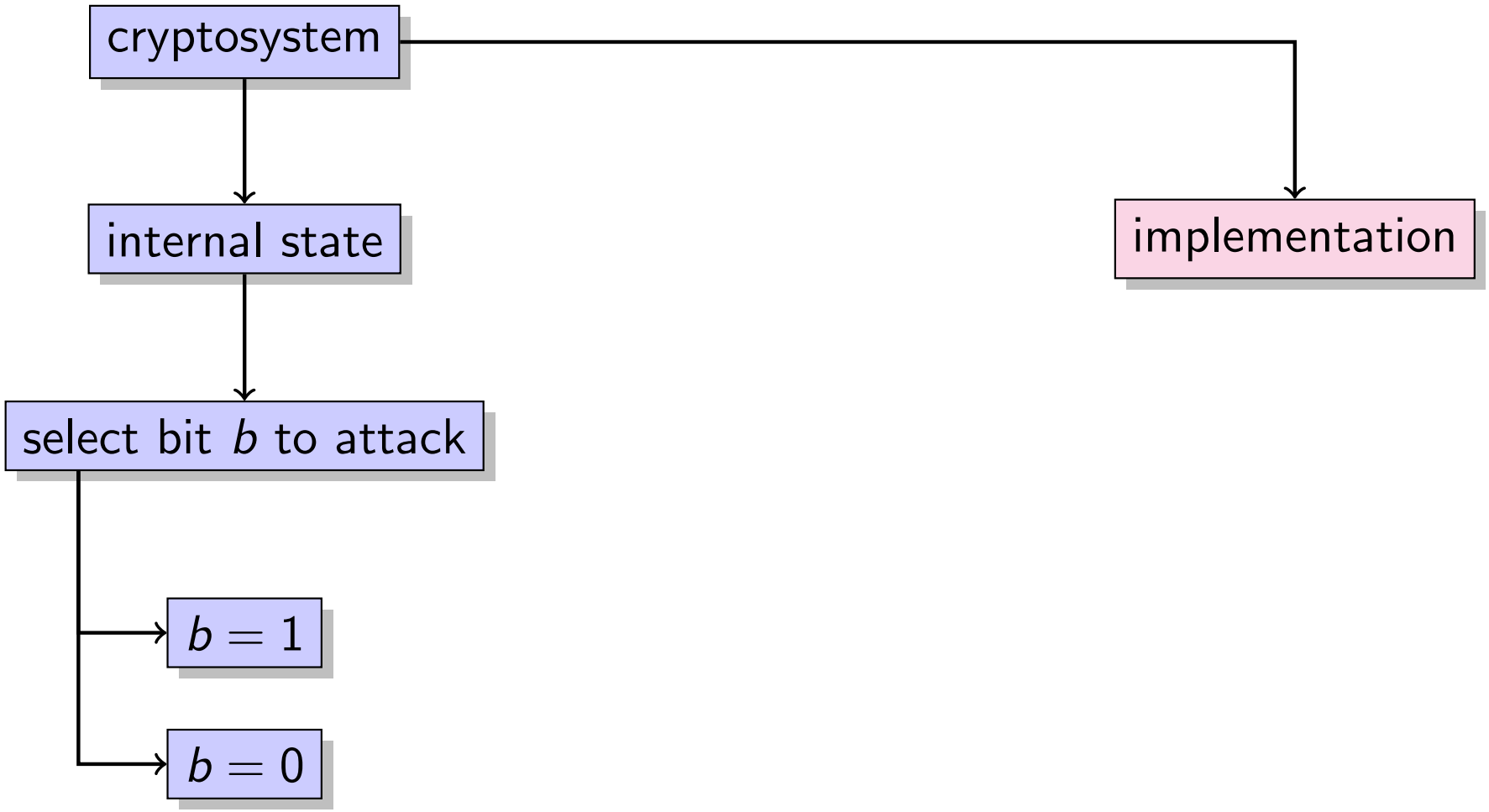
Differential Power Analysis (DPA)



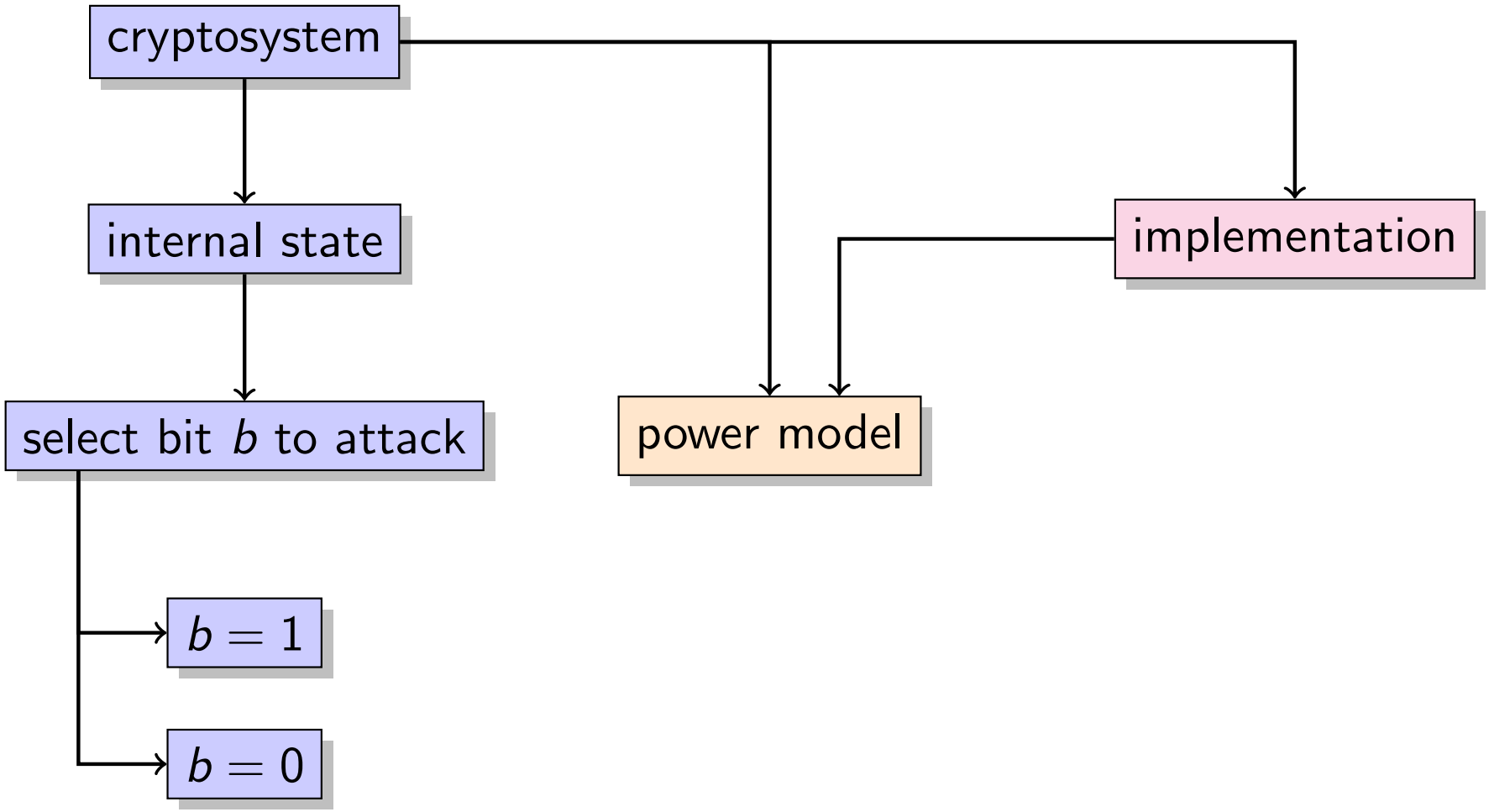
Differential Power Analysis (DPA)



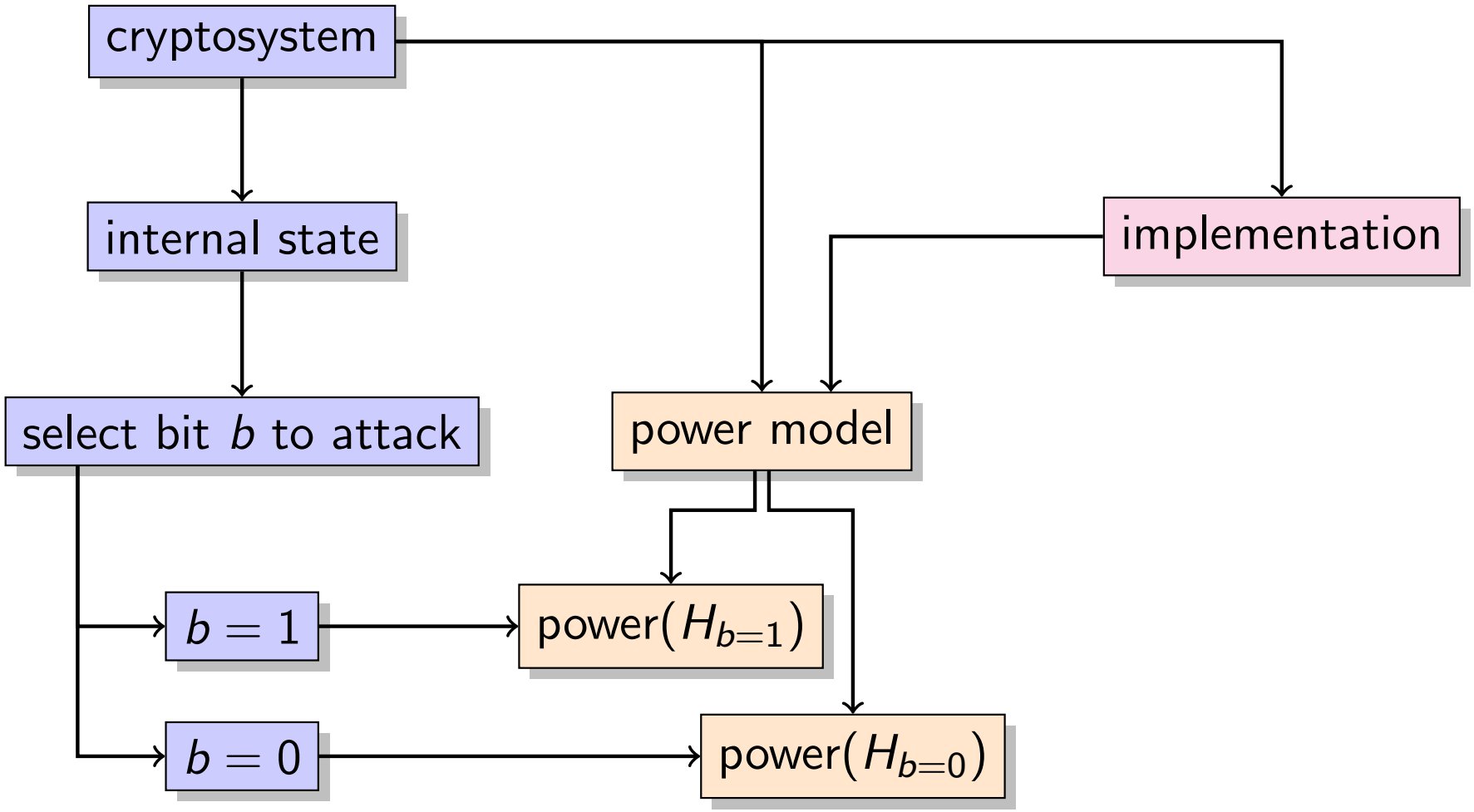
Differential Power Analysis (DPA)



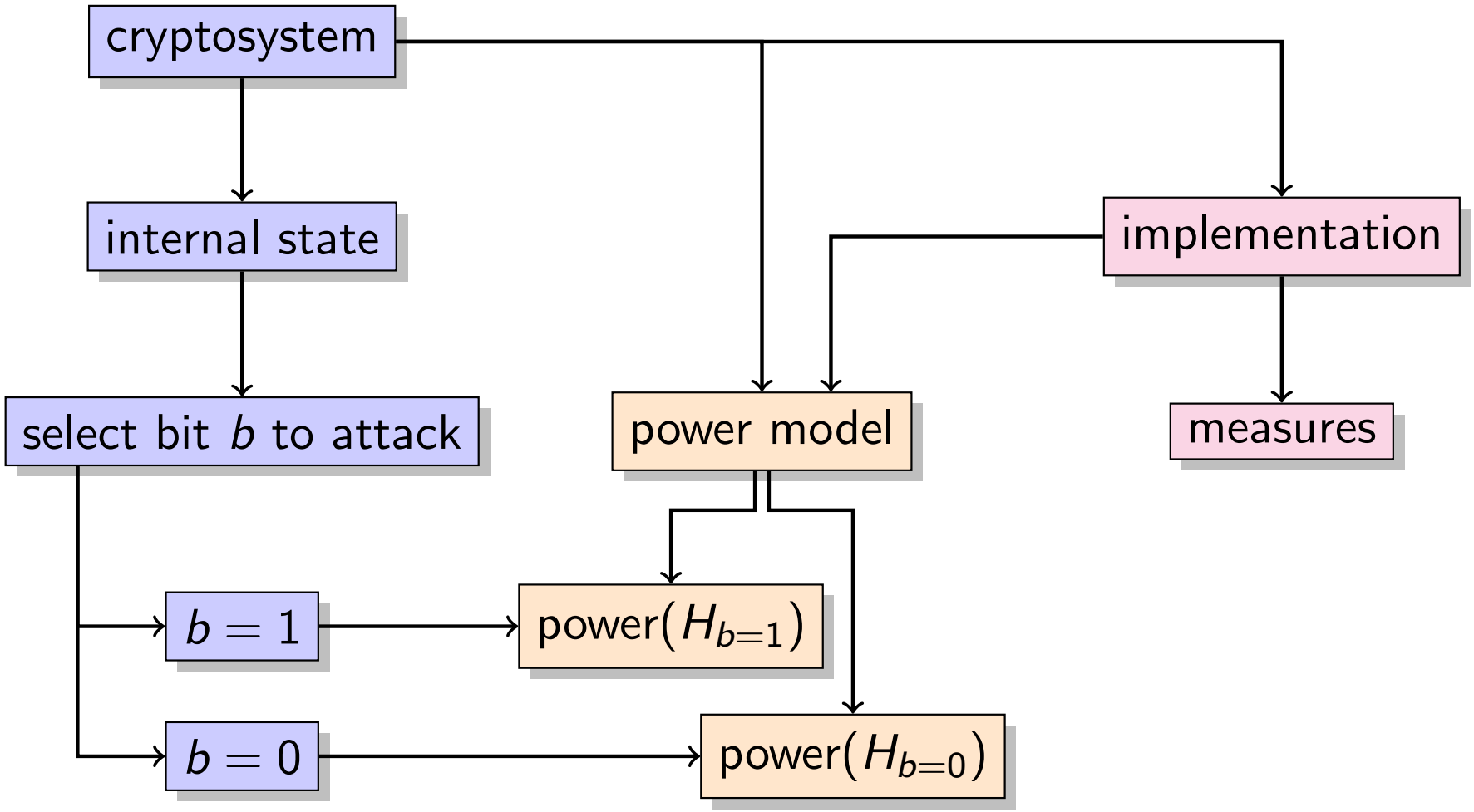
Differential Power Analysis (DPA)



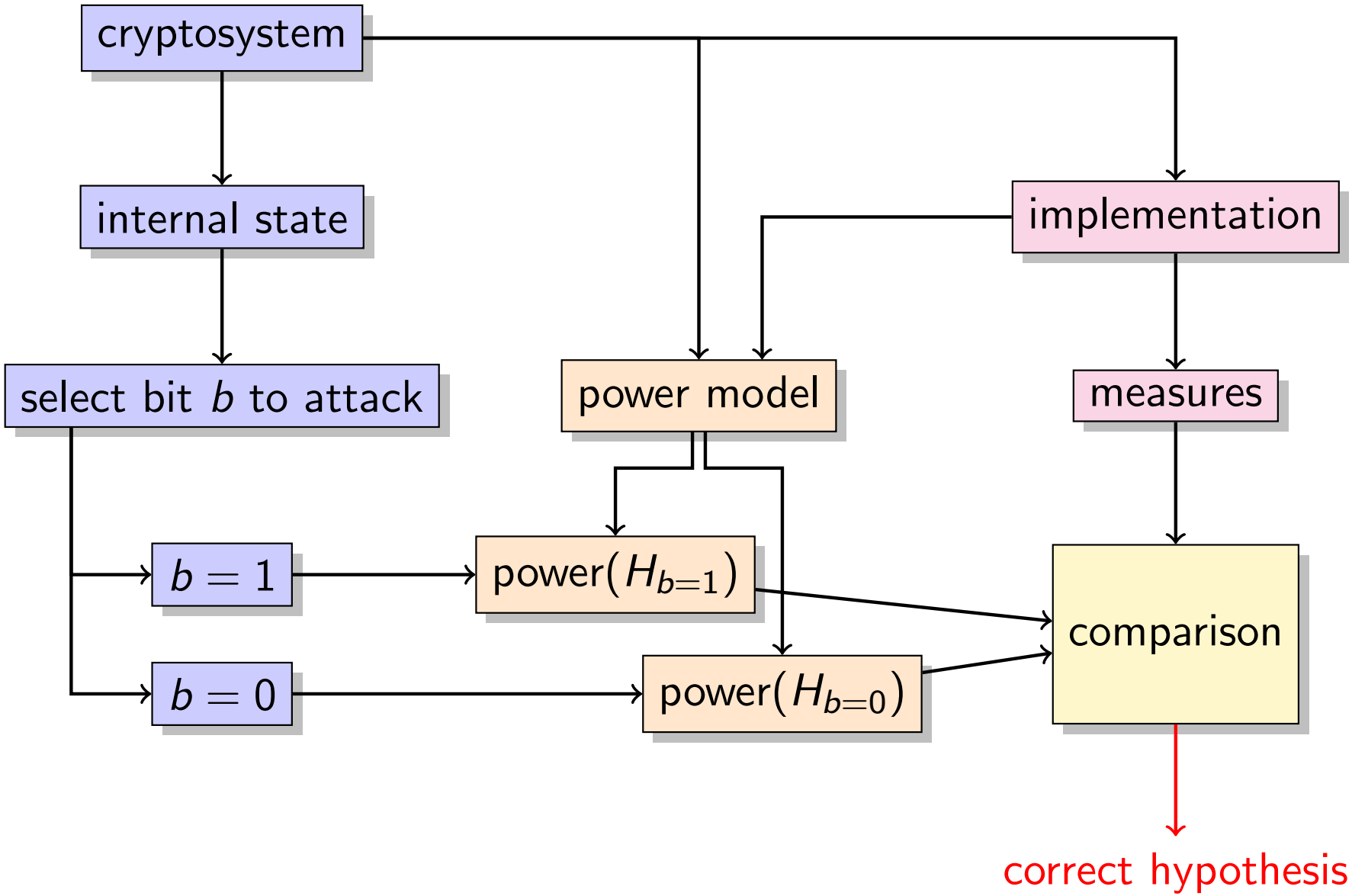
Differential Power Analysis (DPA)



Differential Power Analysis (DPA)



Differential Power Analysis (DPA)



Fault Injection Attacks

Objective: alter the correct functioning of a system "from outside"

Fault effects examples:

- modify a value in a register
- modify a value in the memory hierarchy
- modify an address (data location or code location)
- modify a control signal (e.g. status flag, branch direction)
- skip/modify the instruction decoding
- delay/advance propagation of internal control signals
- etc.

Also called perturbation attacks

Fault Injection Techniques

Typical techniques:

- perturbation in the power supply voltage
- perturbation of the clock signal
- temperature (over/under-heating the chip)
- radiation or electromagnetic (EM) disturbances
- exposing the chip to intense lights or beams
- etc

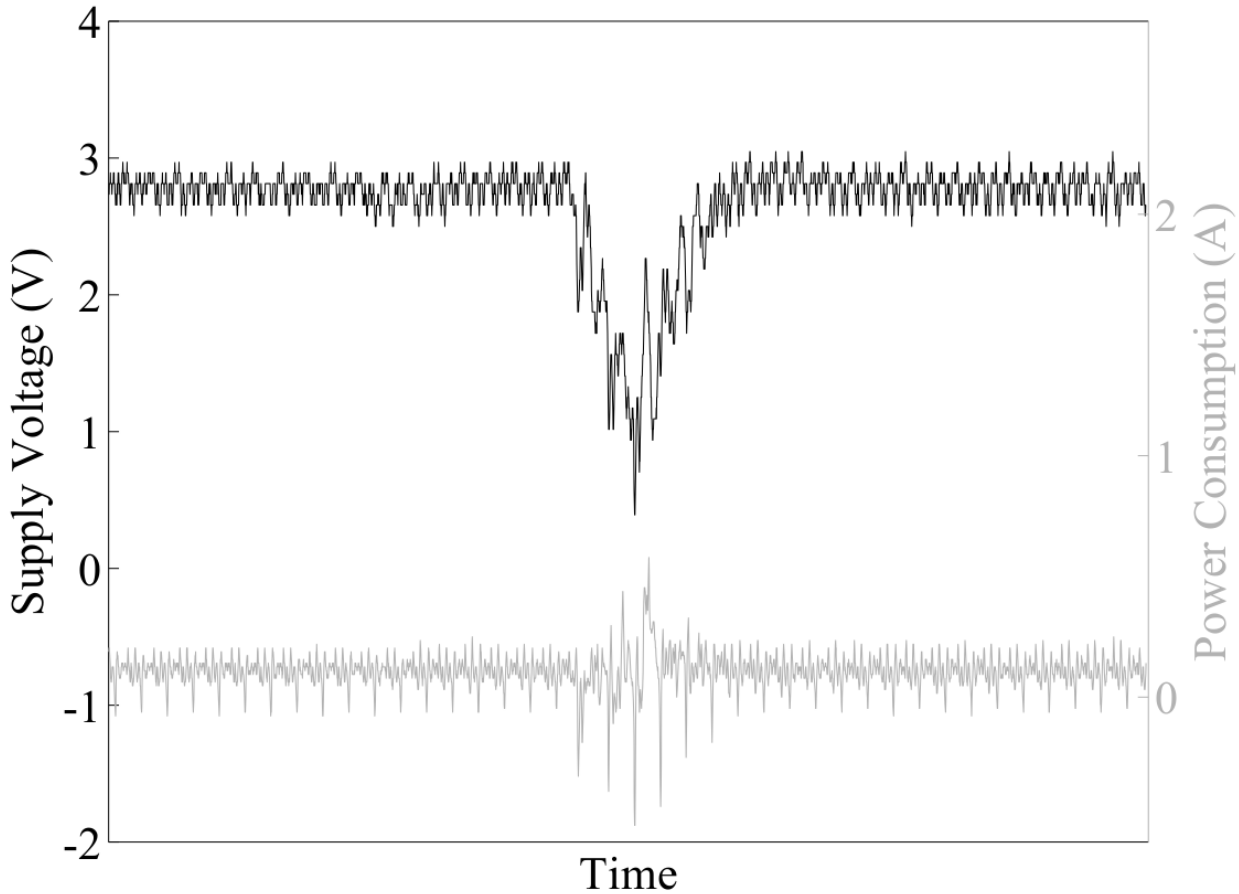
Accuracy:

- time: part of clock cycle, clock cycle, code block (instruction sequence)
- space: gate, block, unit, core, chip, package
- value: set to a specific value, bit flip, stuck-at 0 or 1, random modification

Power Glitching Example

Source: FDTC 2008 conference paper [4]

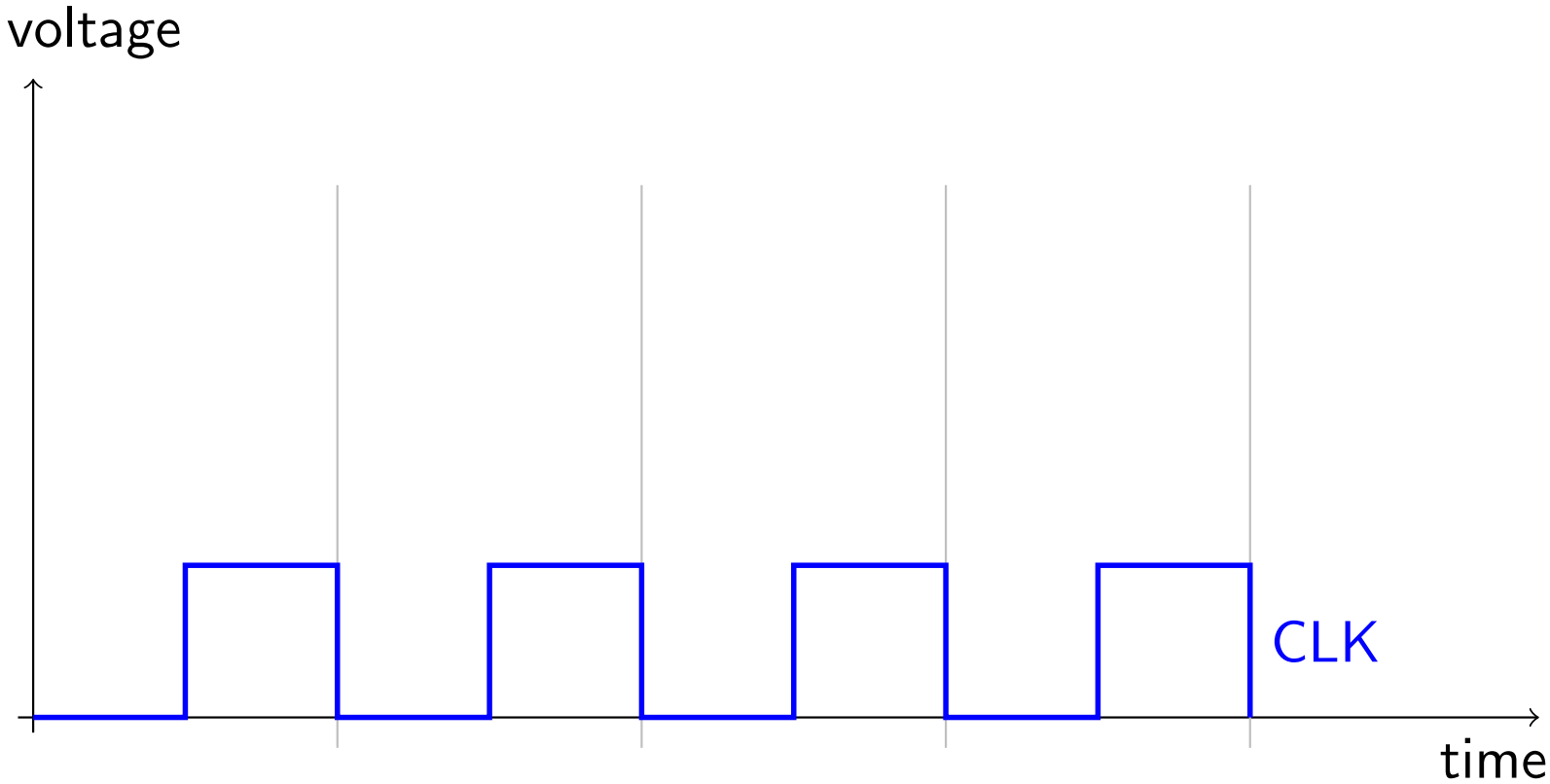
Setup: AVR microcontroller with RSA implementation



Attack result: a power glitch causes to skip some instruction

Perturbation on the External Clock

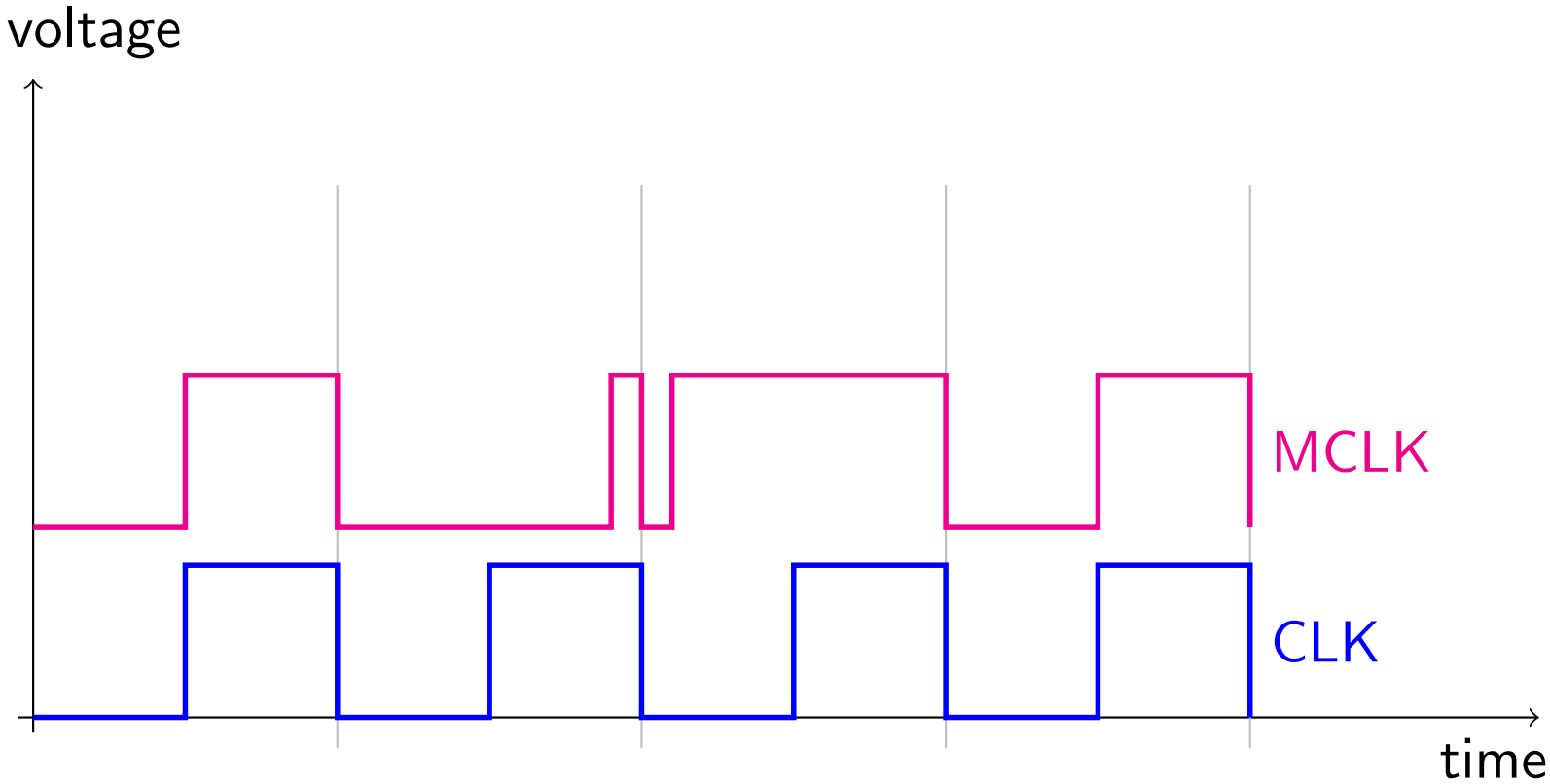
Principle:



- Normal clock (at a given frequency, duty cycle $\approx 50\%$)

Perturbation on the External Clock

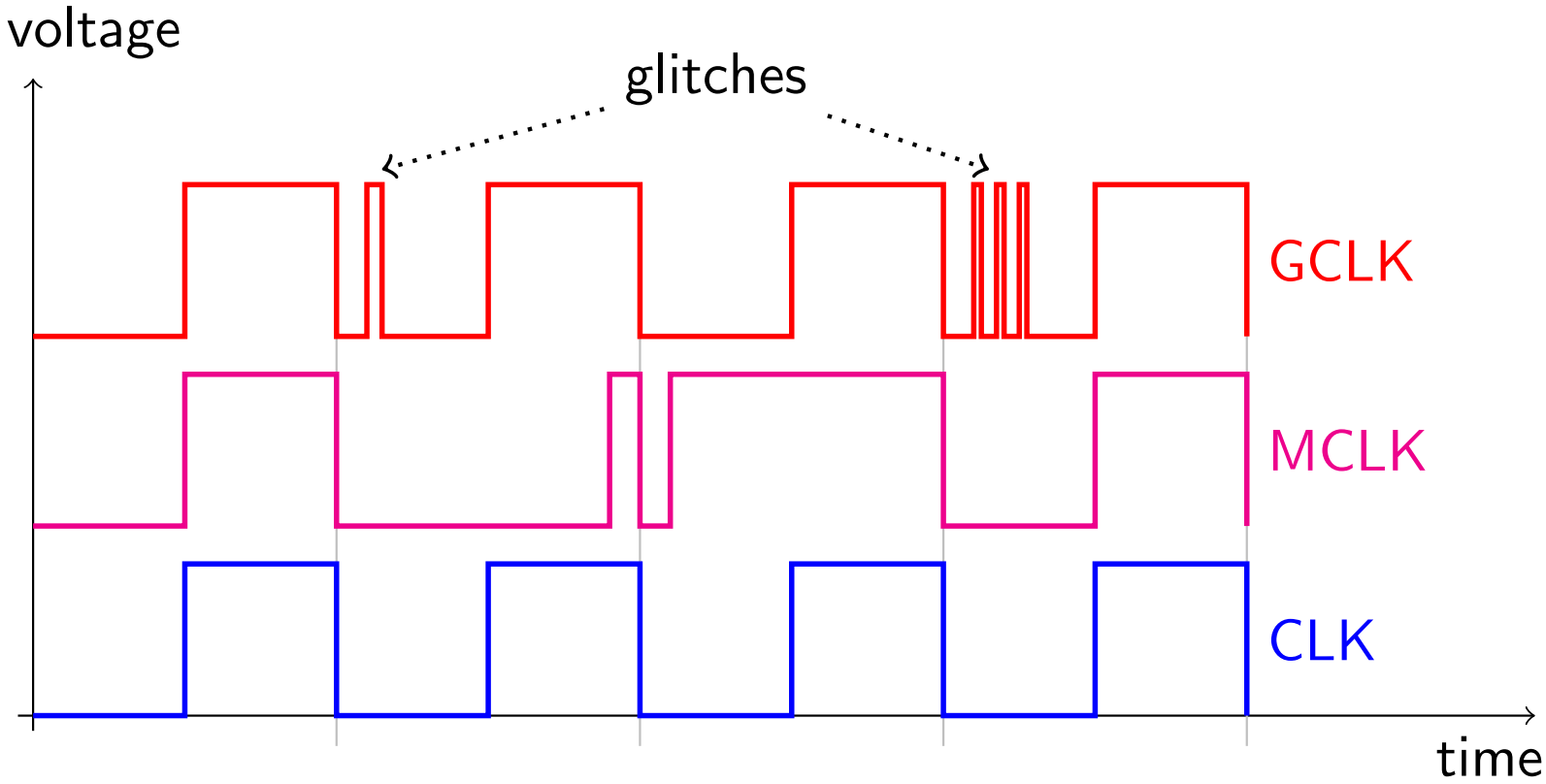
Principle:



- Normal clock (at a given frequency, duty cycle $\approx 50\%$)
- Clock with a modified duty cycle

Perturbation on the External Clock

Principle:



- Normal clock (at a given frequency, duty cycle $\approx 50\%$)
- Clock with a modified duty cycle
- Glitched clock
- Etc.

Clock Glitch Attack Example

Source: paper [1] presented at FDTC 2011 conference

Setup: AVR ATMega 163 microcontroller @ 1MHz

mode	glitch period	cycle	instruction	opcode (bin)
normal	-	i	`NOP`	0000 0000 0000 0000
normal	-	$i+1$	`EOR R15,R5`	0010 0100 1111 0101

Clock Glitch Attack Example

Source: paper [1] presented at FDTC 2011 conference

Setup: AVR ATMega 163 microcontroller @ 1MHz

mode	glitch period	cycle	instruction	opcode (bin)
normal	-	i	`NOP`	0000 0000 0000 0000
normal	-	$i+1$	`EOR R15,R5`	0010 0100 1111 0101
glitch	59 ns	$i+1$	`NOP`	0000 0000 0000 0000

Clock Glitch Attack Example

Source: paper [1] presented at FDTC 2011 conference

Setup: AVR ATMega 163 microcontroller @ 1MHz

mode	glitch period	cycle	instruction	opcode (bin)
normal	-	i	`NOP`	0000 0000 0000 0000
normal	-	$i+1$	`EOR R15,R5`	0010 0100 1111 0101
glitch	59 ns	$i+1$	`NOP`	0000 0000 0000 0000

mode	glitch period	cycle	instruction	opcode (bin)
normal	-	i	`NOP`	0000 0000 0000 0000
normal	-	$i+1$	`SER R18`	1110 1111 0010 1111

Clock Glitch Attack Example

Source: paper [1] presented at FDTC 2011 conference

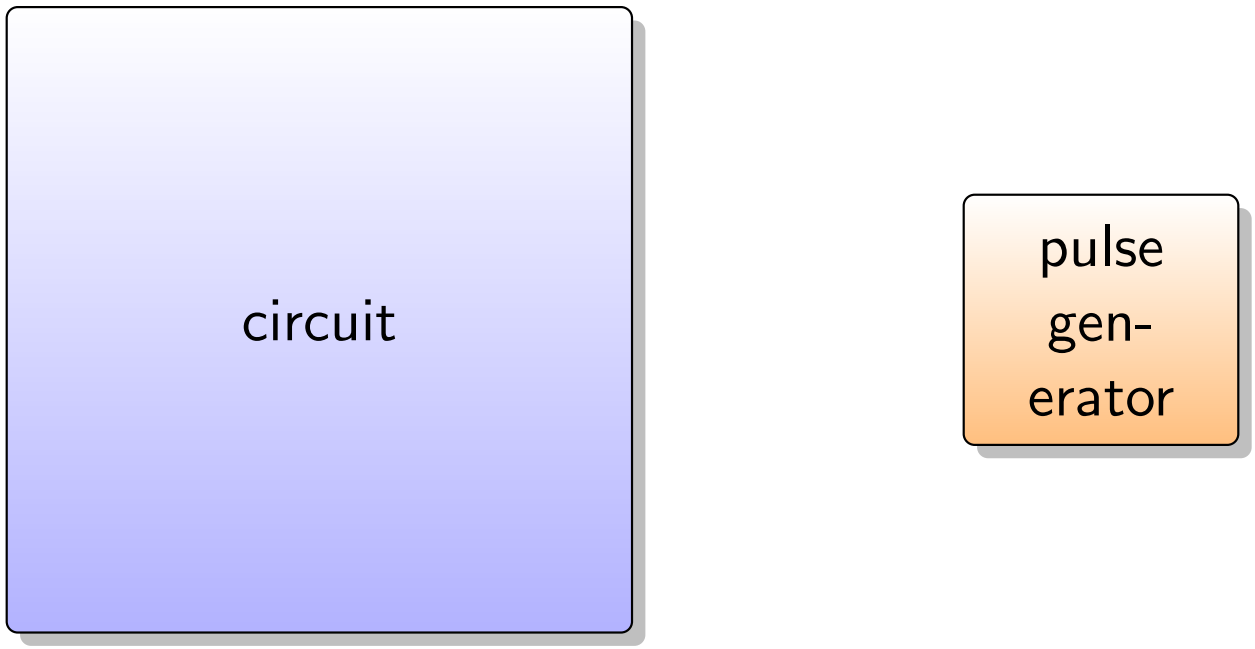
Setup: AVR ATMega 163 microcontroller @ 1MHz

mode	glitch period	cycle	instruction	opcode (bin)
normal	-	i	`NOP`	0000 0000 0000 0000
normal	-	$i+1$	`EOR R15,R5`	0010 0100 1111 0101
glitch	59 ns	$i+1$	`NOP`	0000 0000 0000 0000

mode	glitch period	cycle	instruction	opcode (bin)
normal	-	i	`NOP`	0000 0000 0000 0000
normal	-	$i+1$	`SER R18`	1110 1111 0010 1111
glitch	61 ns	$i+1$	`LDI R18,0xEF`	1110 1110 0010 1111
glitch	60 ns	$i+1$	`SBC R12,R15`	0000 1000 0010 1111
glitch	59 ns	$i+1$	`NOP`	0000 0000 0000 0000

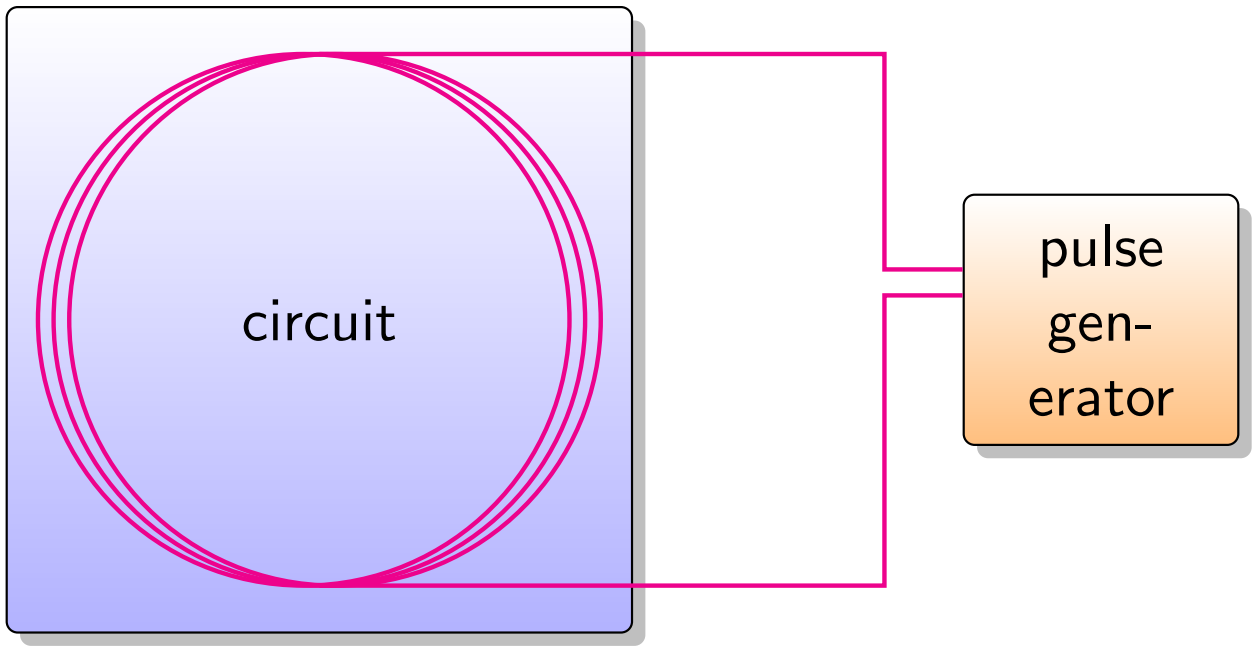
Electromagnetic Perturbations

Principle:



Electromagnetic Perturbations

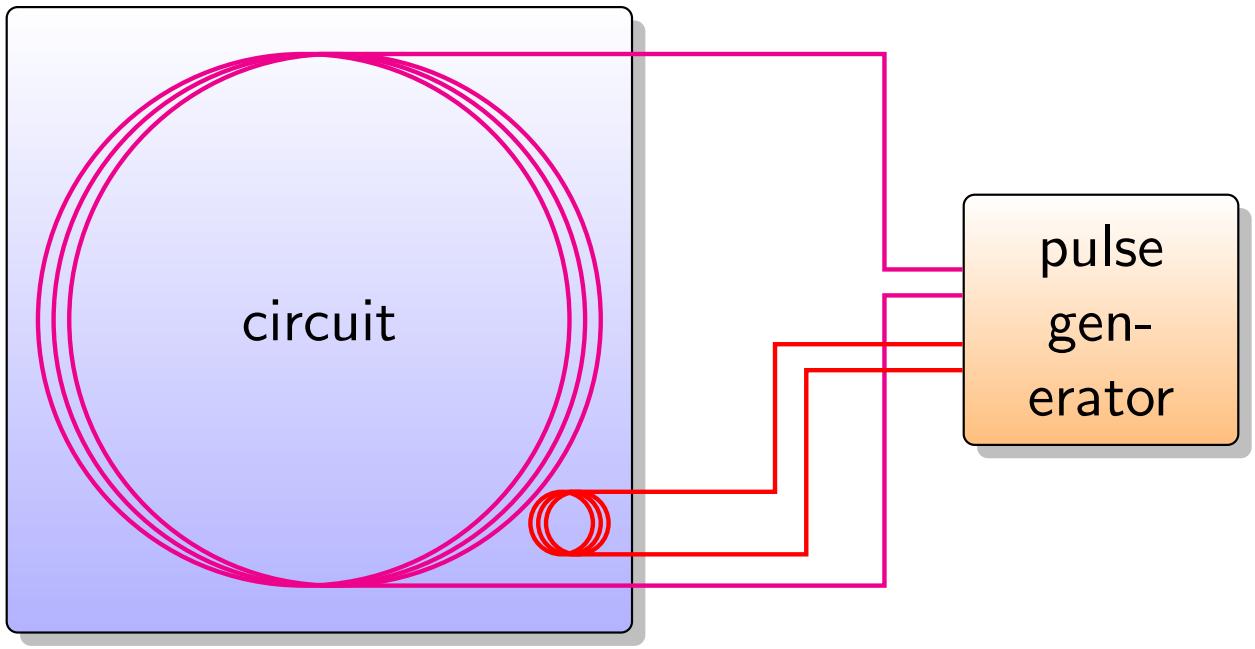
Principle:



- large antenna

Electromagnetic Perturbations

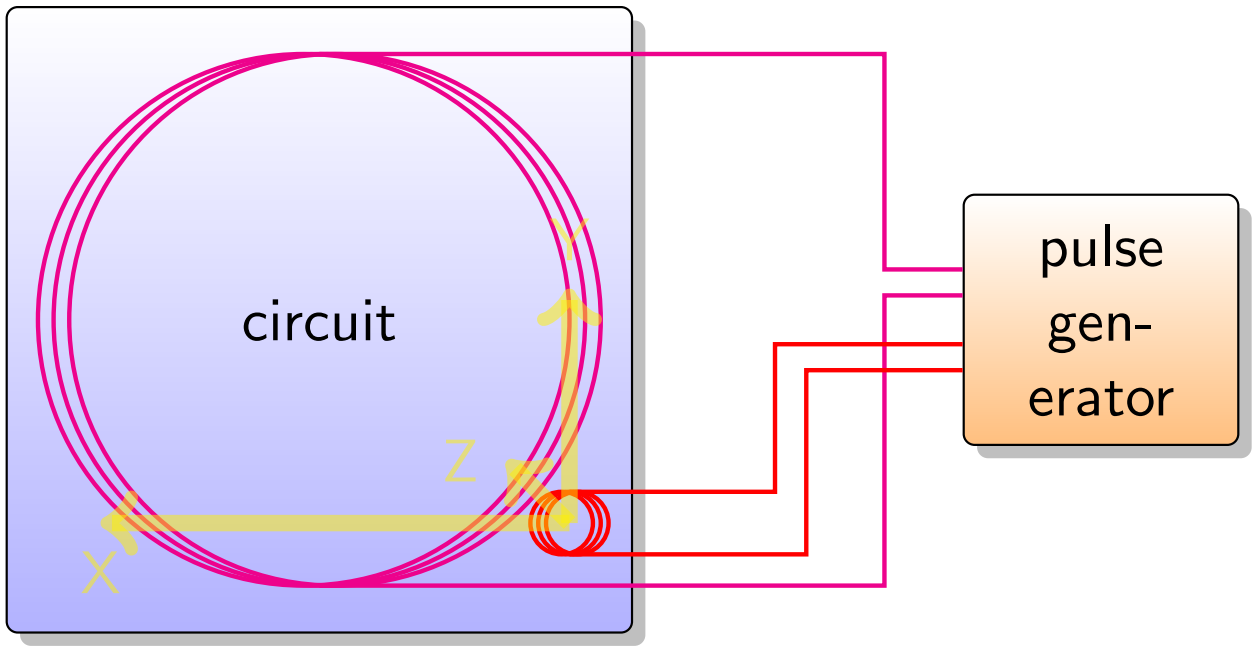
Principle:



- large antenna
- micro-antenna

Electromagnetic Perturbations

Principle:



- large antenna
- micro-antenna with motorized (X,Y,Z) stage/table

Electromagnetic Attack Example

Source: article [3] presented at FDTC 2013 conference

Setup: 32-b Cortex-M3 ARM microprocessor (CMOS 130 nm SoC at 56 MHz), magnetic antenna with pulses in [-200, 200] V and [10, 200] ns

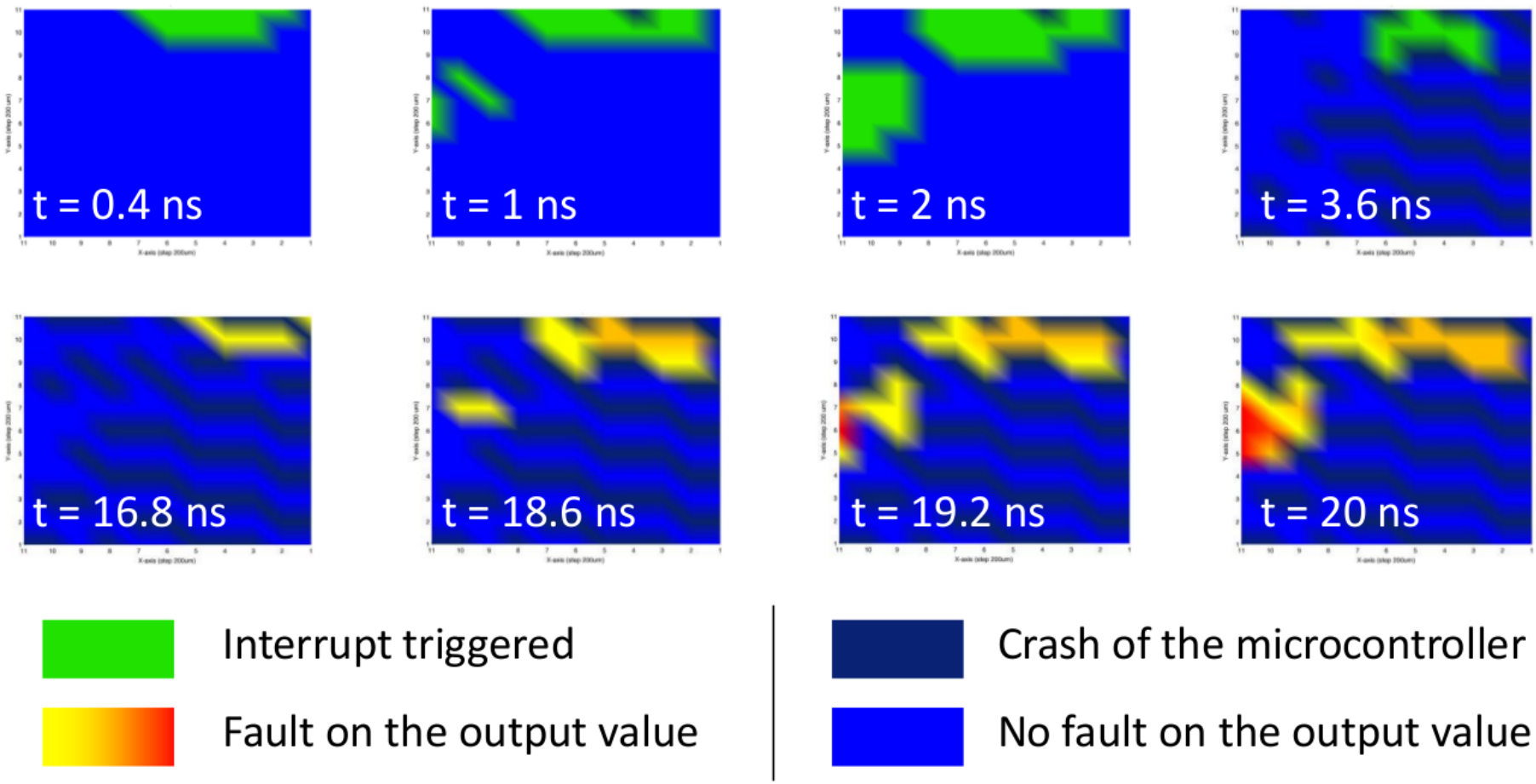


Figure 3: Impact of the probe's position

Loaded value: 12345678

Pulse voltage [V]	Loaded value	Occurrence rate [%]
170	1234 5678	100
172	1234 5678	100
174	9234 5678	73
176	FE34 5678	30
178	FFF4 5678	53
180	FFFD 5678	50
182	FFFF 7F78	46
184	FFFF FFFB	40
186	FFFF FFFF	100
188	FFFF FFFF	100
190	FFFF FFFF	100

Conclusion

- Side channel and fault attacks are serious threats
- Attacks are more and more efficient (many variants)
- Security analysis is mandatory at all levels (specification, algorithm, operation, implementation)
- Security = trade-off between performances, robustness and cost
- Security = *func*(secret value, attacker capabilities)
- security = computer science + microelectronics + mathematics

References I

[1] J. Balasch, B. Gierlichs, and I. Verbauwhede.
An in-depth and black-box characterization of the effects of clock glitches on 8-bit MCUs.
In *Proc. 8th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 105–114, Nara, Japan, September 2011. IEEE.

[2] P. C. Kocher, J. Jaffe, and B. Jun.
Differential power analysis.
In *Proc. Advances in Cryptology (CRYPTO)*, volume 1666 of *LNCS*, pages 388–397. Springer, August 1999.

[3] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz.
Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller.
In *Proc. 10th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 77–88, Santa Barbara, CA, USA, August 2013. IEEE.

[4] J. Schmidt and C. Herbst.
A practical fault attack on square and multiply.
In *Proc. 5th International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 53–58, Washington, DC, USA, August 2008. IEEE.

The end, questions ?

Contact:

- mailto:arnaud.tisserand@univ-ubs.fr
- http://www-labsticc.univ-ubs.fr/~tisseran
- CNRS, Lab-STICC Laboratory
  University South Brittany (UBS),
  Centre de recherche C. Huygens, rue St Maudé, BP 92116,
  56321 Lorient cedex, France

Thank you