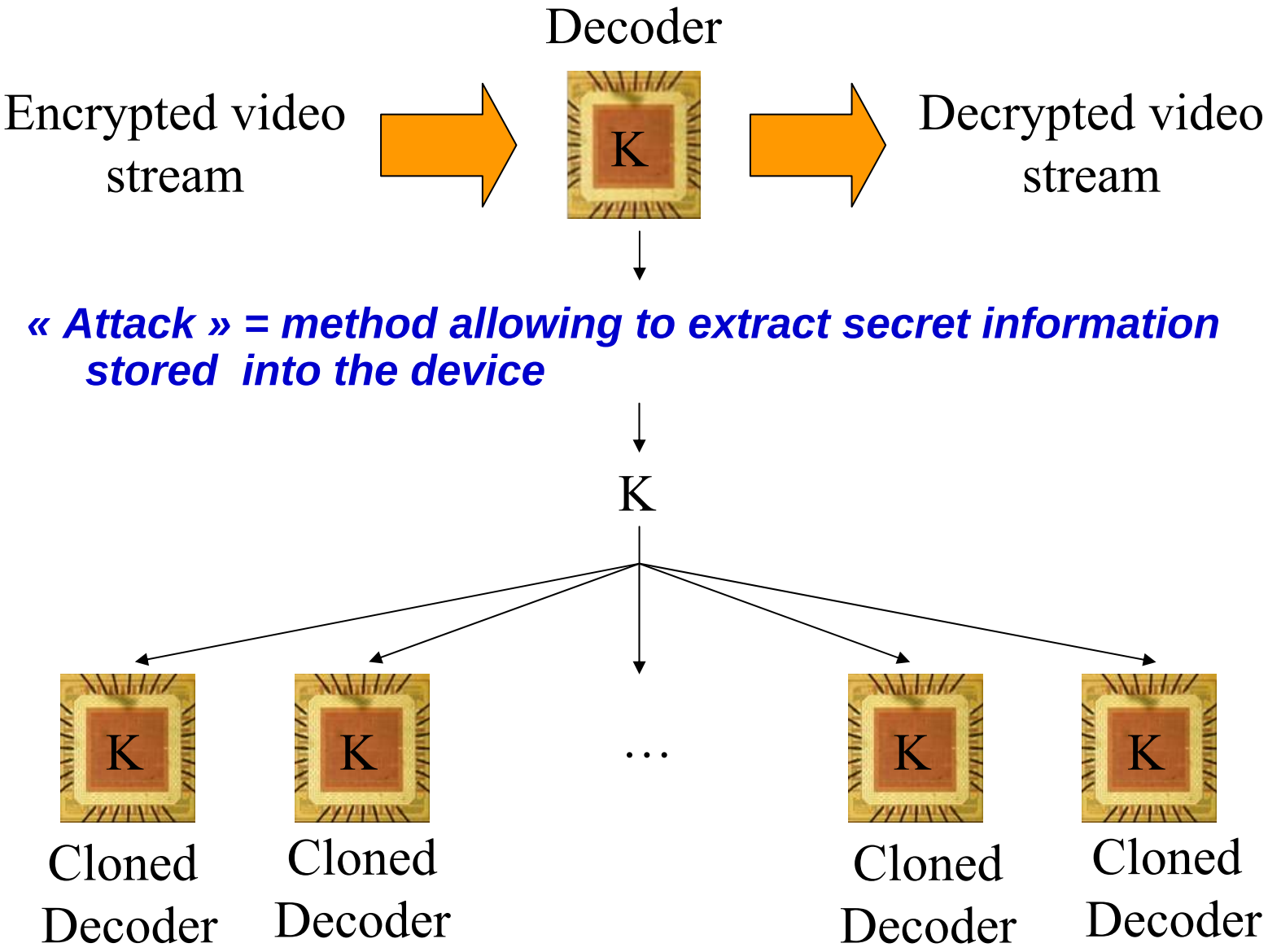
«Circuits sécurisés : nécessité de prendre en compte les fautes»

Bruno ROBISSON

CEA-LETI/DCIS/SCME
Laboratoire de Conception de Circuits Sécurisés

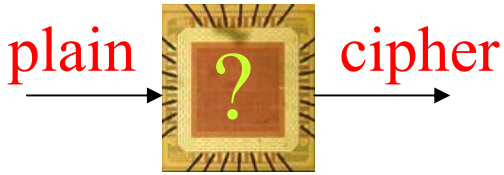
SESAM Laboratory (joint R&D team CEA-LETI/EMSE),
Centre Microélectronique de Provence
Avenue des Anémones, 13541 Gardanne, France

Problem

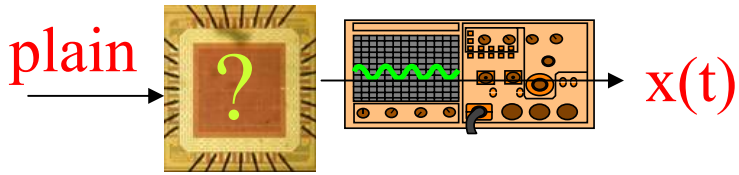

Decoder
Encrypted video stream
K
Decrypted video stream
« Attack » = method allowing to extract secret information stored into the device
K
K
K
…
K
K
Cloned Decoder
Cloned Decoder
Cloned Decoder
Cloned Decoder

Attacks

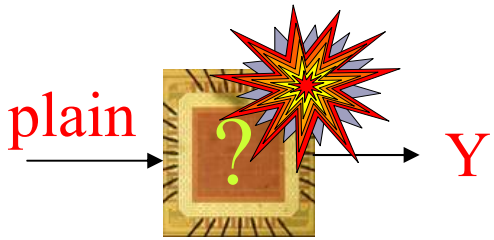
Cryptanalysis : mathematical analysis of plain and cipher texts sets



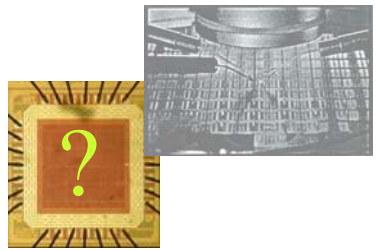
Side channel attacks : analysis of the chip environment when it performs sensitive computations



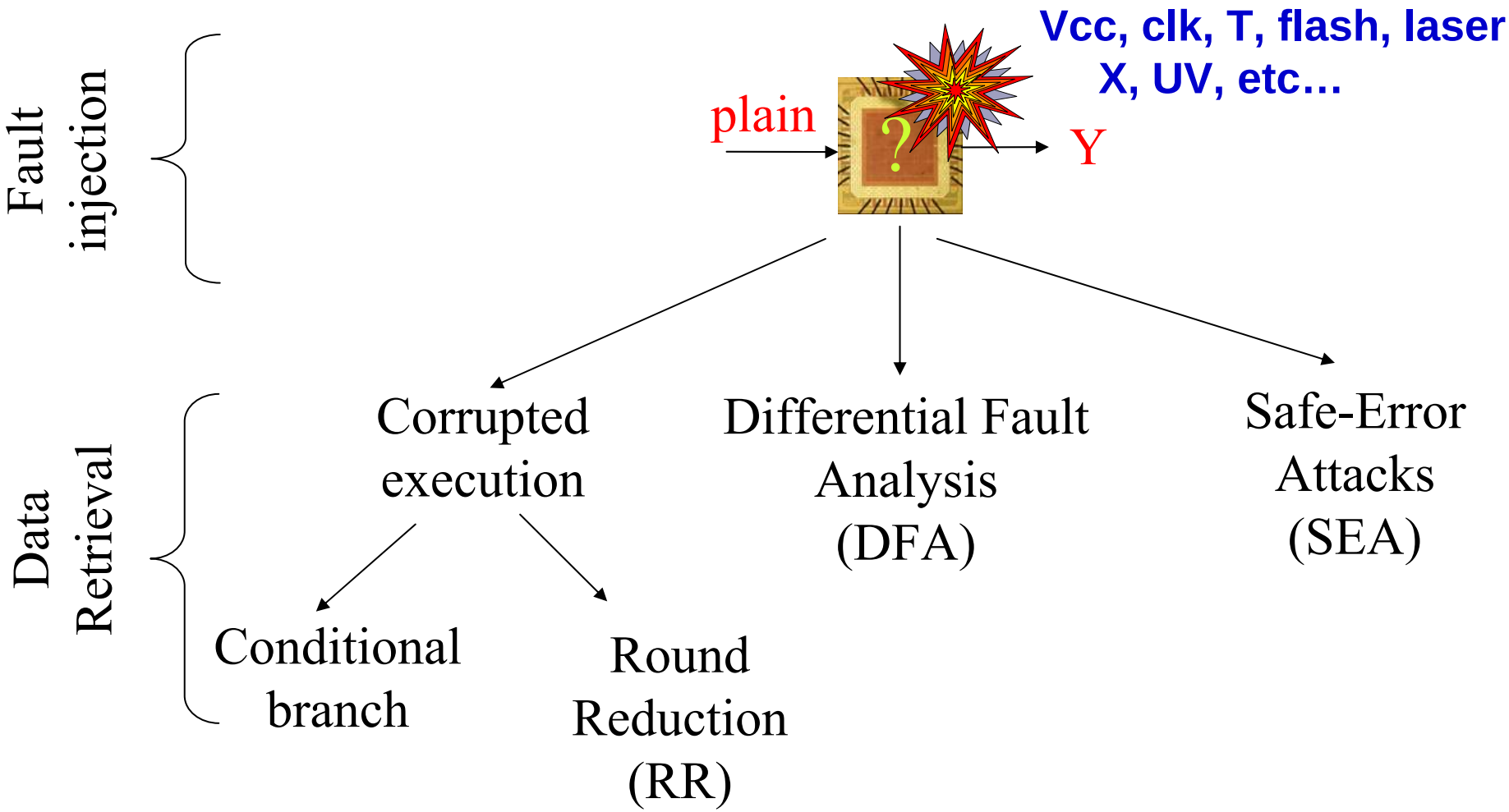
Fault attacks : modifications of the chip environment to bypass H/S protections



Invasives attacks : probing of internal signals



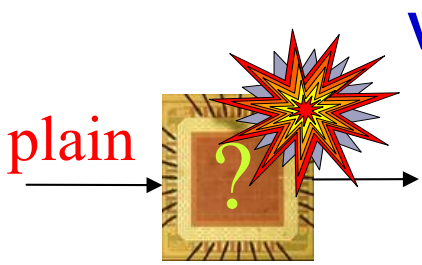
Fault attacks



Fault injections methods

Fault injection

Data Retrieval



Vcc, clk, T, flash, laser
X, UV, etc…

Corrupted execution

Diffential Fault Analysis (DFA)

Safe-Error Attacks (SEA)

Conditional branch

Round Reduction (RR)

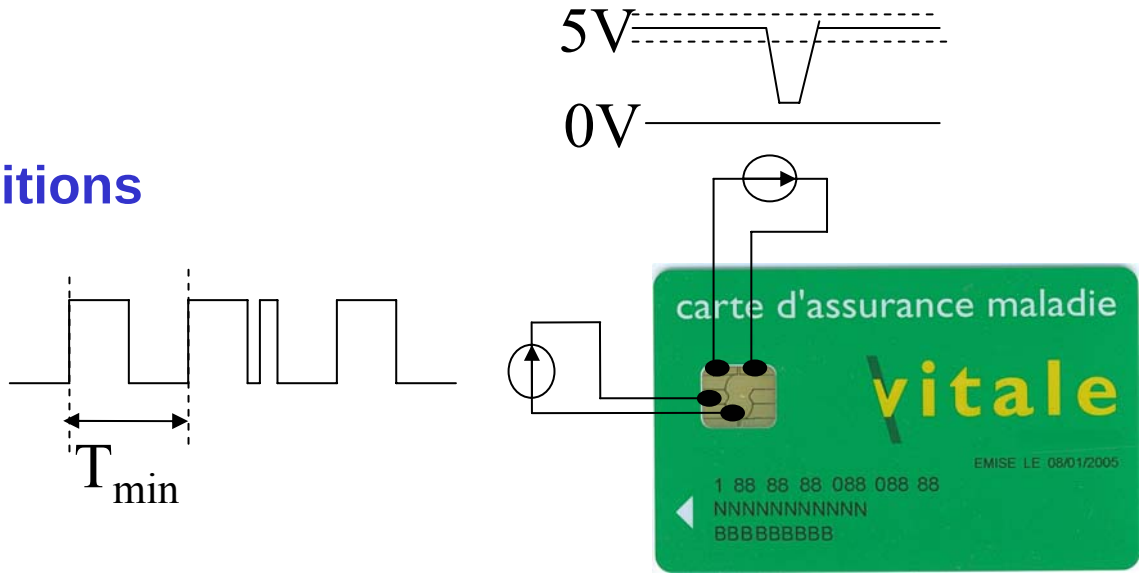
Fault injection methods

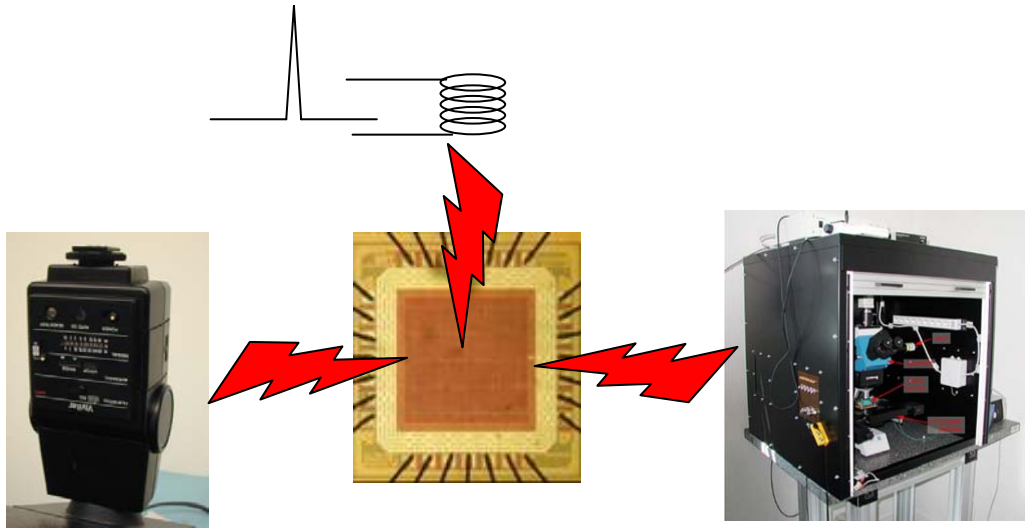
Standart ISO 7816

Normal environment conditions

Perturbations

- Power
- Clock
- Temperature
- Light
- EM pulse
- Laser IR, UV, green, etc…
- X-Ray
- …

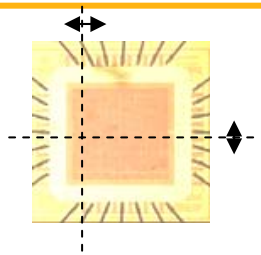




Source : [Skorobogatov02]

Source : LETI

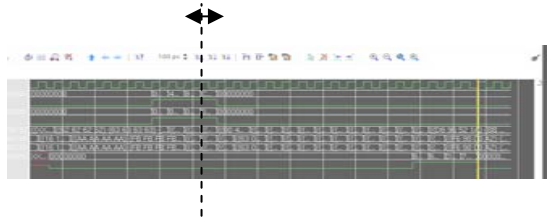
Towards…



Location control (x,y,z)

+

Timing control

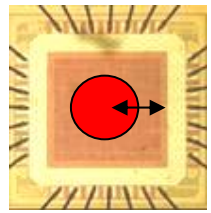


+

Fault type control (stuck at, bit flip, random, etc..)

+

Focalization control (number of faulty bits)



+

Reproductibility

+

Low cost

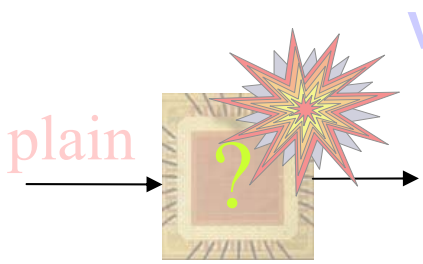
+

Easy to realize

=

Ideal but (not existing?) injection method

Data retrieval methods



Vcc, clk, T, flash, laser
X, UV, etc…

Faults

Fault model

Fault model

Fault model

Data Retrieval

Corrupted execution

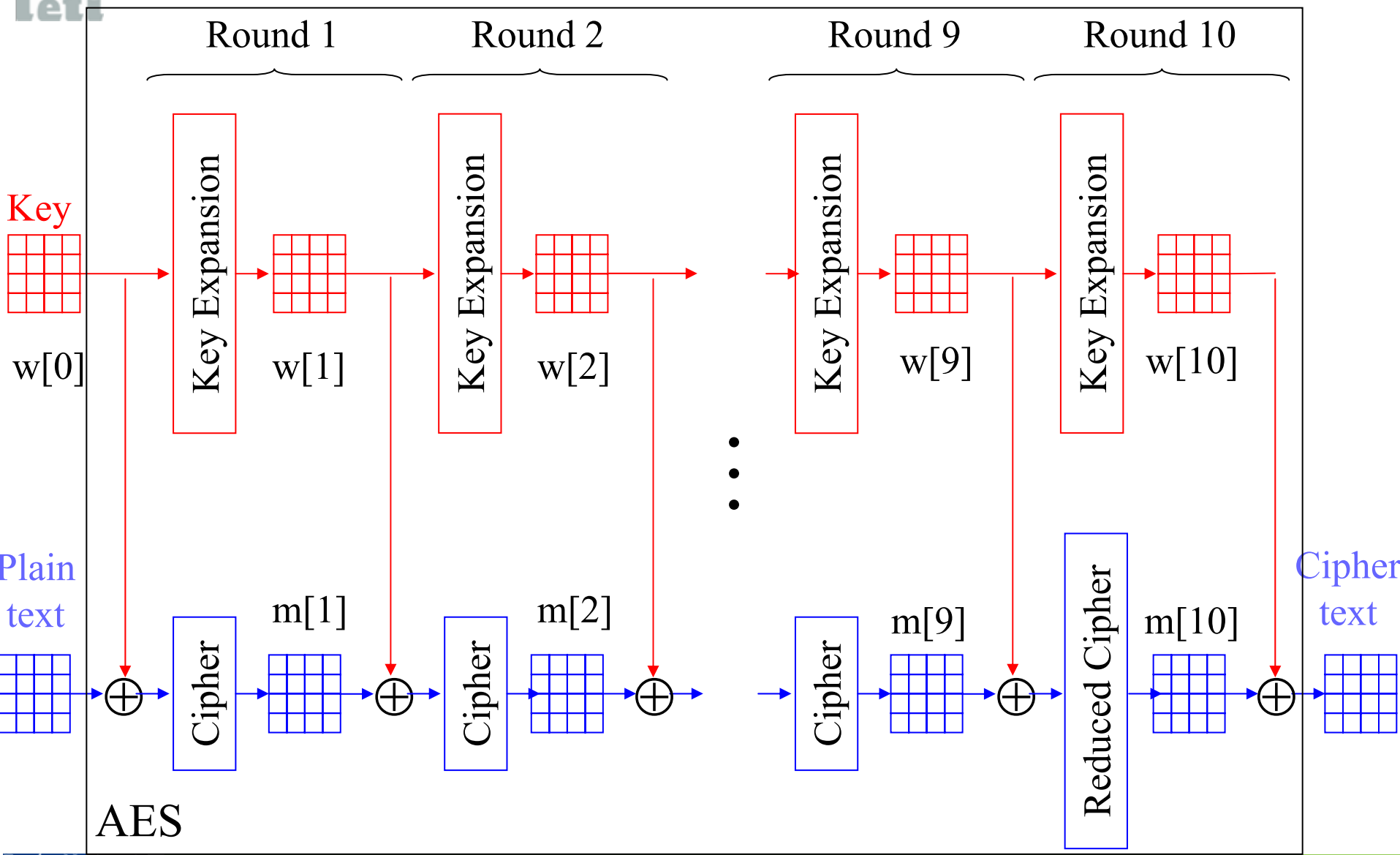
Differential Fault Analysis (DFA)

Safe-Error Attacks (SEA)

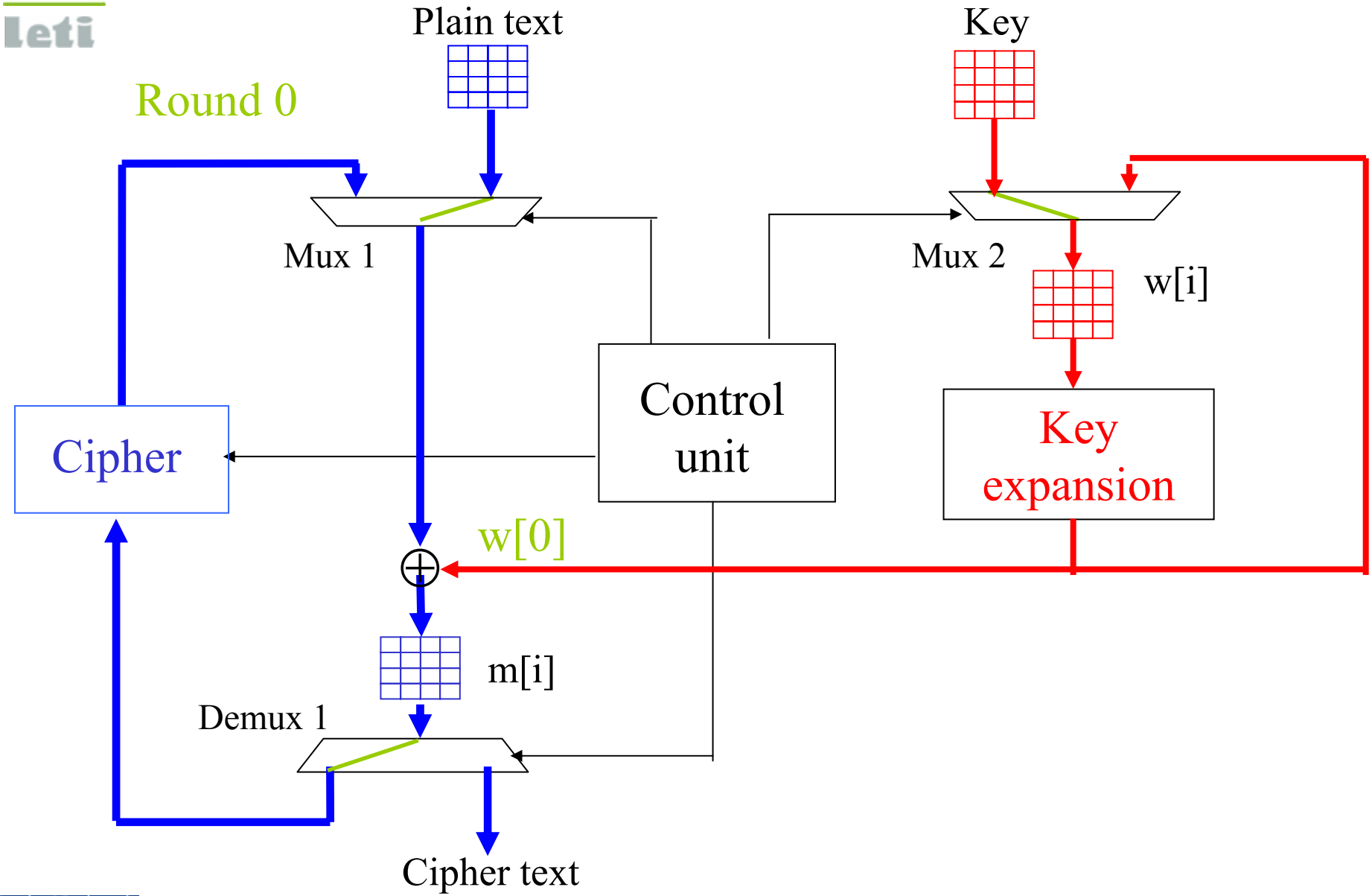
Conditional branch

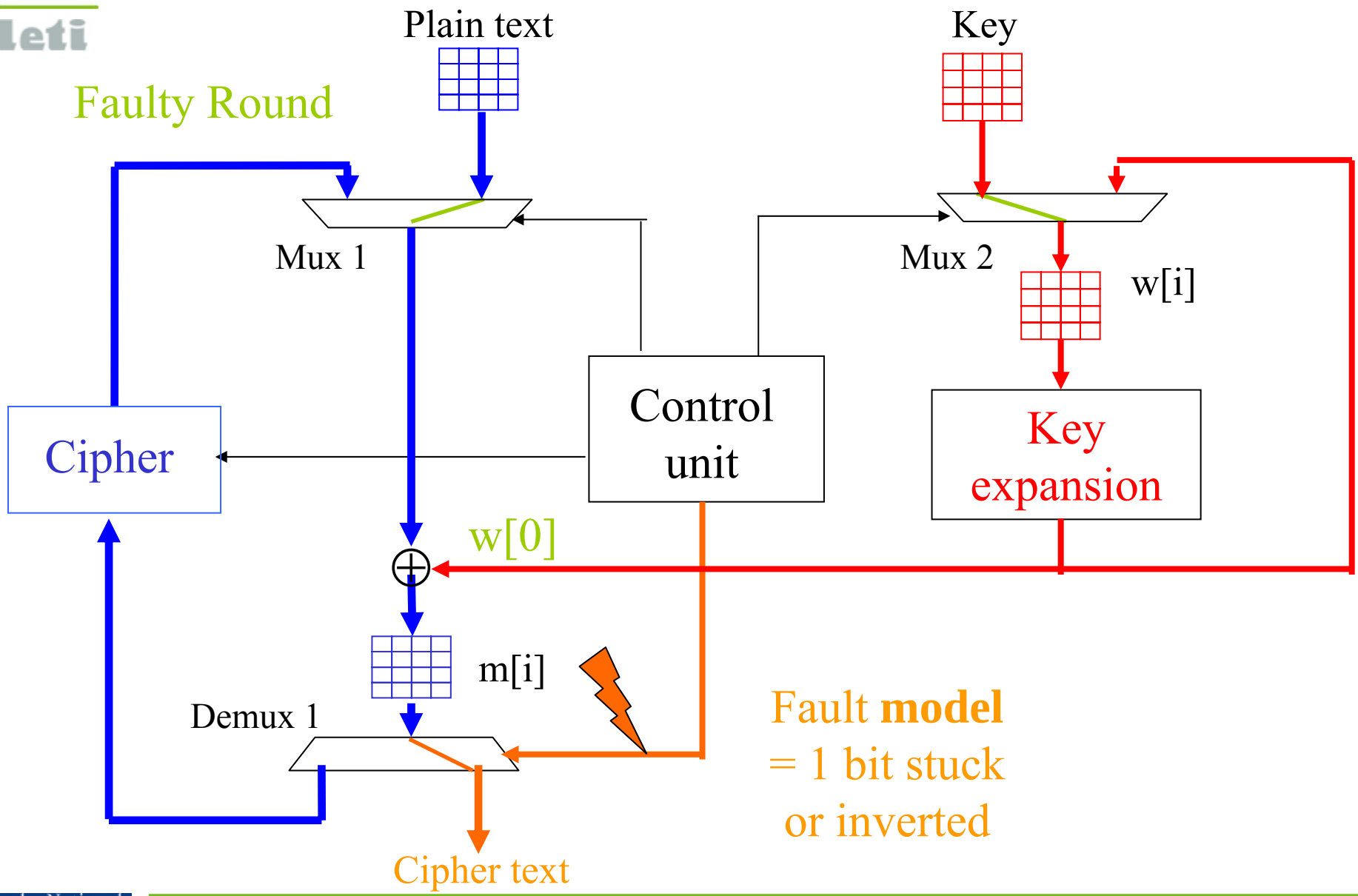
Round Reduction (RR)

AES-128

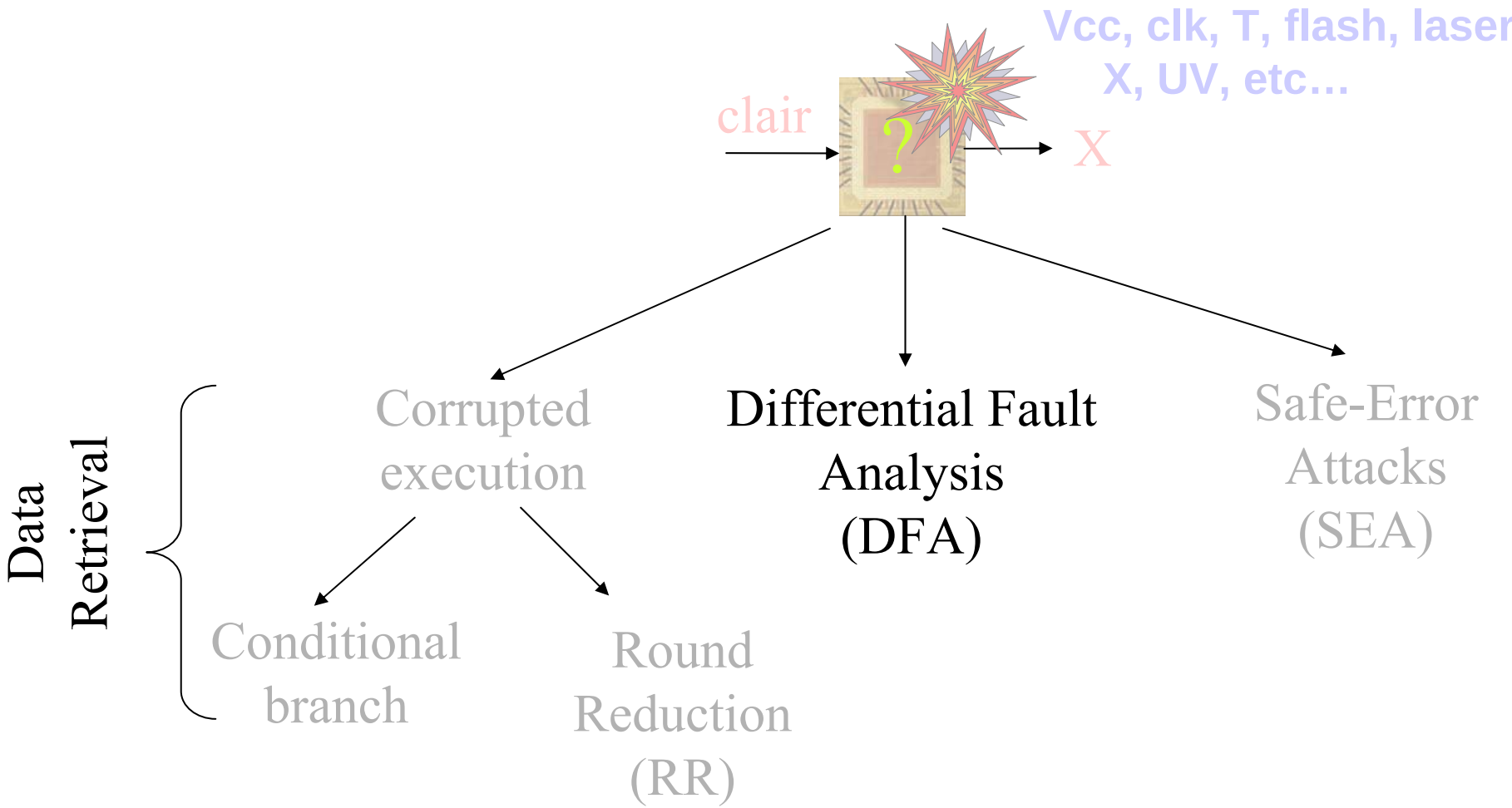

Round 1
Round 2
Round 9
Round 10
Key
Key Expansion
Key Expansion
Key Expansion
Key Expansion
w[0]
w[1]
w[2]
w[9]
w[10]
Plain text
Cipher text
m[1]
m[2]
m[9]
m[10]
Cipher
Cipher
Cipher
Reduced Cipher
AES

AES-128

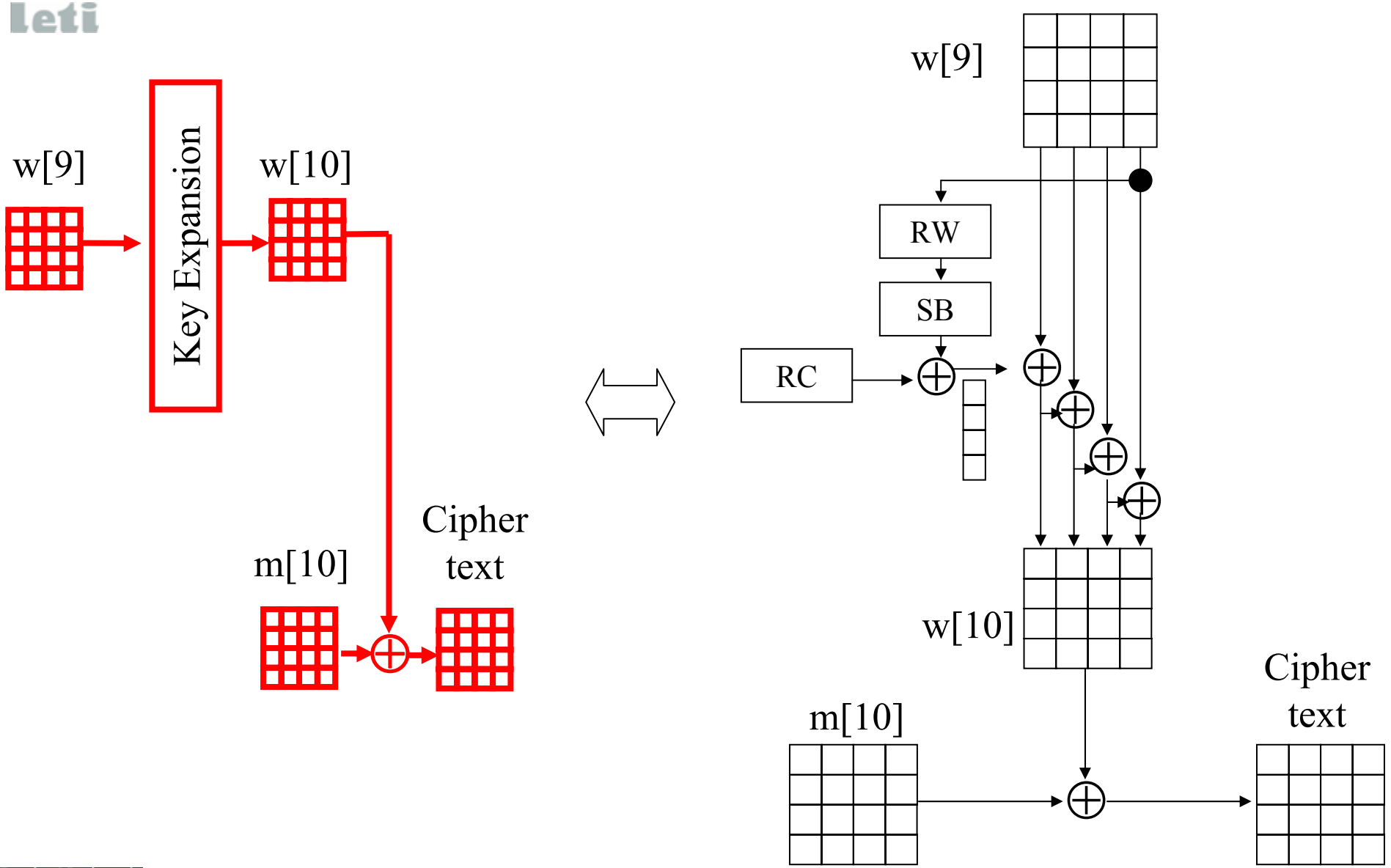

Plain text
Key
Round 0
Mux 1
Mux 2
w[i]
Control unit
Cipher
Key expansion
w[0]
m[i]
Demux 1
Cipher text


Plain text
Key
Faulty Round
Mux 1
Mux 2
w[i]
Control unit
Cipher
Key expansion
w[0]
m[i]
Demux 1
Fault **model**
= 1 bit stuck
or inverted
Cipher text

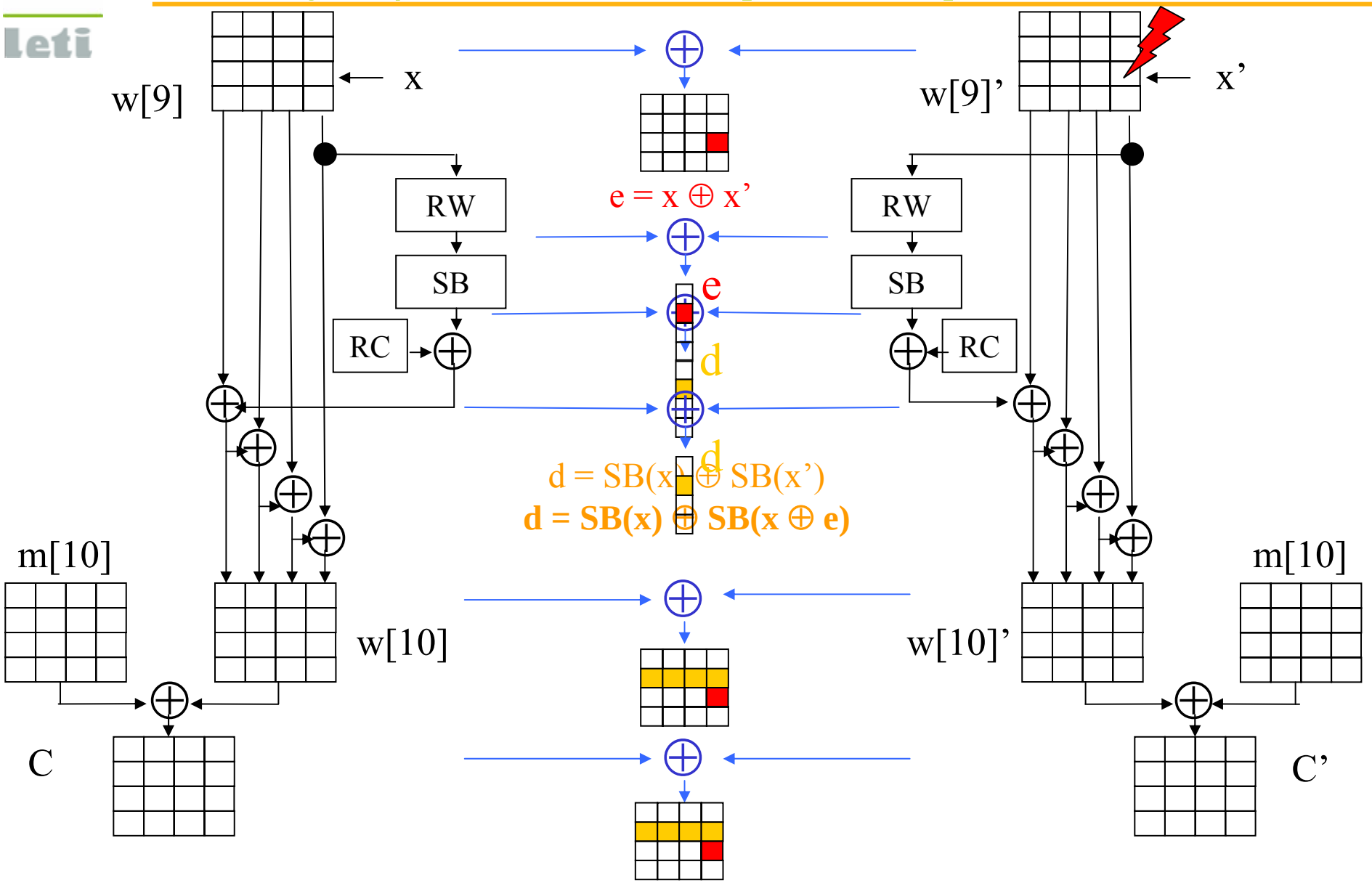
Differential fault analysis



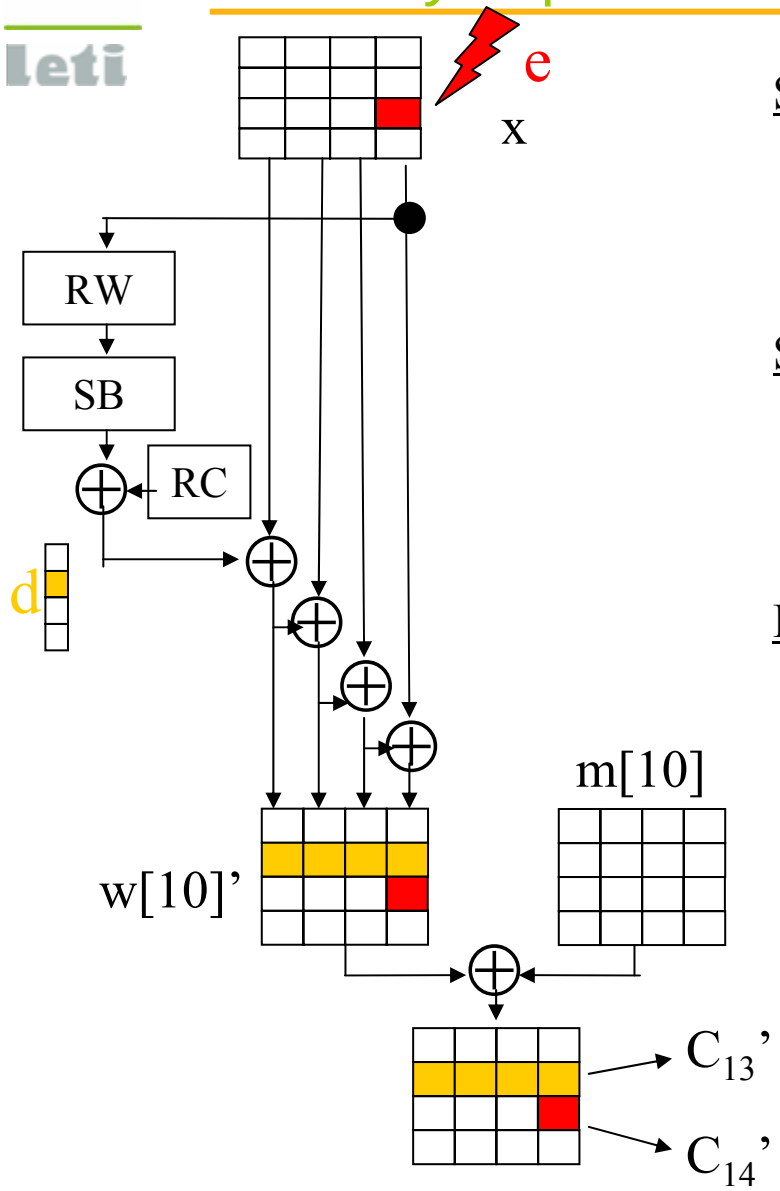
AES-128


w[9]
Key Expansion
w[10]
m[10]
Cipher text
w[9]
RW
SB
RC
w[10]
m[10]
Cipher text

DFA key expansion round 9 [Giraud03]



DFA key expansion round 9



Step 0 : Random fault injection on $w_{14}[9]$,

$e = x \oplus x'$ (def)

$d = SB(x) \oplus SB(x \oplus \mathbf{e})$ **(AES)**

Step 1 : Fault computing

$e = C_{14}' \oplus C_{14}$

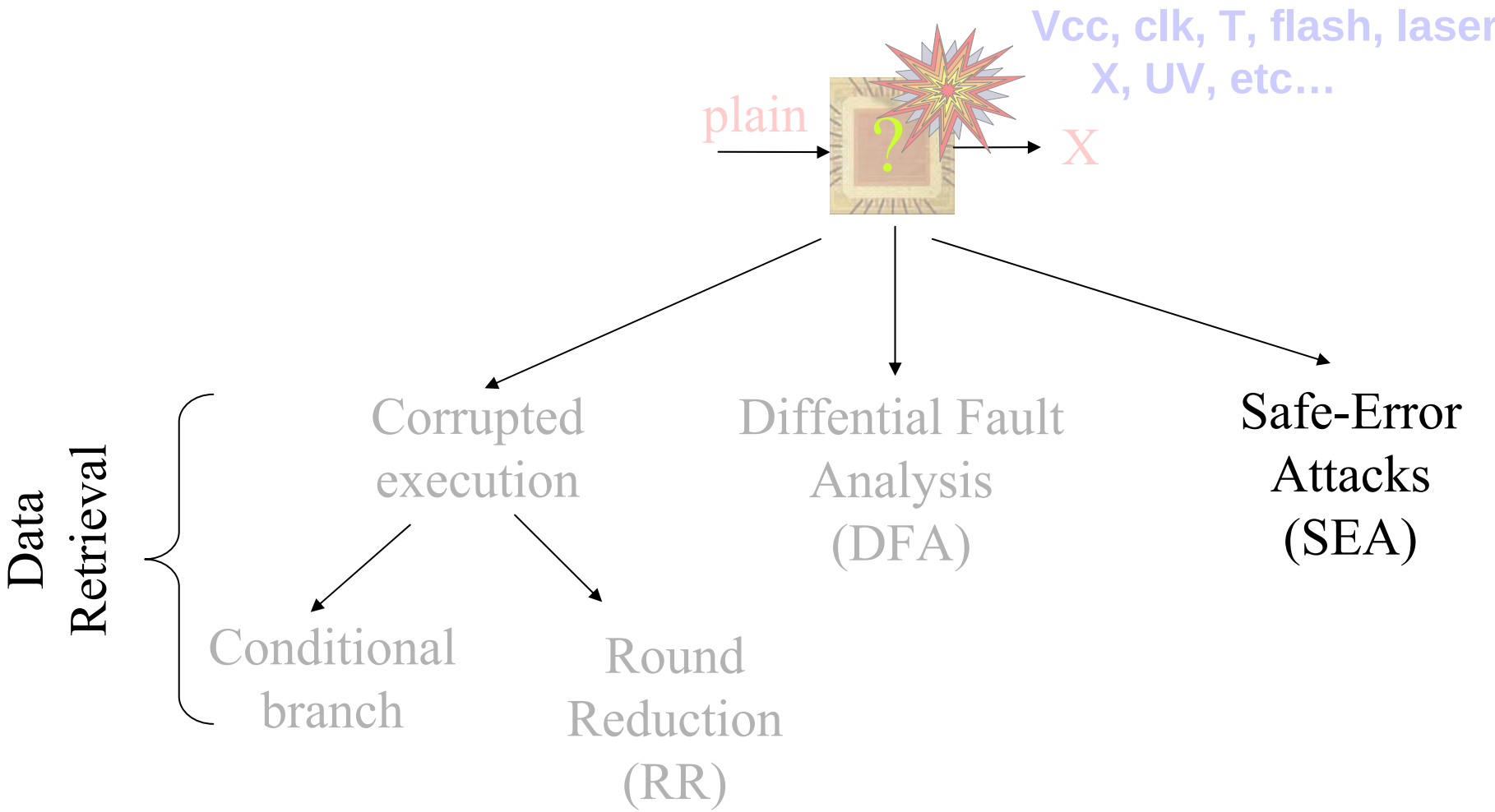
$d = C_{13}' \oplus C_{13}$

Etape 3 : Exhaustive search (2^8=256 tries) for x

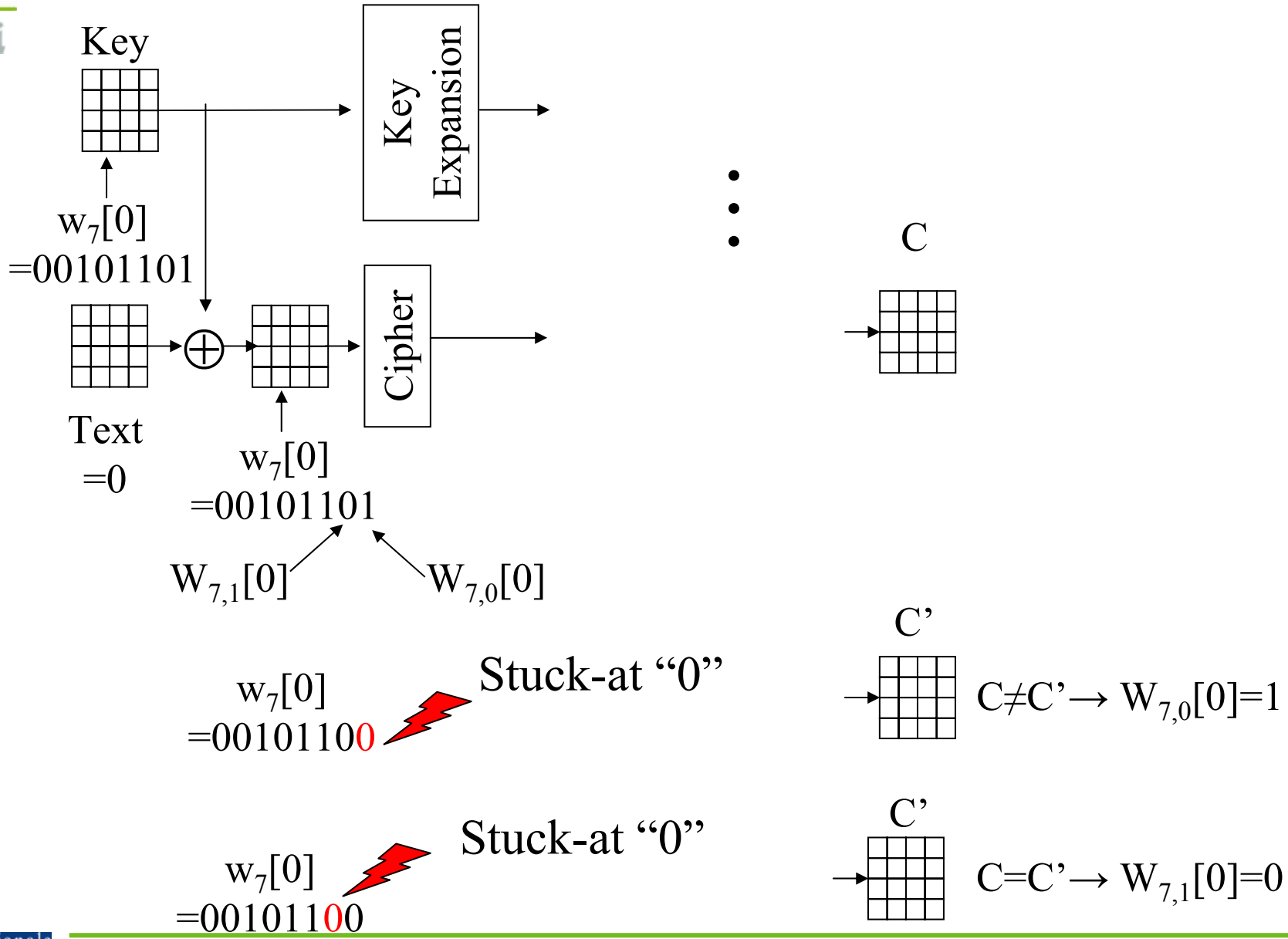
$In = \{x \mid SB(x) \oplus SB(x \oplus e) = d\}$

Rq: $card(In) = \{0;2;4\}$

Safe error attacks



Safe error AES-128 [Blömer03]



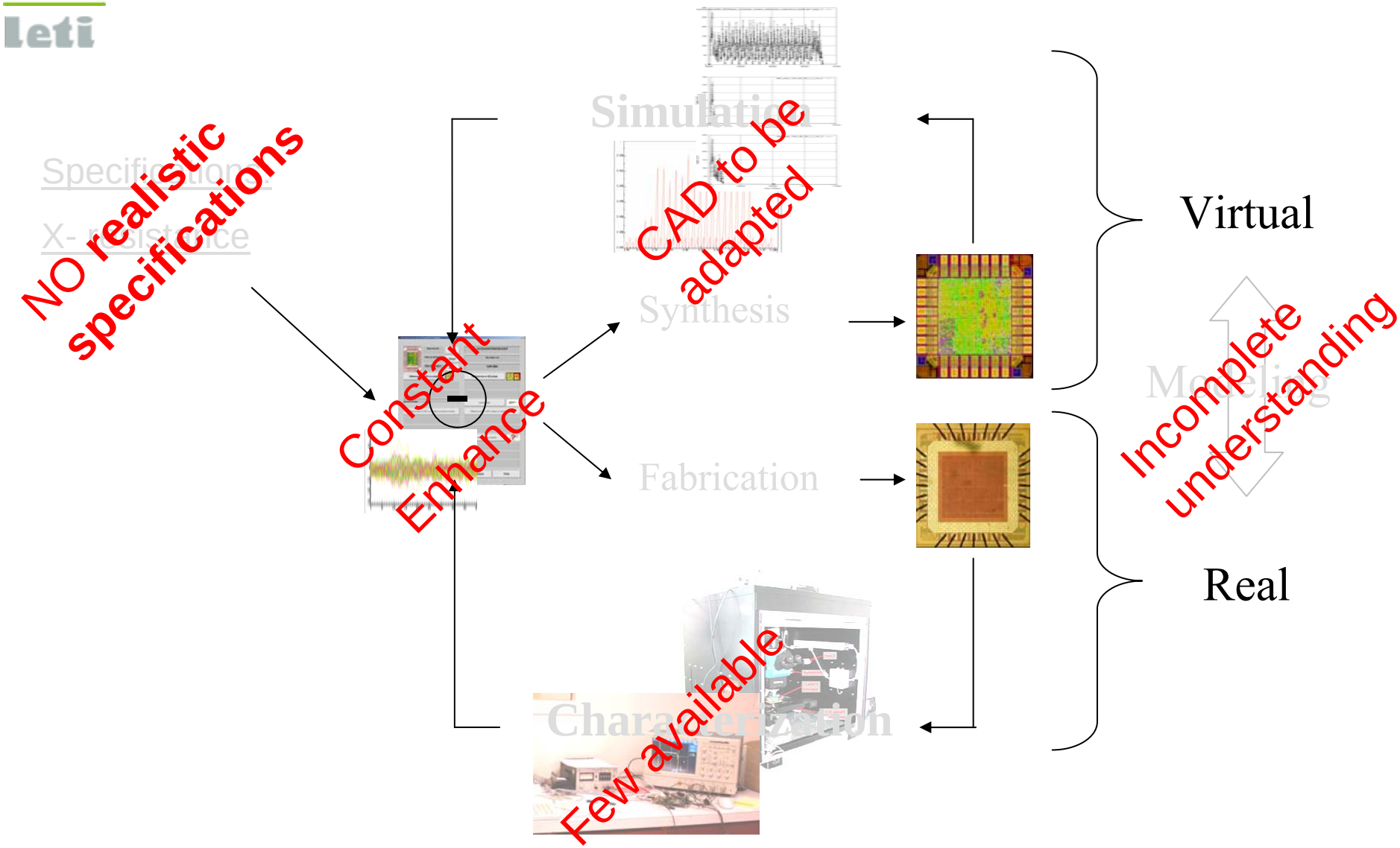
State of the art data retrieval (AES)

Ref	Type	Location	Fault	Focalization	Number of distinct faults	Number of faulty realization
[Giraud03]	DFA	Data (16*start[9])	Inversion	Bit	16	approx. 50
[Giraud03]	DFA	Key (4*w[9] et 4*w[8]) Data (4*m[8])	Random	Byte	12	250 (for 14 bytes)
[Chen03]	DFA	Key (4*w[9]) Data 7*w[8]	Random	Byte	11	32 (for 13 bytes)
[Piret03]	DFA	Data (4*(anywhere between the 2 last mixcolumns) ou 1*m[8])	Random	Byte	4 ou 1	+8 ou +2
[Dusart03]	DFA	Data (4*(anywhere between the 2 last mixcolumns))	Random	Byte	4	+8
[Blomer02]	SEA	Data (start[0])	Stuck-at	Byte	128	128
[Rob07]	SEA	Data (entre sbox[0] et start[1])	Stuck-at	Bit	16	approx. 256
[Rob07]	SEA	Data (sbox[0])	Stuck-at	Bit to Byte	16	approx. 256 to 4096
[Choukri05]	RR	Round counter	Depending	Depending	1	3
[Monnet06]	RR	Round counter	bit-flip	1 or 2 bits	depends	depends

State of the art conter-measures

		Focalization	Location	Timing	Faults	DFA	SEA	RR
Masking / filtering	**Metal shield**	x	x					
	Optical layer	x	x					
	Hardware obfuscation		x					
	Internal clock + jitter			x				
	Random data instruction			x				
	Software obfuscation		x	x				
	Low band power filter				x			
	Quasi delay insensitive logic				x			
	Masking						x	
Detection / Reaction	**Voltage, light, frequency, temperature sensors**					x	x	
	Error detecting codes					x		x
	Temporal and spatial duplication					x		x
	id=f(inverse f)					x		
	Linear and non linear predictor					x		
	Error spreading					x		
	Communication stop					x		
	Reset					x		
	Memory delete					x	x	x
Correction	**Temporal or spatial triplication**					x	x	x

One challenge



Conclusions

- Circuits for security applications are subject of physical attacks
- Fault injection methods may be very efficient but in practice require high level skills and state of the art (costly) equipments
- Data retrieval methods are particularly efficient (the most efficient one recovers the entire key with only a couple of faulty/correct cipher-texts and rather reduced computing power)
- Gap between fault injection and data retrieval methods?
- Without doupt, take into account fault attacks during the design of circuits for security applications

Thank for your attention

This work has been realized in the frame of the CIMPACA/Micro-PackS BTRS Project cofunded by the “Fonds Social Européen” (FSE) and the “Direction Générale des Entreprises” (DGE).

Conclusion

[AES97] Federal Information Processing Standards. Advanced Encryption Standard (AES). FIPS publication 197.
[Blomer03] J. Blomer and J.-P. Seifert. Fault Based Cryptanalysis of the Advanced Encryption Standard (AES). In Rebecca N. Wright, editor, *Financial Cryptograhy, 7th International Conference, FC 2003, Guadeloupe, January 27-30, 2003*, Lecture Notes in Computer Science, pages 162-181. Springer-Verlag, 2003.
[Chen03] C.-N. Chen and S.-M. Yen. Differential Fault Analysis on AES Key Schedule and Some Countermeasures. In R. Safavi-Naini and J. Seberry, editors, *Information Security and Privacy, 8th Australasian Conference, ACISP 2003, Wollongong, Australia, July 9-11, 2003*, volume 2727 of *Lecture Notes in Computer Science*, pages 118-129. Springer-Verlag, 2003.
[Choukri05] Round Reduction Using Faults Hamid Choukri and Michael Tunstall, In L. Breveglieri and I. Koren, Eds., Workshop on Fault Diagnosis and Tolerance in Cryptography 2005 – FDTC 2005, pp. 13–24, 2005.
[Dusart03] P. Dusart, G. Letourneux, and O. Vivolo. Differential Fault Analysis on A.E.S.In J. Zhou, M. Yung, and Y. Han, editors, *Applied Cryptography and Network Security, First International Conference, ACNS 2003. Kunming, China, October 16-19, 2003*, volume 2846 of *Lecture Notes in Computer Science*, pages 293-306. Springer-Verlag, 2003.
[Giraud03] C. Giraud. DFA on AES. Technical Report 2003/008, IACR eprint archive, 2003. Available at http://eprint.iacr.org/2003/008.ps.
[**Monnet06]** Yannick Monnet, Marc Renaudin, Regis Leveugle, Christophe Clavier, Pascal Moitrel, *Case study of a fault attack on asynchronous DES crypto-processors***,** Workshop on Fault Diagnosis and Tolerance in Cryptography 2006 – FDTC 2006
[Piret03] G. Piret and J. J. Quisquater. A differential fault attack technique against SPN structures, with application to the AES and Khazad. Cryptographic Hardware and Embedded Systems Workshop (CHES-2003), pages 77-88, 2003. Lecture Notes in Computer Science No. 2779.
[Rob07] B. Robisson, P. Manet, Differential Behavioral Analysis, Accepted paper to CHES 2007.
[Skorobogatov02] S. Skorobogatov and R. Anderson. Optical fault induction attacks. Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), pages 2-12, 2002. Lecture Notes in Computer Science No. 2523.