DE LA RECHERCHE À L'INDUSTRIE

www.cea.fr

ROUND MODIFICATION ANALYSIS ON AES USING ELECTROMAGNETIC GLITCH

Amine DEHBAOUI [1], Amir-Pasha MIRBAHA [2], Nicolas MORO[1], Jean-Max DUTERTRE [2], Assia TRIA [1]

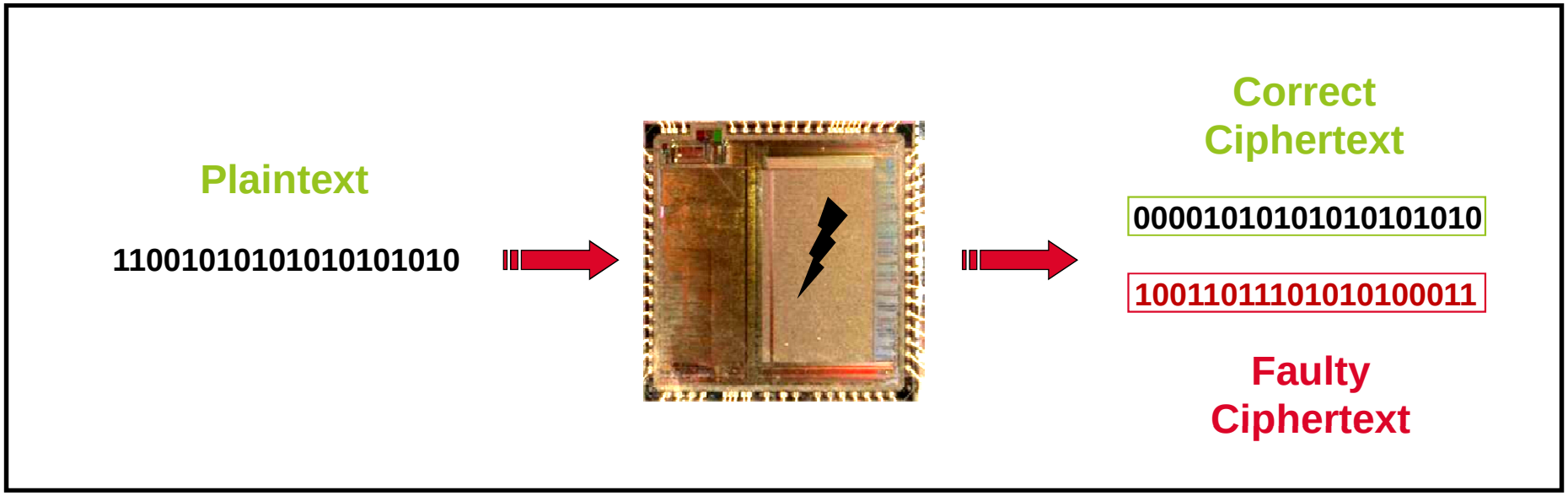
COSADE 2013
Paris, France

(1)	(2)
cea leti	Ecole Nationale Supérieure des Mines SAINT-ETIENNE

OUTLINE

- Context
- Round Modification Analysis on AES
- Proposed Round Modification Analysis on AES
- Electromagnetic Glitch Injection Technique
- Concrete Results with EMG
- Conclusion

CONTEXT : FAULT INJECTION



Fault injection means : Power supply glitch, Clock glitch, EM glitch, Laser shot …

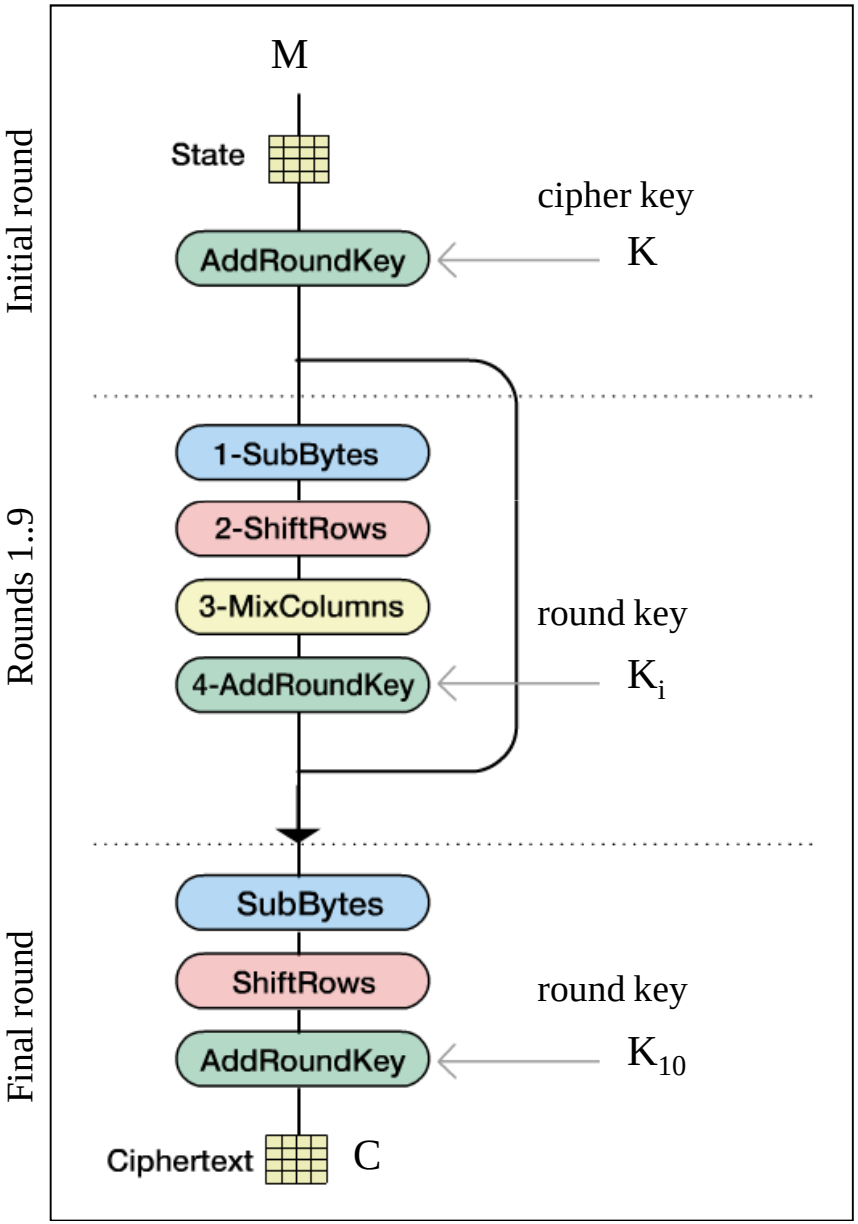
disturb the encryption/decryption process through unusual environmental conditions in order to :

- reduce the encryption complexity (e.g. round reduction analysis),
- differential fault analysis = comparison between correct and faulty ciphertexts.
- safe errors, HW/SW reverse engineering , …

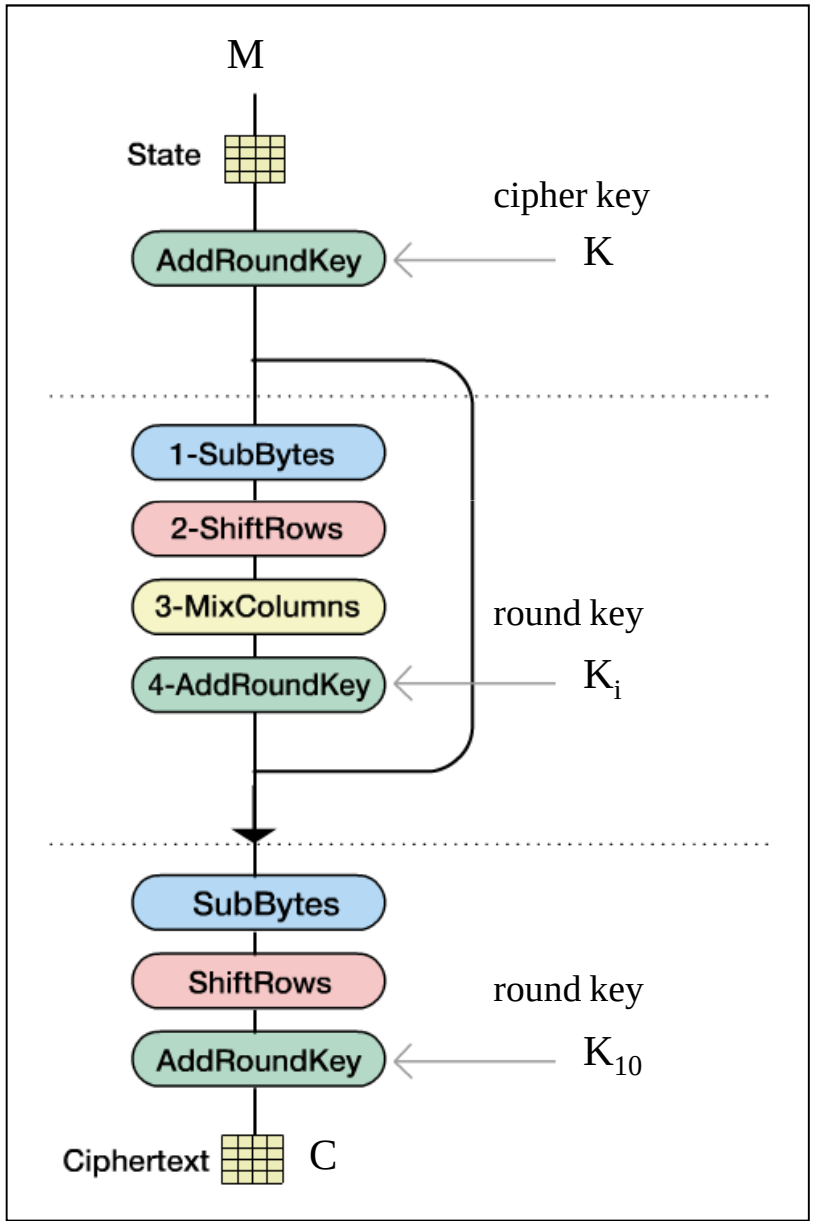
⇨ retrieve information on the encryption process (i.e. information leakage)

Round Modification Analysis on AES

ADVANCED ENCRYPTION STANDARD
128 BITS REMINDER



STATE-OF-THE-ART OF ROUND MODIFICATIONS ANALYSIS



Round **M**odification **A**nalysis

- **R**ound **R**eduction **A**nalysis

  decrease the number of executed rounds

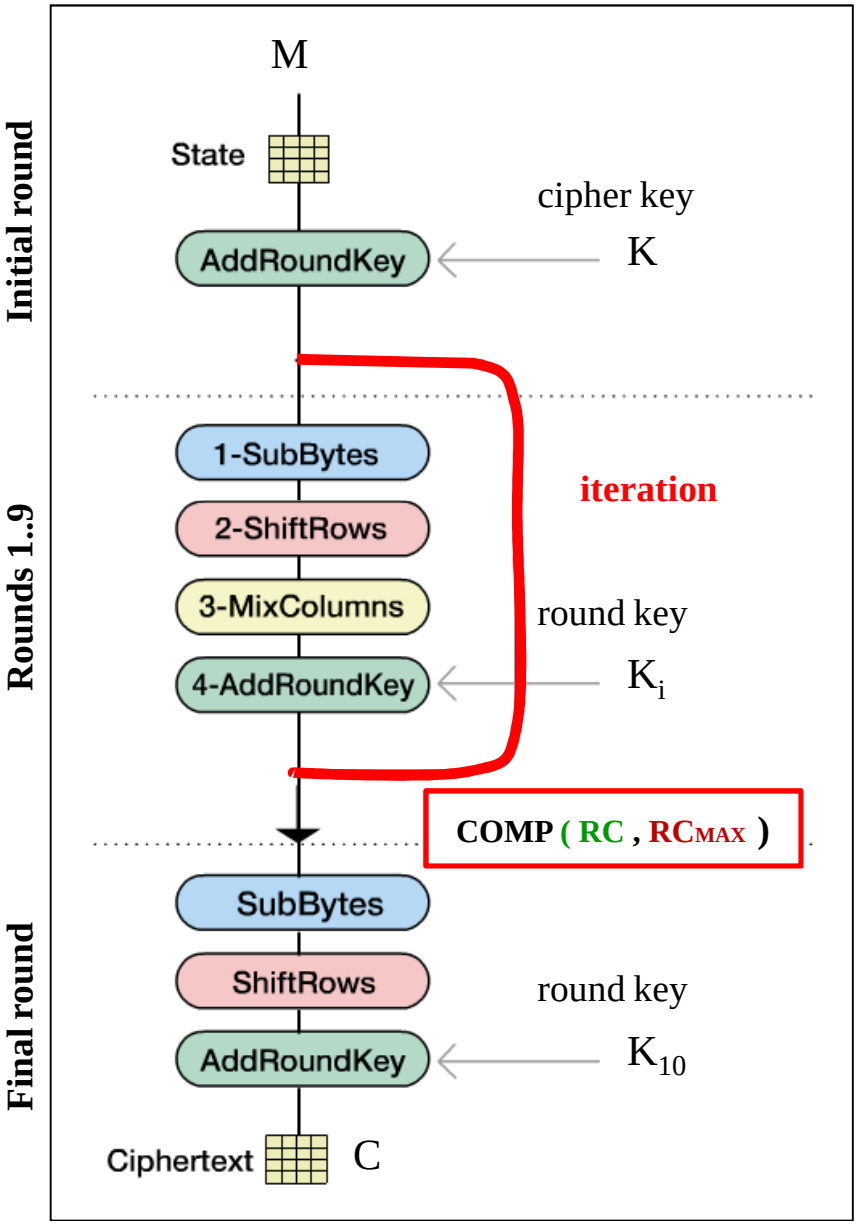
- **R**ound **A**ddition **A**nalysis

  increase the number of executed rounds

- **R**ound **A**lteration **A**nalysis

  modification of the round order

STATE-OF-THE-ART OF ROUND MODIFICATIONS ANALYSIS



Round Modification Analysis

❑ Round Reduction Analysis

- H. Choukri et al. [2005]
- J.H. Park et al. [2011]
- K.S. Bae et al.[2011]

❑Round Addition Analysis

- J.M. Dutertre et al. #3 [2012]

❑Round Alteration Analysis

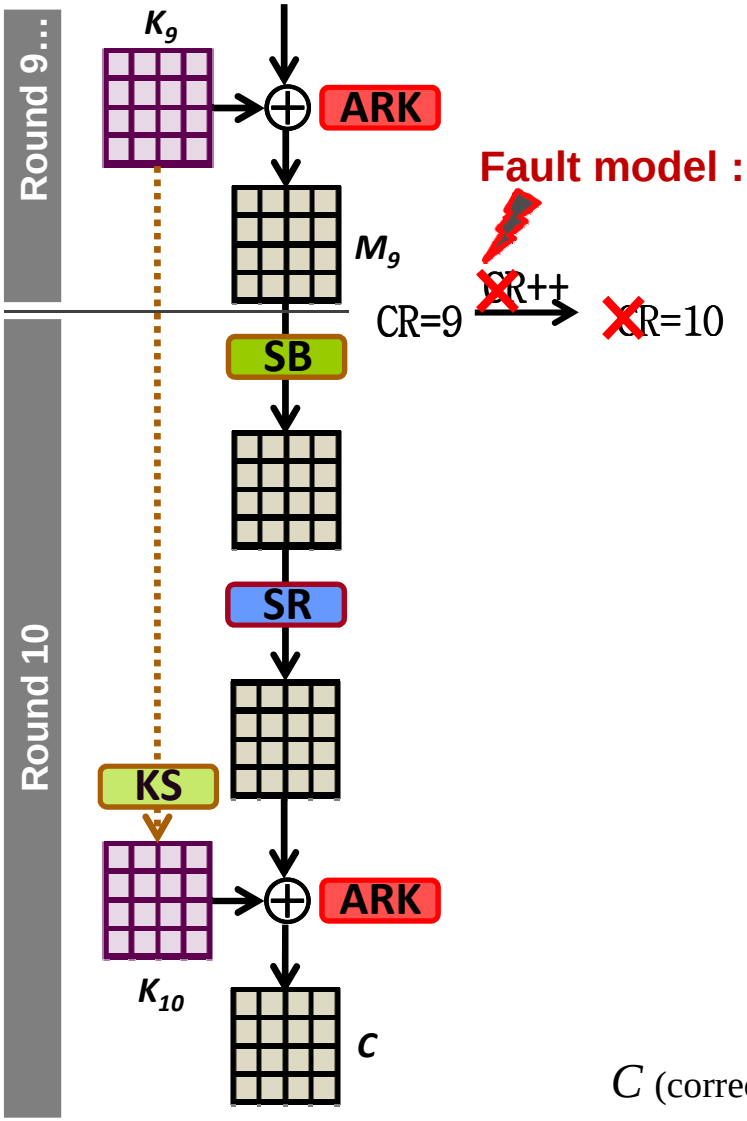
- J.M. Dutertre et al. #2 [2012]

STATE-OF-THE-ART OF ROUND MODIFICATIONS ANALYSIS

Attack	Target	Mean	Type	Encryption sequence	Req. texts	Key search average time
H. Choukri et al. [FDTC'05]	PIC16F877 8-bit	Power Glitch	Round Reduction	R_0-R_m	2	≈ 1 second
J.H. Park et al. [ETRI'11]	ATmega128 8-bit	Laser	Round Reduction	R_0-R_1-R_{10}	10	≈ 10 hours
K.S. Bae et al. [ICCIT'11]	ATmega128 8-bit	Laser	Round Reduction	R_0..R_8-R_{10}	2	≈ 1 second
J.M. Dutertre et al. #2 [HOST'12]	Unknown mcu 0.35µm 8-bit	Laser	Round Alteration	R_0..R_8-R_m-R_f	3	≈ 1 second
J.M. Dutertre et al. #3 [HOST'12]	Unknown mcu 0.35µm 8-bit	Laser	Round Addition	R_0..R_9-$R_{m=10}$-$R_{f=11'}$	3	≈ 1 hour & 30 minutes

Proposed Round Modification Analysis on AES

PROPOSED ROUND MODIFICATIONS ANALYSIS



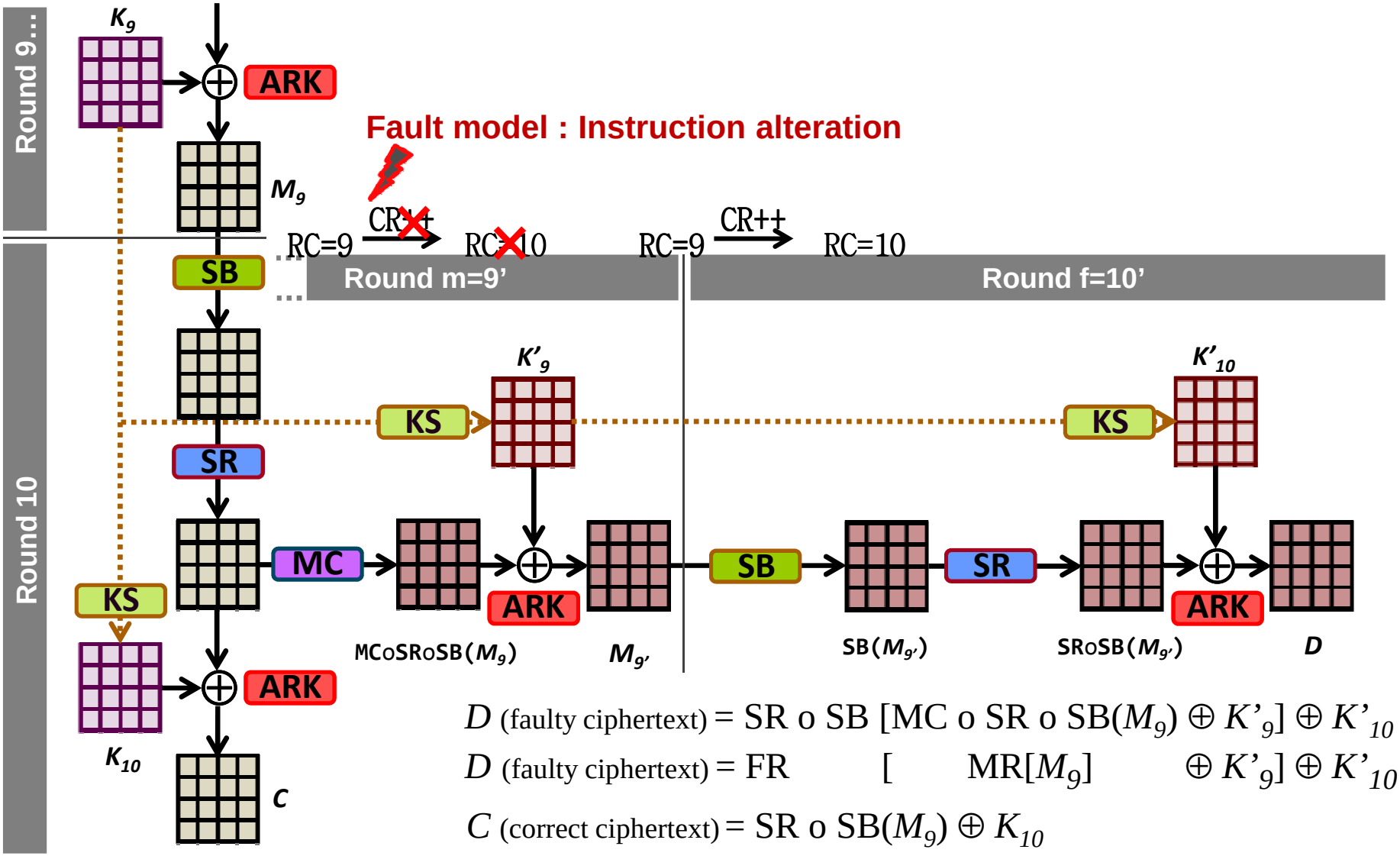
Fault model : Instruction alteration

CR=9 → CR++ → CR=10

C (correct ciphertext) = SR o SB(M_9) $\oplus$ K_{10}

C (correct ciphertext) = FR (M_9) $\oplus$ K_{10}

PROPOSED ROUND MODIFICATIONS ANALYSIS



D (faulty ciphertext) = SR o SB [MC o SR o SB(M_9) $\oplus$ K'_9] $\oplus$ K'_{10}

D (faulty ciphertext) = FR [MR[M_9] $\oplus$ K'_9] $\oplus$ K'_{10}

C (correct ciphertext) = SR o SB(M_9) $\oplus$ K_{10}

C (correct ciphertext) = FR (M_9) $\oplus$ K_{10}

PROPOSED ROUND MODIFICATIONS ANALYSIS

1 plaintext

$$D \text{ (faulty ciphertext)} = \text{FR}\,[\text{MR}(M_9) \oplus K'_9] \oplus K'_{10}$$
$$C \text{ (correct ciphertext)} = \text{FR}\,(M_9) \oplus K_{10}$$

2 plaintexts
M^a M^b

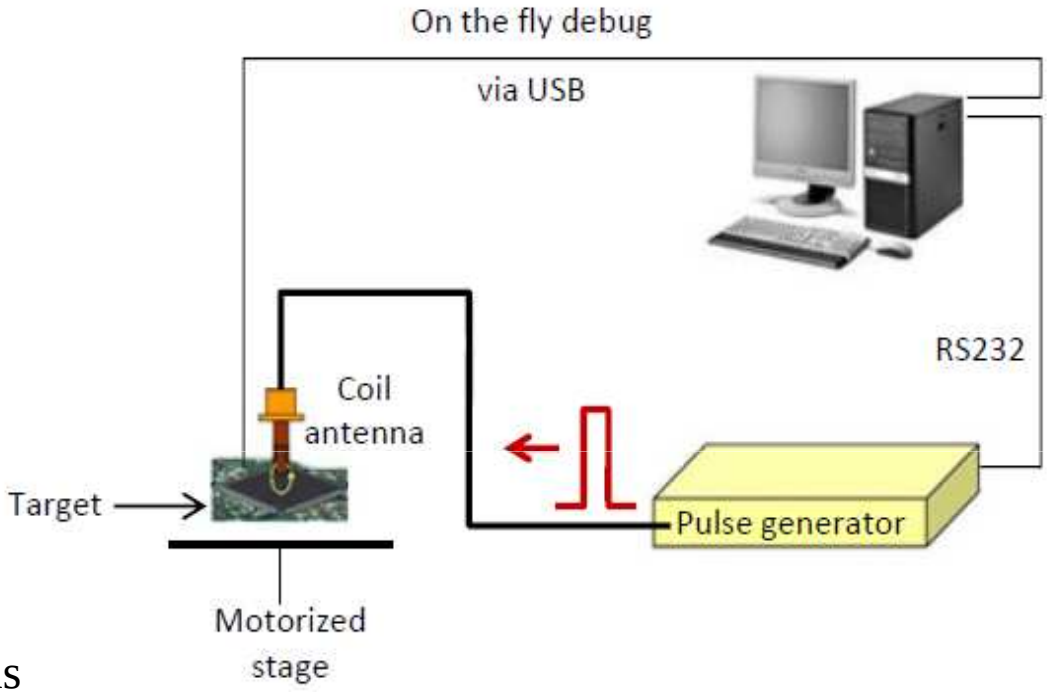
$$\text{FR}^{-1}(D^a \oplus \mathbf{K'_{10}}) \oplus \text{FR}^{-1}(D^b \oplus \mathbf{K'_{10}}) = \text{MC}(C^a \oplus C^b)$$

- 2 hypothese on each $\mathbf{K'_{10}}$ byte ($2^{\wedge 16}$ for a 128-bits AES key)
- Calculation time : < 1 second
- Alternative solution : 3 plaintexts, instead of 2
  thus, 1 hypothesis for each K'_{10} byte

Electromagnetic Glitch injection Technique

PRACTICAL ELECTROMAGNETIC GLITCH SETUP

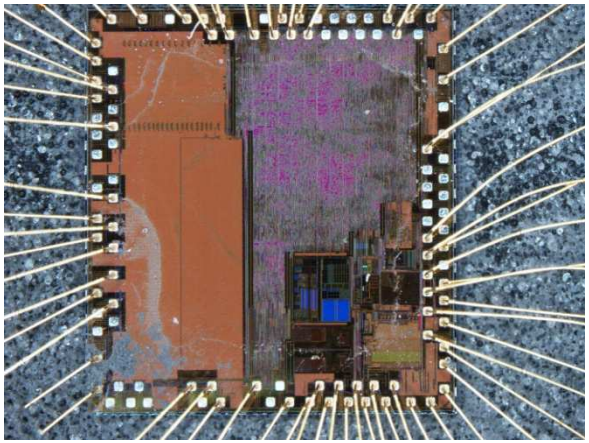
- Control computer
- The target device
- Motorized stage
- Pulse generator
- Coil antenna.



- Pulse width : 10 ns
- Rise and fall transition time : 2ns
- Pulse amplitude : -200V / +200V

The computer controls both the pulse generator (through a rs-232 link) and the target board (through a usb link).

Target Description



- Up-to-date 32-bit microcontroller
- Designed in a cmos 130nm technology
- Based on the arm Cortex-M3 processor.
- Operating frequency is set to 24MHz.
- Can detect several types of hardware faults.
- When a specific type of hardware fault is detected, the processor raises its associated interrupt.

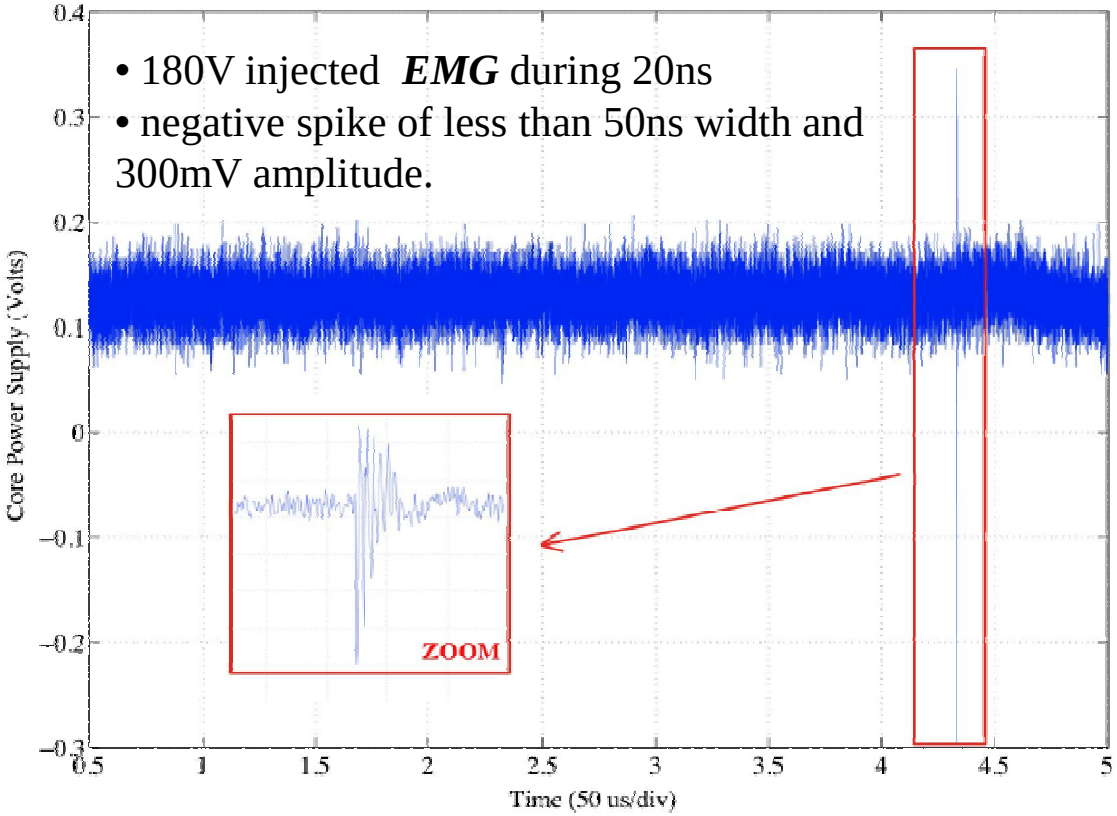
Exception	Description
Hard fault	Error during exception processing Has the highest priority
Bus fault	Memory related fault For an instruction or data memory transaction
Memory Management Fault	Triggered by the memory protection unit Possible access to a restricted memory area
Usage Fault	Fault related to instruction execution Undefined instruction, illegal unaligned access, etc.
Clock Security System	Error on the high speed external clock
Programmable Voltage Detect	The power supply is under a user-defined threshold

Concrete Results with EMG

EMG PROFILE OF THE TARGET

EM Channel : main strengths

- Does **not require depackaging** the target.
- Does **target the upper metal Layer** (Power/Ground or Clock networks).



Logical Effect :

instruction alteration

EXPERIMENTAL OUTLINE

Algorithm 2 Experimental process

Set the relative position of the antenna on top of the surface of the package
Define a time interval $[t_{min};t_{max}]$ to inject the EMG
Initialize the pulse generator
Define a time step Δt
Initialize a random fixed key and plaintext
for $t = t_{min}$ step Δt to t_{max} do
  microcontroller_reset()
  launch AES()
  send_pulse_with_delay(t)
  sleep(100ms)
  microcontroller_stop()
  results = microcontroller_get_status()
  print_and_store(*results*)
end for

```
Execution normale pour calibration
-----------------------------------------
[ OK ] Debut de l'execution du programme
[ OK ] 1 seconde de pause
[ OK ] Arret de la carte
[ OK ] Recuperation des registres
[ OK ] Recuperation du registre xPSR
[ OK ] Recuperation du Fault Status Register
[ OK ] Reset de la carte pour l'execution suivante
-----------------------------------------
Registres:
R0=0x200003F0
R1=0x200003E8
R2=0x00010000
R3=0x00010800
R4=0x00000008
R5=0x0800088C
R6=0x00000000
R7=0x00000000
R8=0x00000000
R9=0x20000160
R10=0x00000000
R11=0x00000000
R12=0x00000100

Registres particuliers:
R13 Stack Pointer = 0x200003C8
R14 Link Register = 0xFFFFFFF9
R15 Program Counter = 0x080006E6
xPSR Program Status Register = 0x21000006

Flags:
N - Negative = 0
Z - Zero = 0
C - Carry = 1
V - Overflow = 0
Q - Saturation = 0

Interruption:
Execution : UsageFault
UNDEFINSTR - Undefined instruction UsageFault
```

TIMING CARTOGRAPHY OF EMG EFFECT

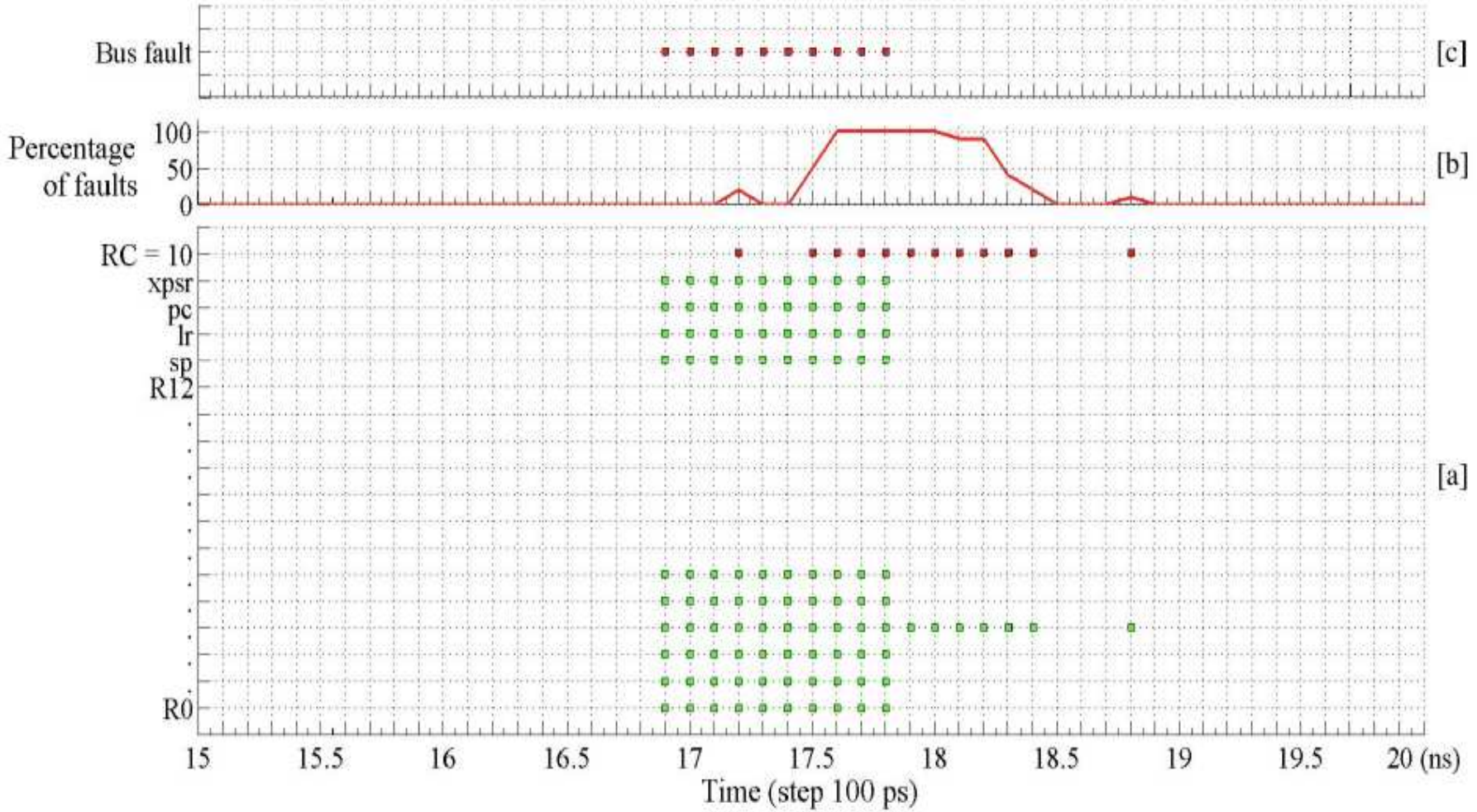


Fig. 3. Timing cartography of the EMG effect on the microcontroller

Conclusion

Conclusion

- Round Modification Analysis by **targeting the round counter**
- Fault induced at the end of the penultimate round
- **Execution of a second penultimate round**
- EMG Fault model : **instruction alteration**
- High occurrence rate / without triggering hardware interrupts

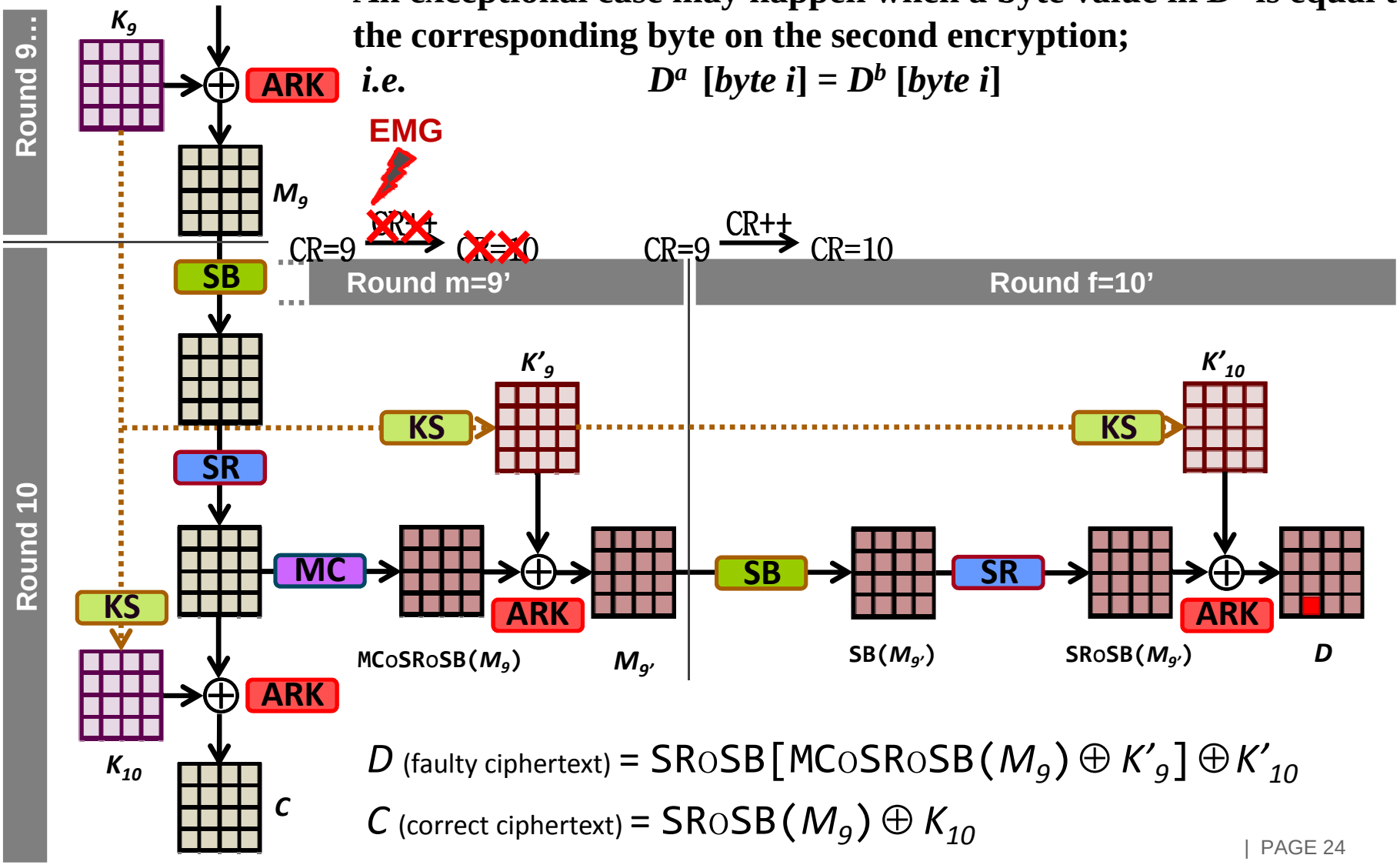
Attack	Target	Mean	Type	Encryption sequence	Req. texts	Key search average time
H. Choukri et al. [FDTC'05]	PIC16F877 8-bit	Power Glitch	Round Reduction	R_0-R_m	2	≈ 1 second
J.H. Park et al. [ETRI'11]	ATmega128 8-bit	Laser	Round Reduction	R_0-R_1-R_{10}	10	≈ 10 hours
K.S. Bae et al. [ICCIT'11]	ATmega128 8-bit	Laser	Round Reduction	R_0..R_8-R_{10}	2	≈ 1 second
J.M. Dutertre et al. #2 [HOST'12]	Unknown mcu 0.35µm 8-bit	Laser	Round Alteration	R_0..R_8-R_m-R_f	3	≈ 1 second
J.M. Dutertre et al. #3 [HOST'12]	Unknown mcu 0.35µm 8-bit	Laser	Round Addition	R_0..R_9-$R_{m=10}$-$R_{f=11'}$	3	≈ 1 hour & 30 minutes
Our experiment [COSADE'13]	**ARM Cortex-M3 based 130nm 32-bit**	**EM Glitch**	**Round Addition**	**R_0..R_9-$R_{m=9'}$-$R_{f=10'}$**	**2**	**≈ 1 second**

Annexe : RMA Exceptionnel case

RMA – An Exceptional Case

An exceptional case may happen when a byte value in D^a is equal to the corresponding byte on the second encryption;

i.e. D^a **[*byte i*] =** D^b **[*byte i*]**



D (faulty ciphertext) = $\mathrm{SRoSB}[\mathrm{MCoSRoSB}(M_9) \oplus K'_9] \oplus K'_{10}$

C (correct ciphertext) = $\mathrm{SRoSB}(M_9) \oplus K_{10}$

RMA – An Exceptional Case

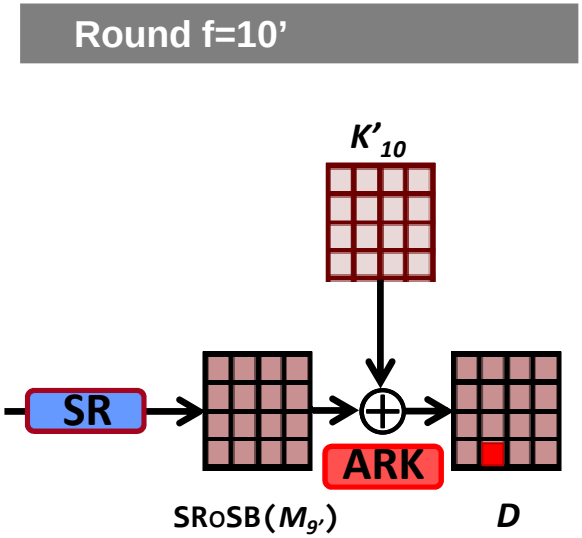
Example:

An exceptional case may happen when a byte value in D^a is equal to the corresponding byte on the second encryption;
i.e. D^a [*byte i*] = D^b [*byte i*]

M^a : 32 43 F6 A8 88 5A 30 8D 31 31 98 A2 E0 37 07 34
M^b : 19 84 B0 92 95 C8 B1 D9 C4 4E 4D 1E F2 C0 36 5E

C^a : 39 25 84 1D 02 DC 09 FB DC 11 85 97 19 6A 0B 32
C^b : 13 AB D8 4B 7B EA FA 58 47 58 48 A5 50 B3 B2 DC

D^a : 49 4a b5 1f 3b 08 83 e0 d1 21 34 6b 32 cd 31 cb
D^b : 8c fc 54 6b 3a 46 9e e0 b7 65 6d 0a 92 7b a0 e1



RMA – An Exceptional Case

D^a : 49 4a b5 1f 3b 08 83 **e0** d1 21 34 6b 32 cd 31 cb

D^b : 8c fc 54 6b 3a 46 9e **e0** b7 65 6d 0a 92 7b a0 e1

$$SB^{-1} \circ SR^{-1}(D^a \oplus K'_{10}) \oplus SB^{-1} \circ SR^{-1}(D^b \oplus K'_{10}) = MC(C^a \oplus C^b)$$

➡ **2^8 hypotheses**
on $K'_{10}[7]$ (byte [7] of K'_{10})
and **2 hypotheses**
on each other K'_{10} byte

➡ **$2^8 \times 2^{15} = 2^{23}$ hypotheses**
on the *whole-*K'_{10}

➡ to be examined by using C^a and D^a,
and by calculating K'_9 and K_{10}

➡ **calculation time : still less than 1 second**

RMA – An Exceptional Case

Probability of this exceptional case =

$$1- \frac{\binom{255}{1}}{\binom{256}{1}} \times \frac{\binom{255}{1}}{\binom{256}{1}} \times \ldots\ldots \frac{\binom{255}{1}}{\binom{256}{1}} = 1-\left(\frac{255}{256}\right)^{16} \approx \%6.070$$

➡ with 1, 2 or even 3 equal byte values on D^a and D^b, the cryptanalysis has an answer in a short calculation time

➡ In any case, there is a faster solution : using 3 plaintexts, instead of 2

Any questions ?

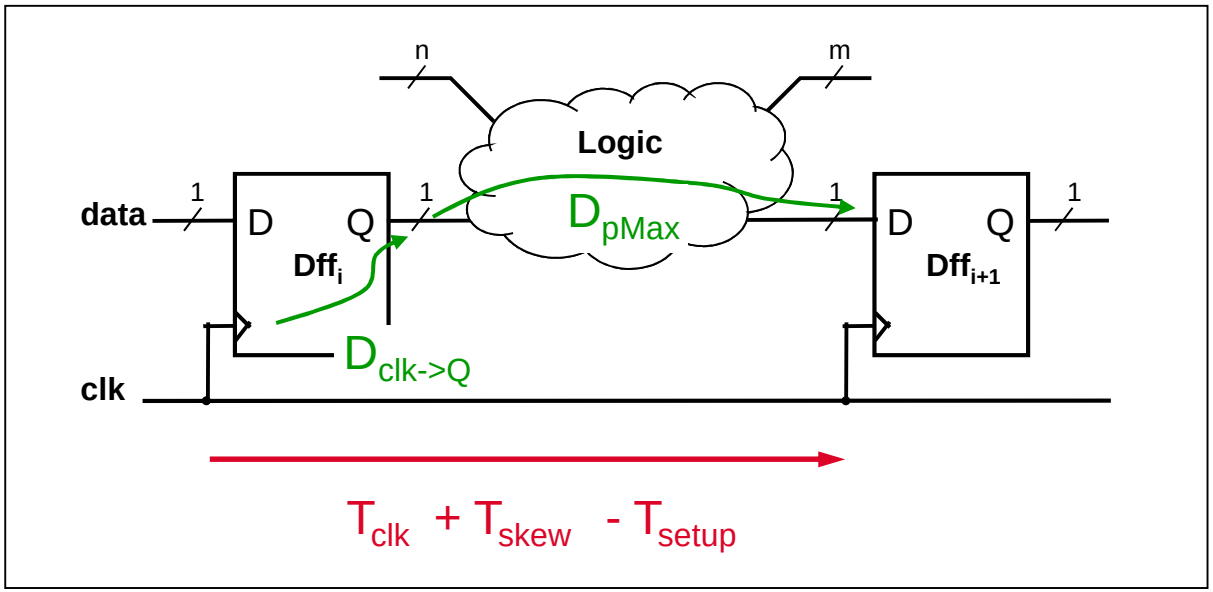
Direction de la Recherche Technologique
DSIS / LCS
Systèmes et Architectures Sécurisés

Commissariat à l'énergie atomique et aux énergies alternatives
Centre de Microélectronique de Provence | 13541 Gardanne
T. +33 (0) 4.42.61.67.31| F. +33 (0) 4.42.61.65.92

Etablissement public à caractère industriel et commercial | RCS Paris B 775 685 019

Annexe : Digital IC

Synchronous Digital IC Timing Constraints



data arrival time = $D_{clk->Q} + D_{pMax}$ **data required time** = $T_{clk} + T_{skew} - T_{setup}$

$$\Rightarrow \quad T_{clk} > D_{clk->Q} + D_{pMax} - T_{skew} + T_{setup}$$

F(Vdd)

Violating this timing constraint results in **fault injection.**
Usually IC are designed to tolerate : **Vdrops < 0.1 x Vdd**