



Soutenance de thèse



Étude de la vulnérabilité des circuits cryptographiques à l'injection de fautes par laser

Amir-Pasha Mirbaha

Mardi 20 décembre 2011, CMP Gardanne

Sommaire

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



- Introduction
- Objectifs et contexte
 - Validation pratique des modèles de faute (extrapolation)
 - Analyse différentielle de fautes (DFA)
 - Attaques par modification du nombre de rondes
- Conclusion
- Perspectives et contributions

Introduction

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

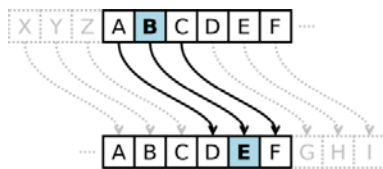


Cryptographie :

Étude et pratique des méthodes d'écriture secrète des messages

But : rendre illisible le message à toute personne n'étant pas le destinataire souhaité

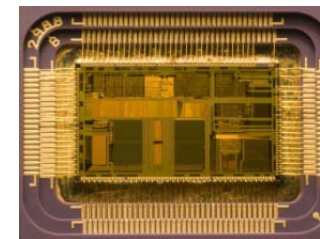
3 périodes historiques :



artisanal



technique



paradoxe

Principe de Kerckhoffs

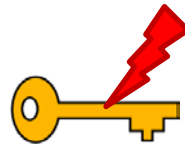
INSPIRING INNOVATION | INNOVANTE PAR TRADITION



Algorithme public, la sécurité repose sur la confidentialité du secret.

Secret : 

Comment trouver le secret ?



Comment attaquer la clef ?

Rechercher des vulnérabilités

Vulnérabilités des circuits cryptographiques

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

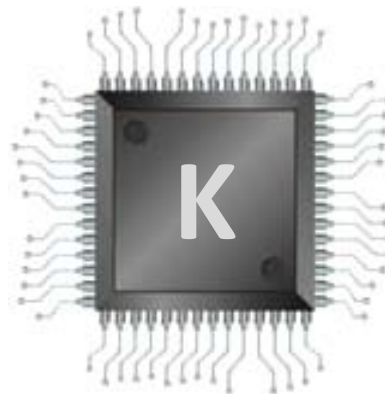


- Attaques cryptanalytiques:
 - Recherche exhaustive et attaques mathématiques
- Attaques matérielles :
 - Attaques par canaux cachés : par observation des paramètres physiques

Analyse de la consommation

Temps du calcul

(Dissipation de la chaleur)



Analyse du champ électromagnétique

...

(Émission de photons)

- Attaques invasives : Ouverture et modification du composant
- Attaques en fautes : Perturbation du circuit ou modification de la clef

Attaques en fautes

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



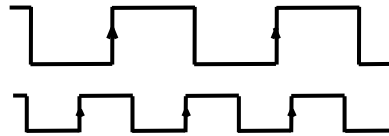
- Méthodes :
 - Modification de l'algorithme : passer en mode test, affaiblir l'algorithme (RR), etc.
 - Safe Error
 - Analyse différentielle de fautes (DFA)
 - Modèles de faute : mono-octet, mono-bit, instant d'injection, etc.
- Mise en œuvre pratique :
 - Perturbation du circuit
 - Fautes respectant les modèles

Perturbation de circuits

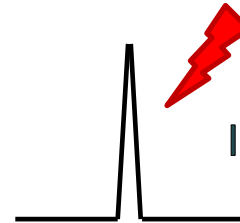
INSPIRING INNOVATION | INNOVANTE PAR TRADITION



Modification
de l'horloge



Impulsion EM



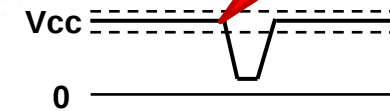
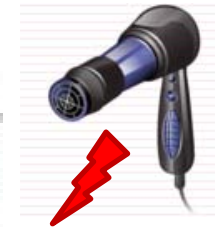
Émission de
lumière



Émission
de laser



Variation
de la
température

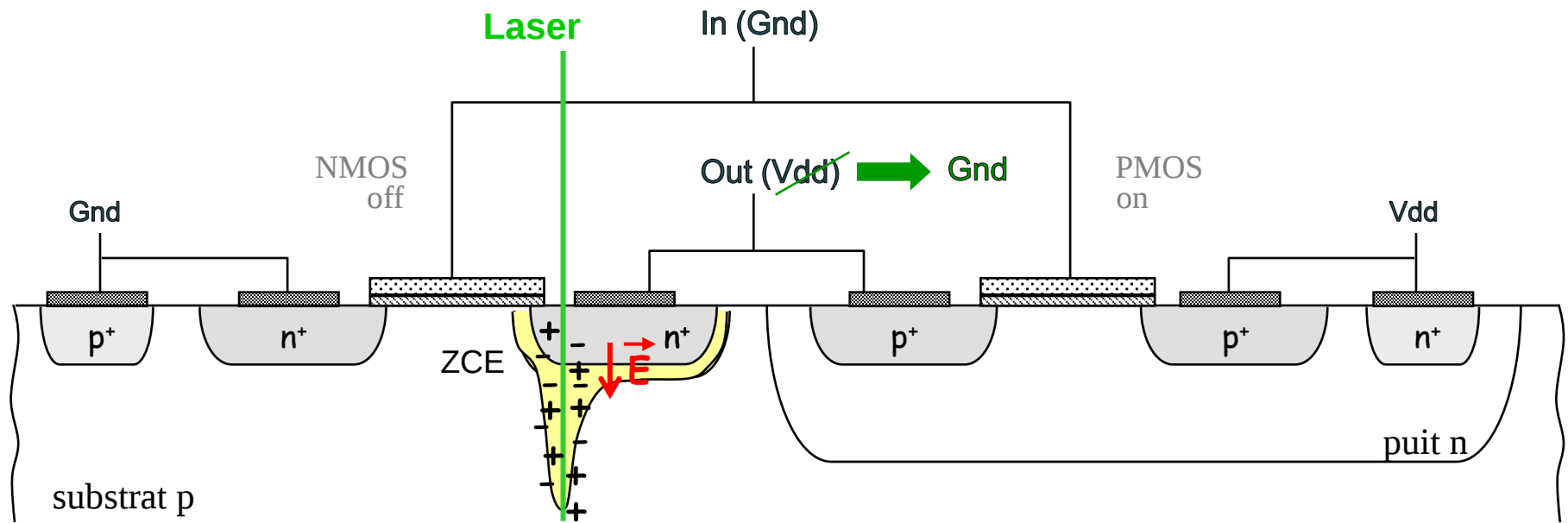


Pic de tension

Bonne précision spatiale et temporelle
pour injection de fautes

Attaque en faute par laser - effet photoélectrique

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



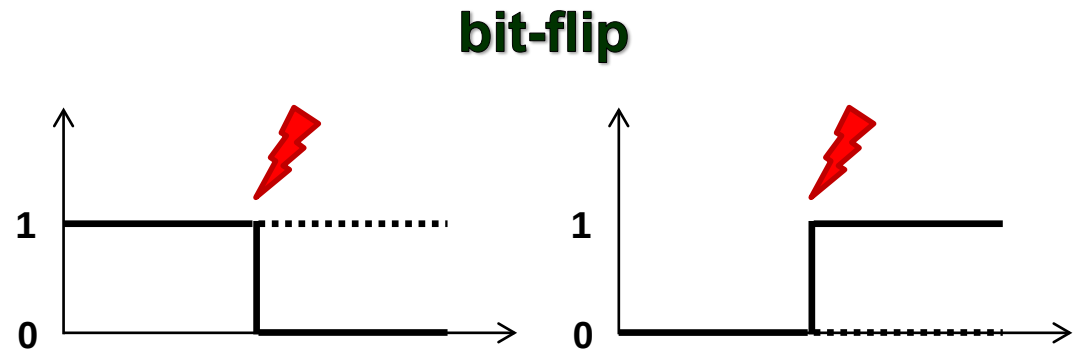
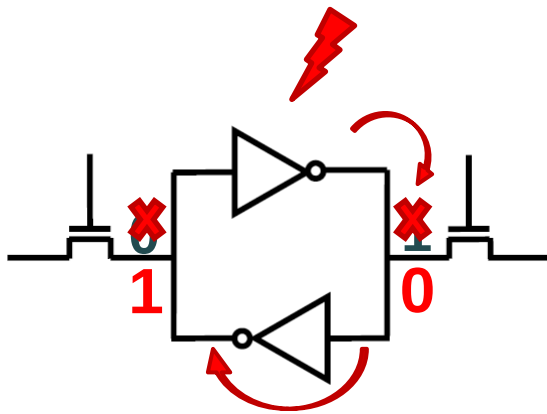
⇒ transitoire de courant au niveau de la jonction

⇒ transitoire de tension en sortie de l'inverseur

effet du transitoire ⇒ bit-flip ⇒ injection de faute

Attaque en faute par laser - effet photoélectrique sur SRAM

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

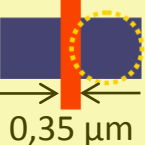
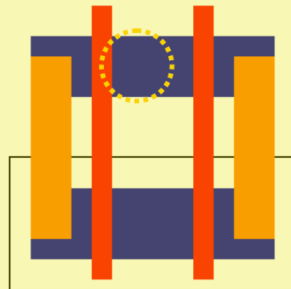
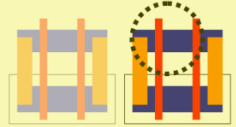
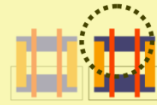
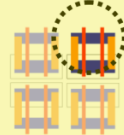


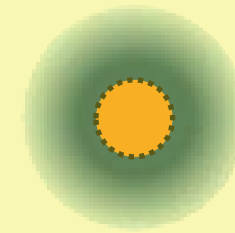
effet du transitoire $\Rightarrow$ bit-flip $\Rightarrow$ injection de faute

Effet de l'évolution technologique sur la précision

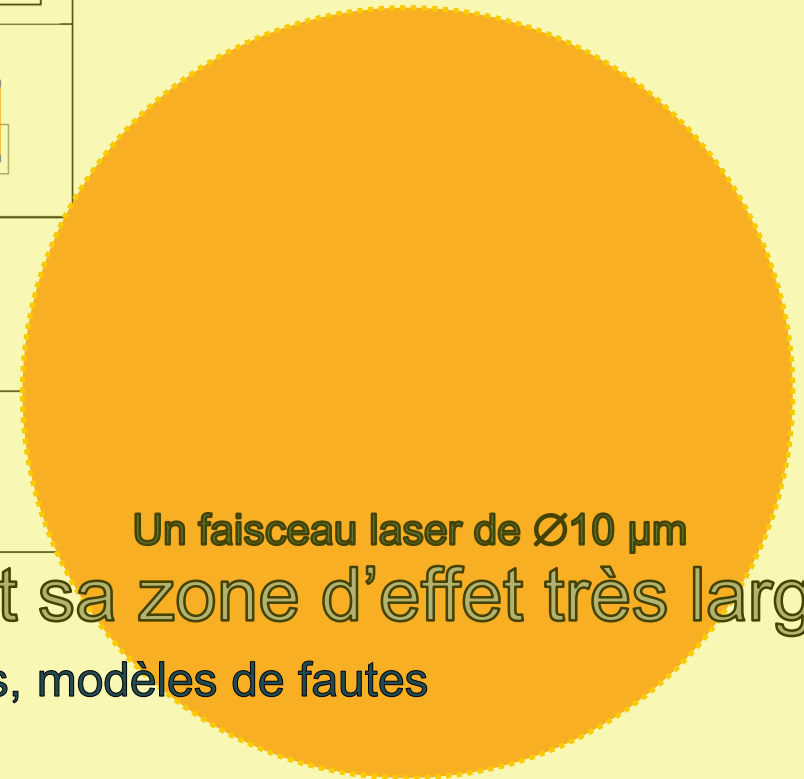
INSPIRING INNOVATION | INNOVANTE PAR TRADITION



	Transistor	SRAM Cell
0,35 μm		
0,13 μm		
90 nm		
65 nm		



Un faisceau laser de $\varnothing 1\mu\text{m}$
et sa zone d'effet



Un faisceau laser de $\varnothing 10\mu\text{m}$
et sa zone d'effet très large

Est-ce qu'avec des évolutions technologiques, modèles de fautes mono-octet ou mono-bit resteront réalistes ?



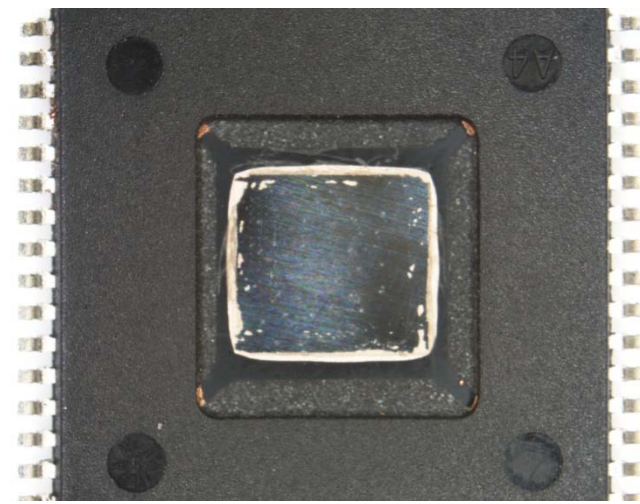
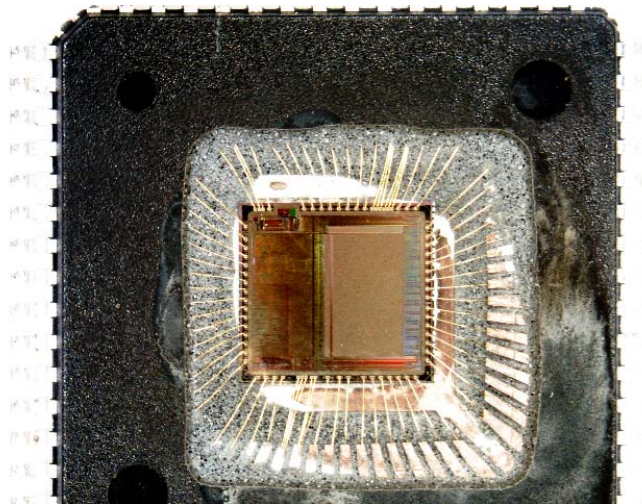
Identification des menaces

- Validation des modèles de fautes théoriques par laser
Cadre : 2 attaques classiques sur AES
Piret & Quisquater (mono-octet) et Giraud (mono-bit)
- Extrapolation aux technologies avancées
Est-ce qu'avec la diminution de la taille de fabrication, des modèles de fautes mono-octet ou mono-bit resteront réalistes ?
- Contribution à l'état de l'art sur les attaques matérielles :
Nouvelle attaque en DFA
Évolution de la RMA



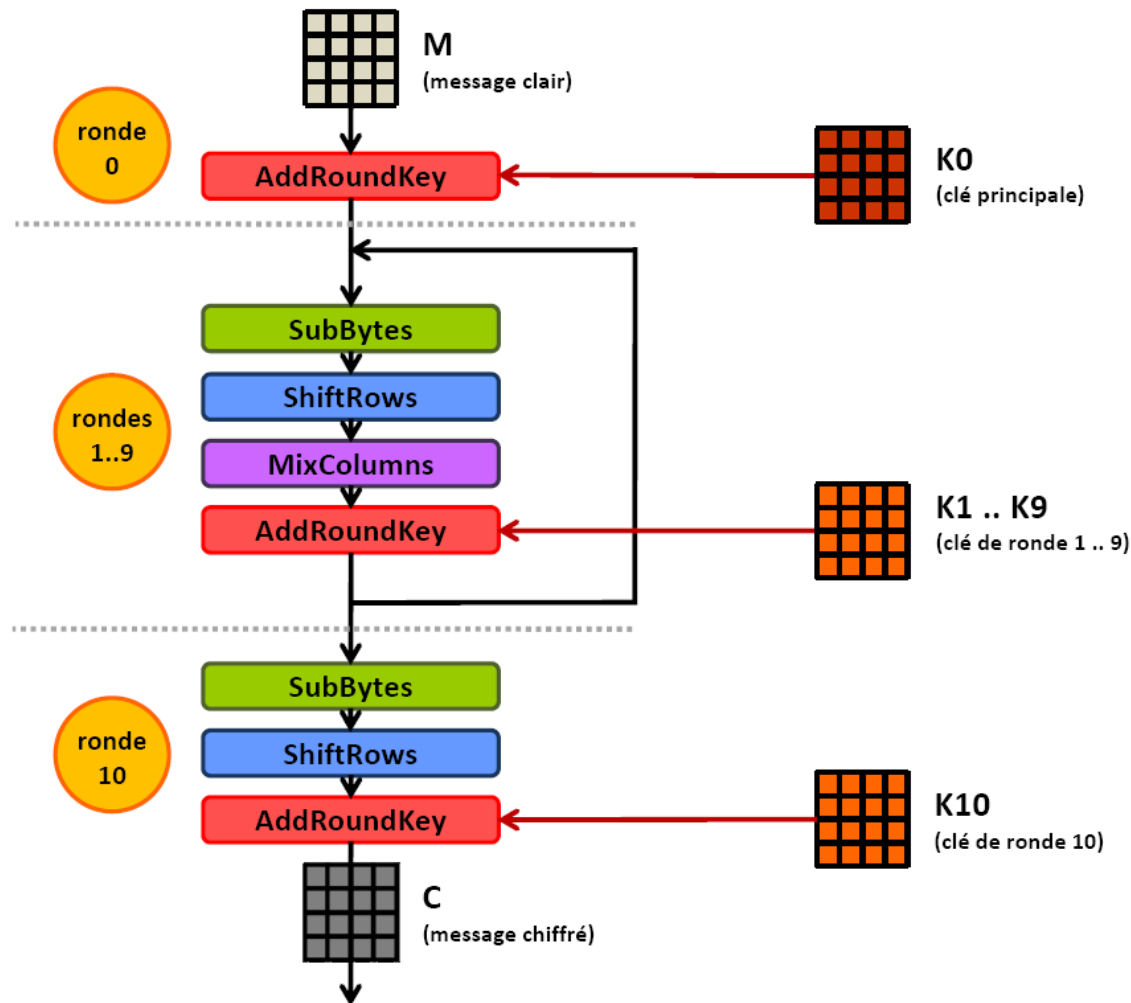
Interface ISO 7816-3 cartes à puce

- 8-bits 16 MHz 0.35 μm sans contremesure
- SOSSE (Simple Operating System for Smartcard Education) embarqué (open source)
- AES-128 bits logiciel



Advanced Encryption Standard

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

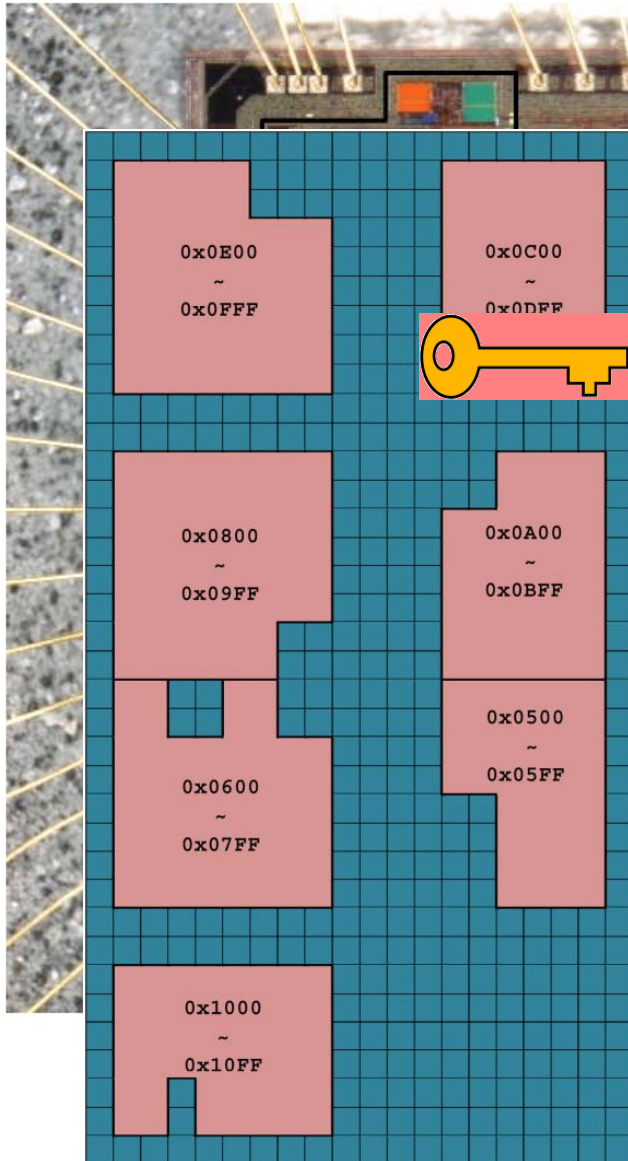


- un algorithme de cryptographie symétrique
- remplaçant de DES depuis 2001
- blocs de 16 octets en entrée et en sortie

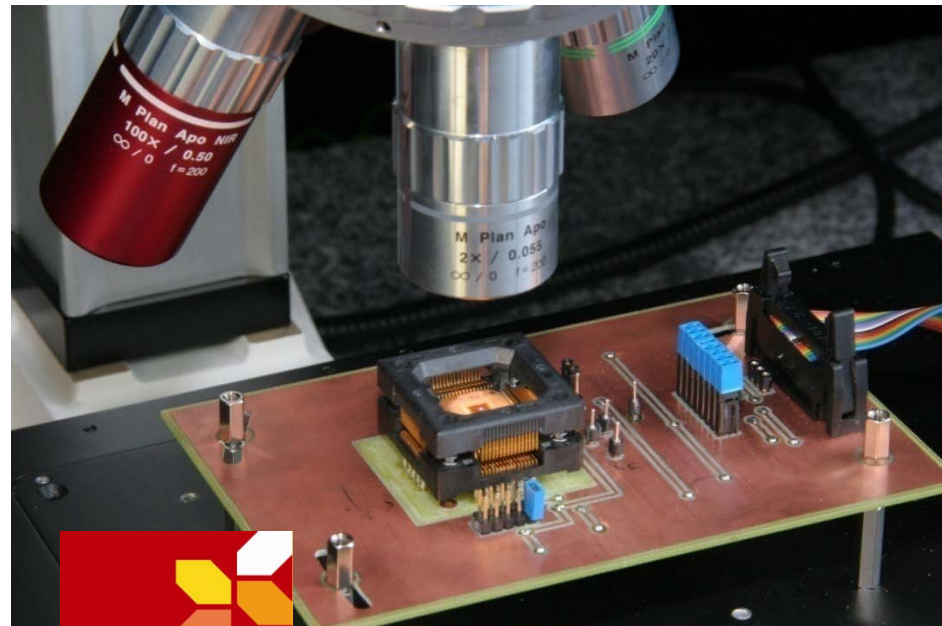
AES-128 bits : 10 rondes (après une ronde initiale) avec une clef principale de 128 bits

Cartographie du circuit

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

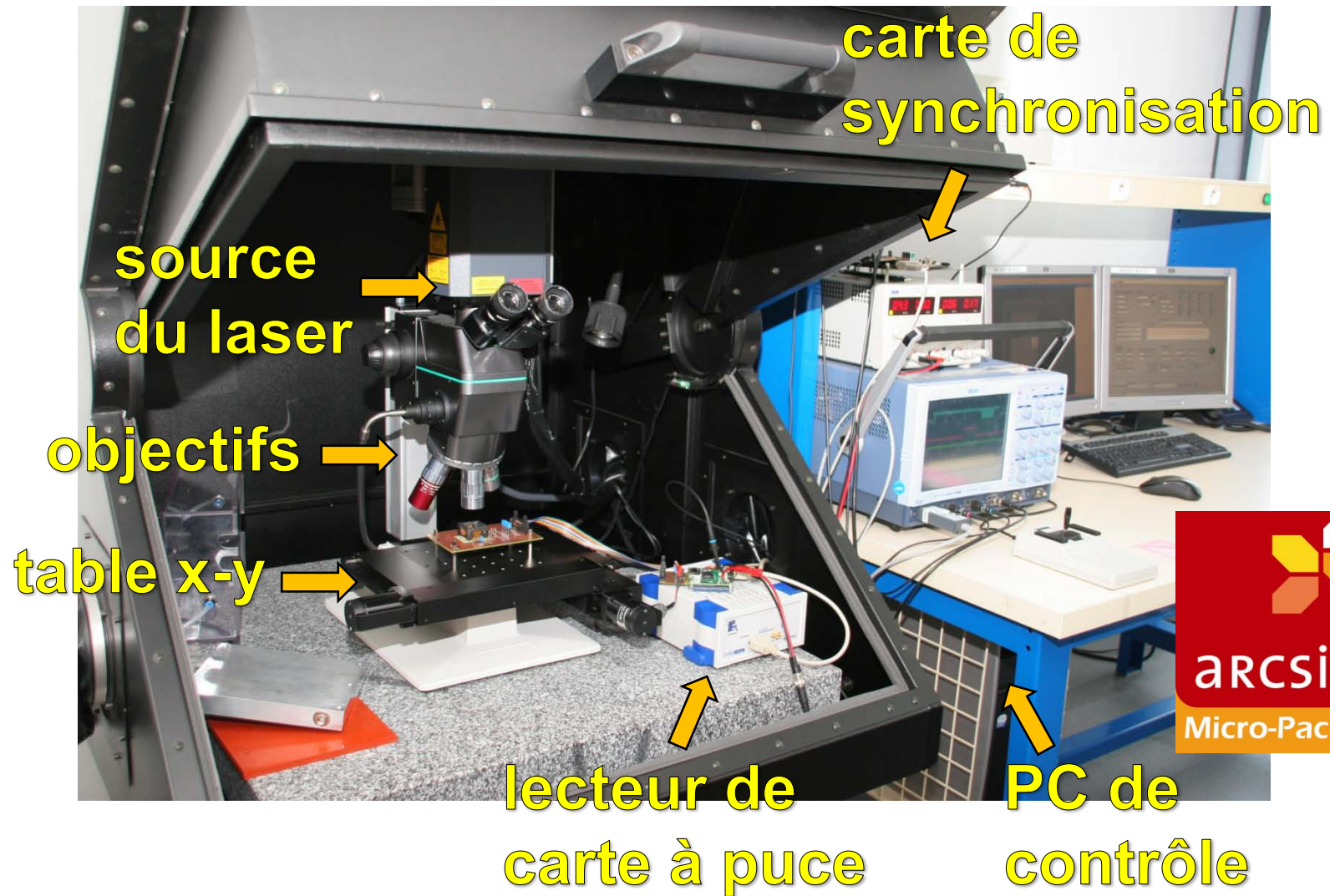


Comment injecter des fautes laser ?



Banc Laser MicroPackS

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



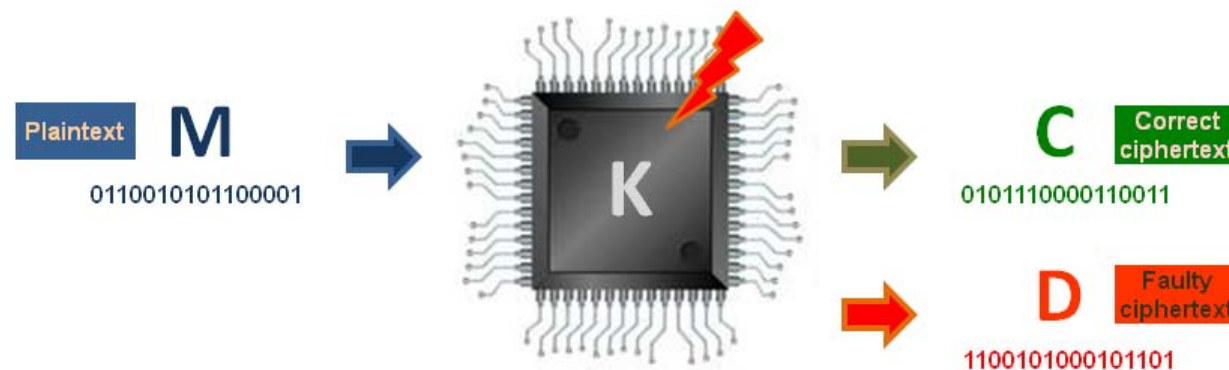
DFA sur AES

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



Principes d'une DFA :

- Injection de fautes lors des calculs cryptographiques



- Extraction d'information sur la clef par comparaison des chiffrés fautés et corrects
- Modèle de faute restreint : injection de fautes mono-octet ou mono-bit

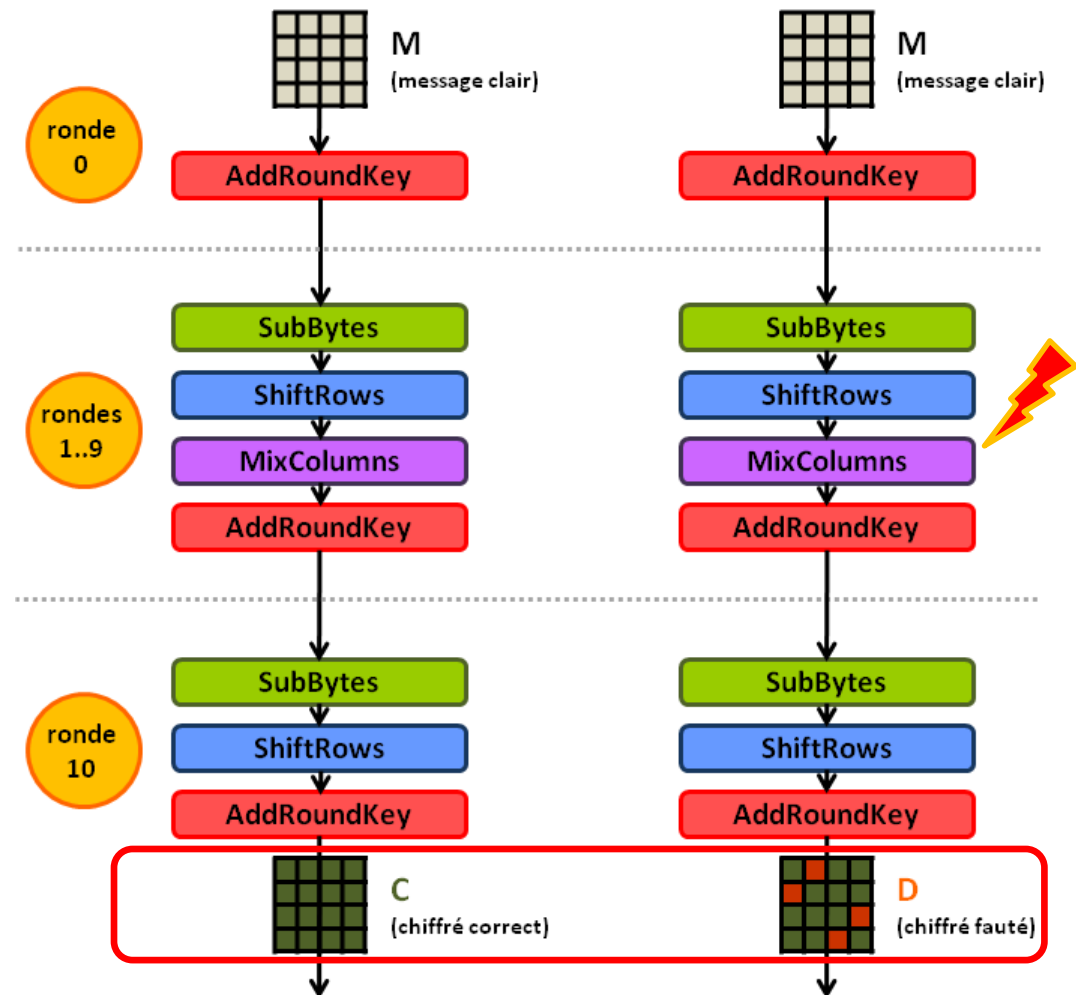
DFA mono-octet : Piret & Quisquater

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



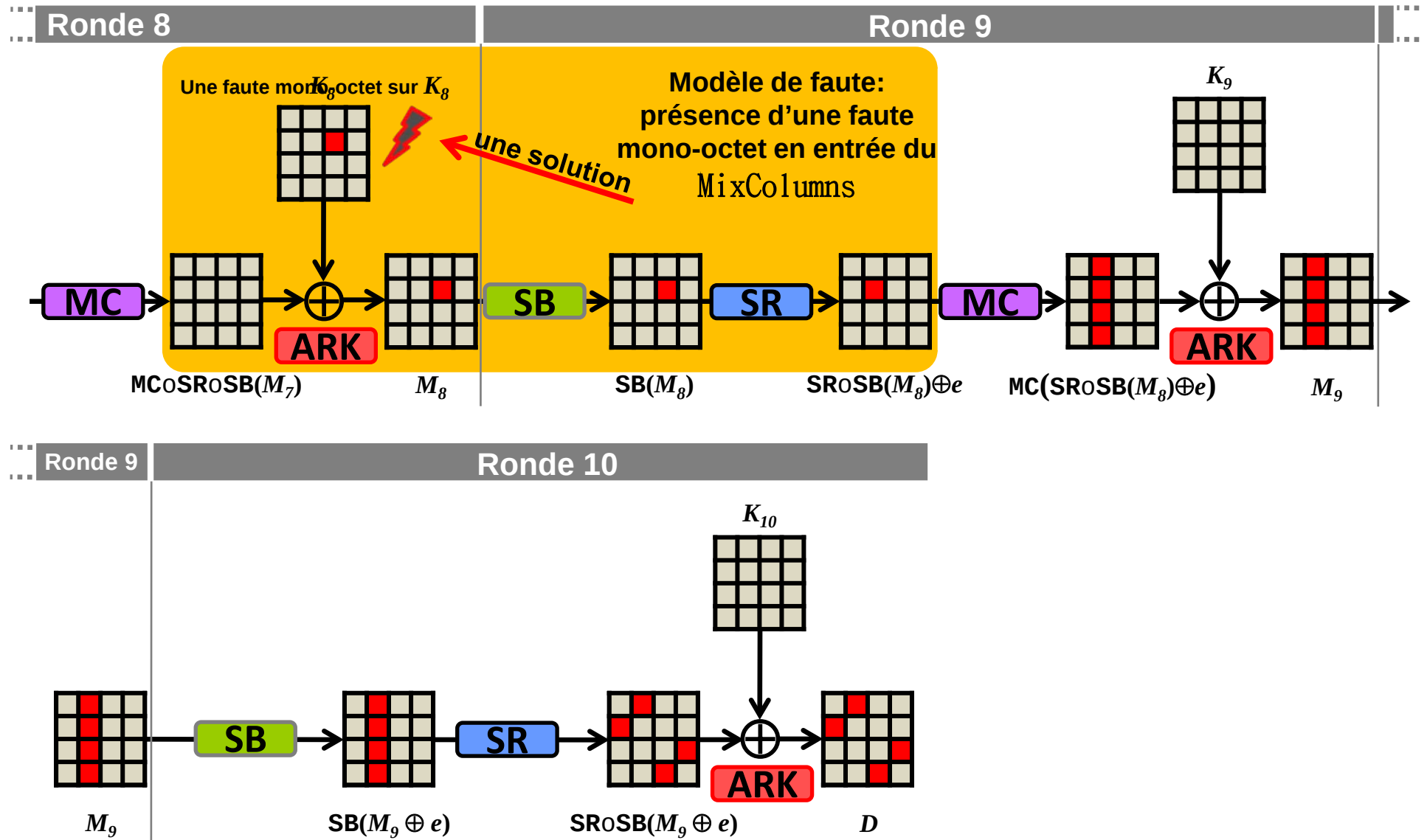
Attaque classique basée sur le modèle de faute mono-octet

Comparaison des chiffrés fautés et corrects correspondants pour en déduire une partie de la clef



DFA mono-octet : Piret & Quisquater

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

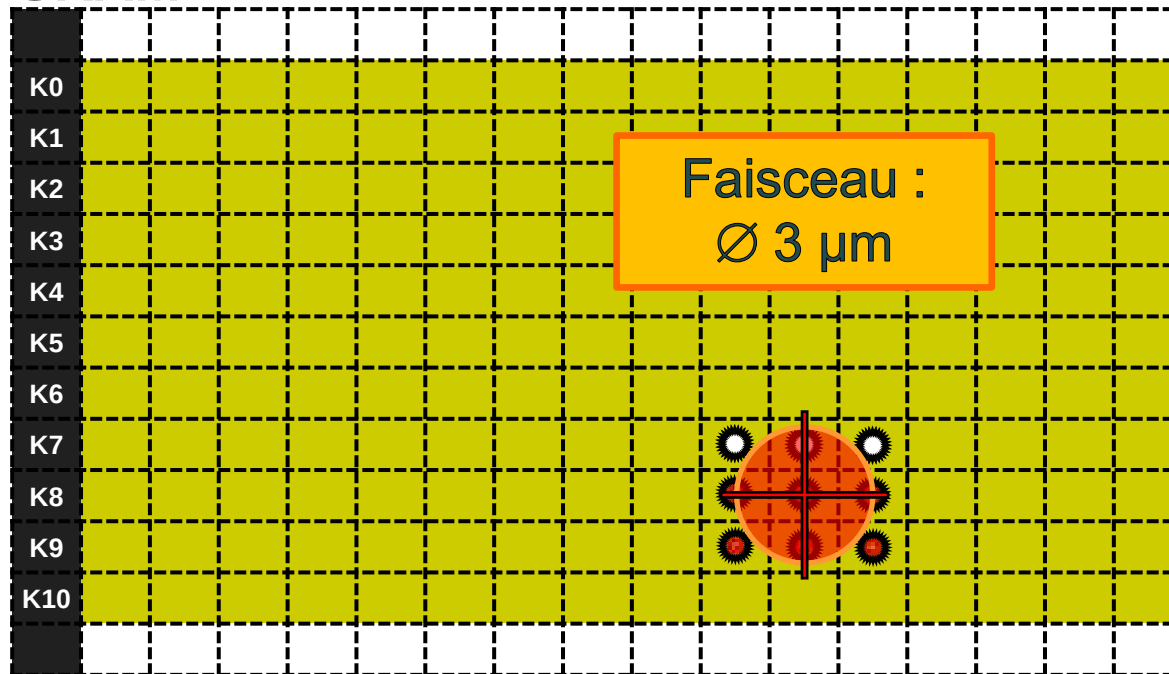


DFA mono-octet : Piret & Quisquater

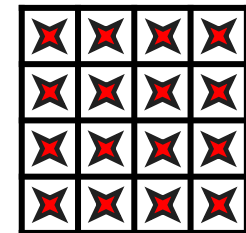
INSPIRING INNOVATION | INNOVANTE PAR TRADITION



SRAM

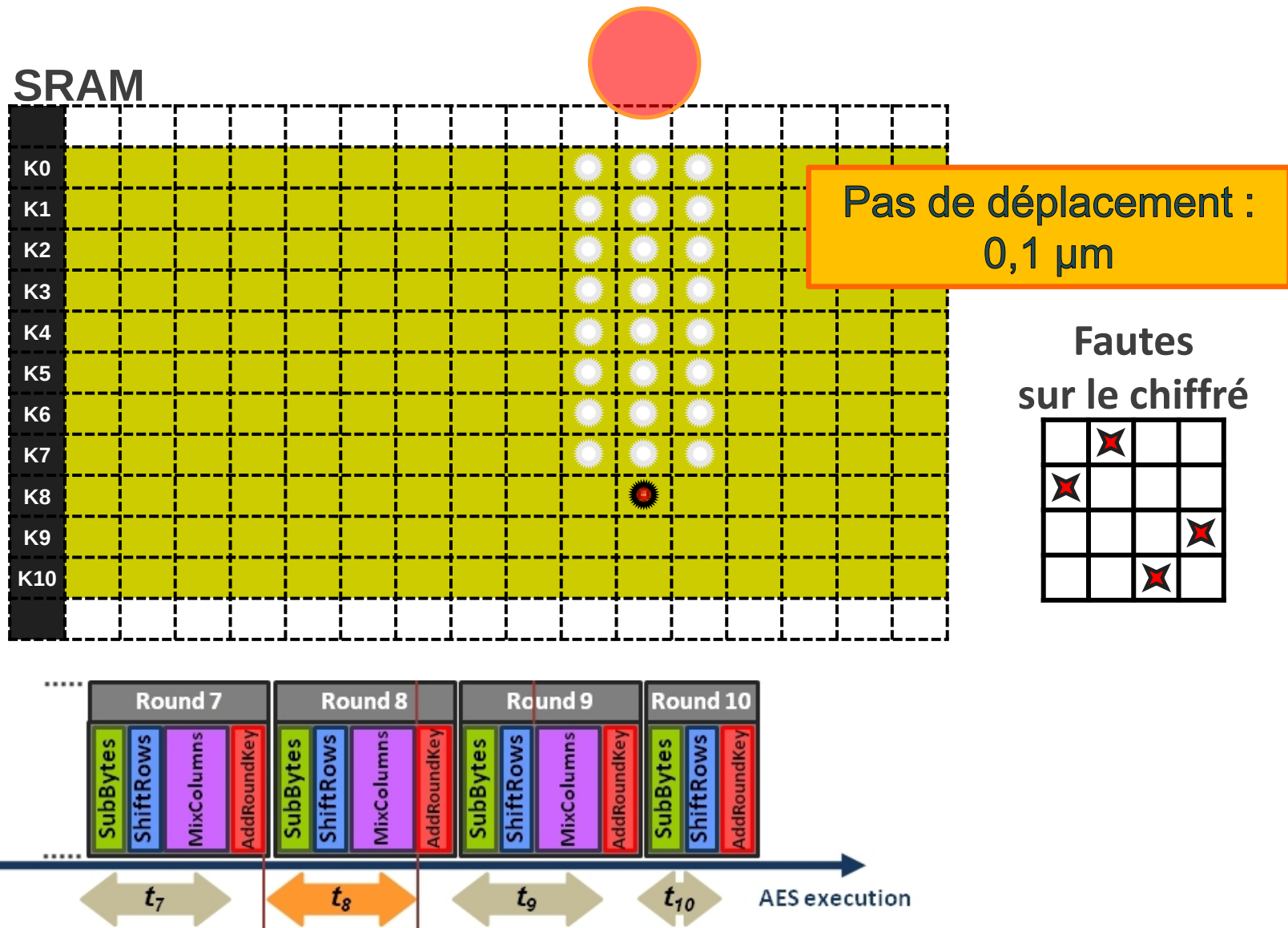


Fautes
sur le chiffré



DFA mono-octet : Piret & Quisquater

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



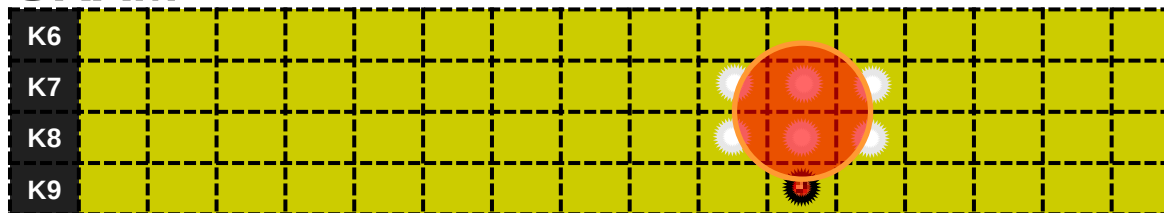
DFA mono-octet et mono-bit

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

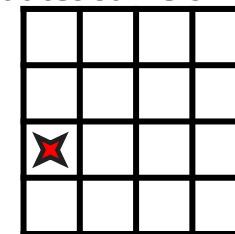


Plusieurs fautes physiques sur le circuit
MAIS une seule faute logique dans le calcul cryptographique

SRAM



Fautes sur le chiffré



Le modèle de faute théorique est respecté

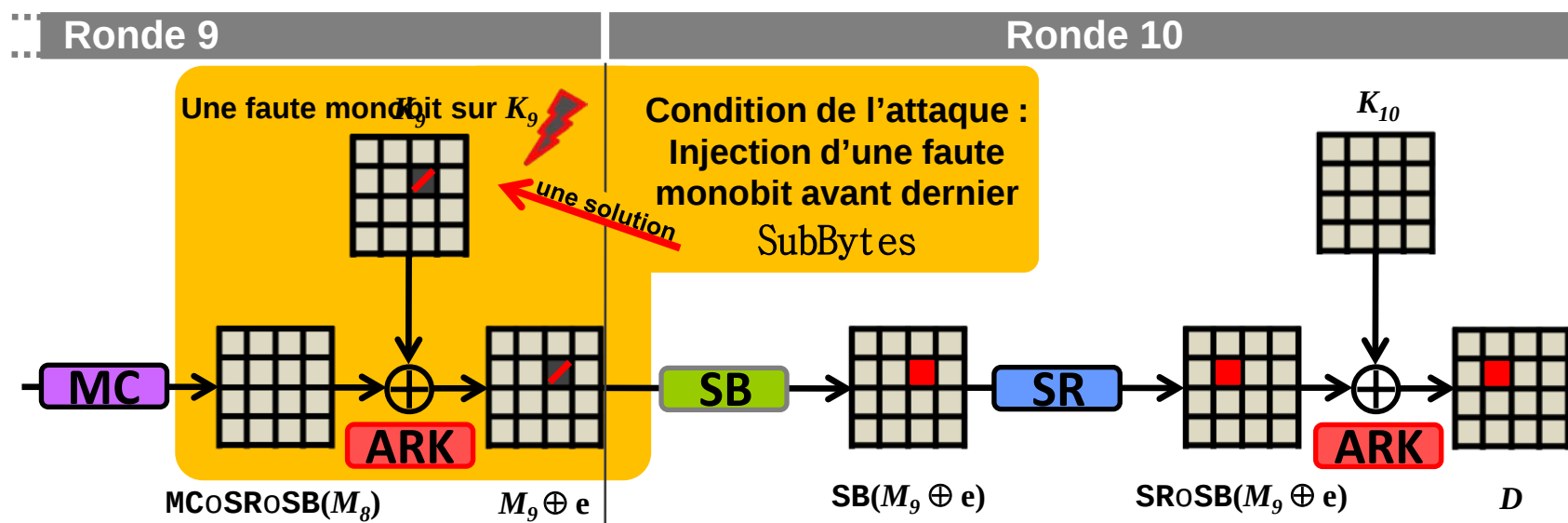
L'attaque est réussie par :

- Choix adéquat de l'instant d'injection
- Transfert de la contrainte sur la taille de spot vers le pas de déplacement de 0,1 μm

✓ **Atteinte du 1^{er} objectif**

- Est-ce qu'il y a la possibilité d'extrapolation ?

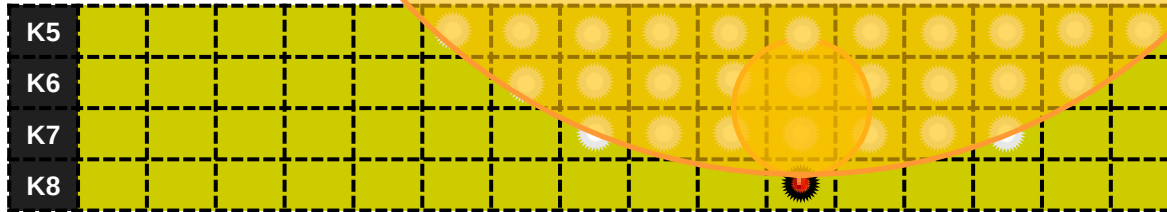
DFA mono-bit : Giraud



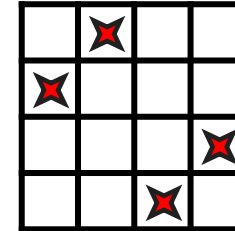
DFA mono-octet et mono-bit

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

SRAM



Fautes sur le chiffré



Avec un faisceau très large : plusieurs fautes physiques sur le circuit
MAIS encore une seule ou quelques fautes logiques dans le calcul cryptographique

Le modèle de faute théorique est respecté ; mais taux d'obtention réduit (de 50% à 5%)

L'attaque est réussie par :

- Choix adéquat de l'instant d'injection
- Transfert de la contrainte sur la taille de spot (jusqu'au 25 μm) vers le pas de déplacement de 0,1 μm

Donc, extrapolation possible vers les technologies plus fines. Toutefois, il faut considérer d'autres paramètres mis en jeu.

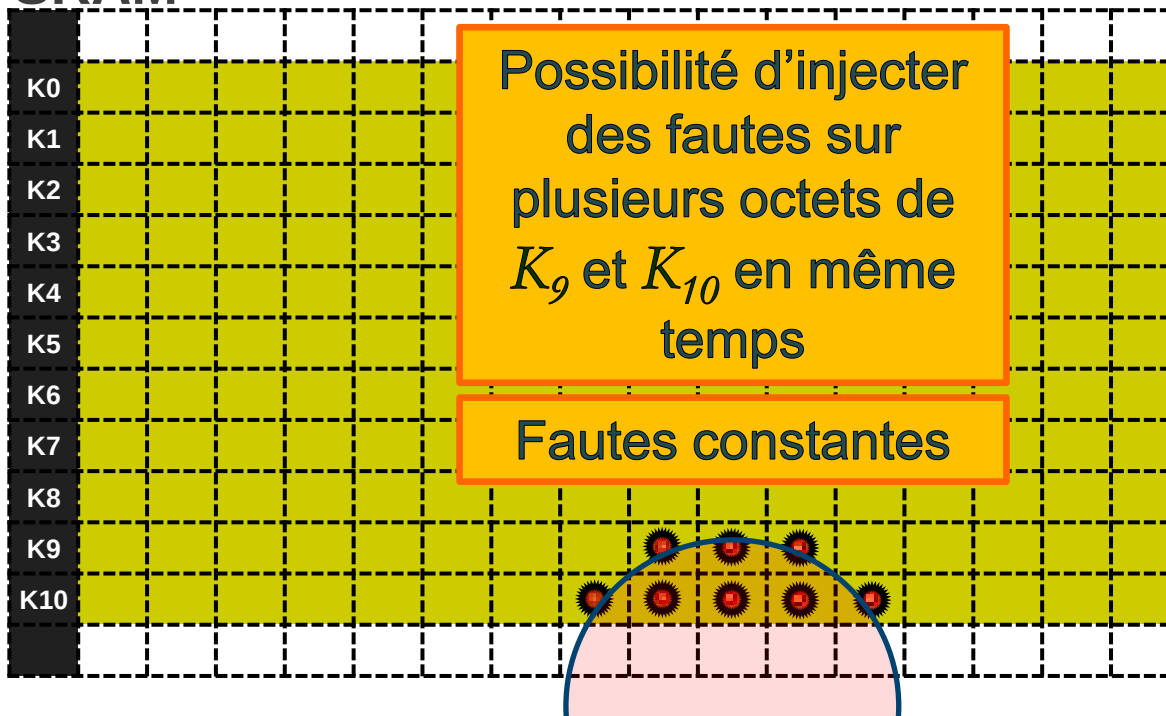
✓ **Atteinte du 2^{ème} objectif**

Nouvelle DFA élargie

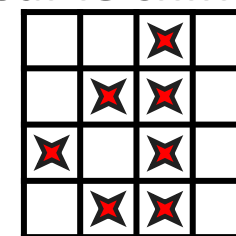
INSPIRING INNOVATION | INNOVANTE PAR TRADITION



SRAM



Fautes sur le chiffré



$$C_{\text{(chiffré correct)}} = SR \circ SB (MC \circ SR \circ SB(M_8) \oplus K_9) \oplus K_{10}$$

$$D_{\text{(chiffré fauté)}} = SR \circ SB (MC \circ SR \circ SB(M_8) \oplus K'_9) \oplus K'_{10}$$

Avec 3 paires de chiffrés corrects et fautés, on obtient une des valeurs de M_9 et ensuite :

$$K_{10} = SR \circ SB (M_9) \oplus C$$

Nouvelle DFA élargie

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



Avantages :

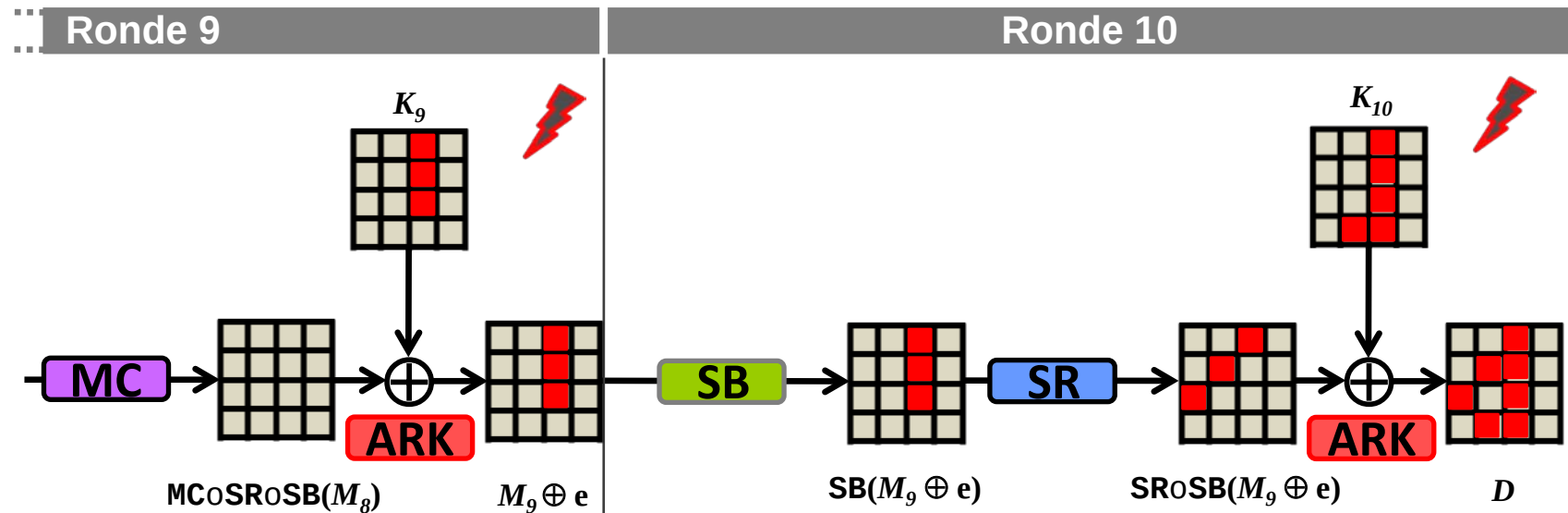
- Fautes en ronde 9 non limitées, ni à mono-bit, ni à mono-octet
- Fautes en ronde 10 acceptées sans limite

Contrainte :

- Répétition des mêmes fautes pour 3 textes
- Fautes constantes

Attaque découverte et présentée également
par V. Lomné, K. Khalfallah et T. Roche à CARDIS 2011

Nouvelle DFA élargie



$$C_{\text{(chiffré correct)}} = \text{SR} \circ \text{SB} (\text{MC} \circ \text{SR} \circ \text{SB}(M_8) \oplus K_9) \oplus K_{10}$$

$$D_{\text{(chiffré fauté)}} = \text{SR} \circ \text{SB} (\text{MC} \circ \text{SR} \circ \text{SB}(M_8) \oplus K'_9) \oplus K'_{10}$$

Avec 3 paires de chiffrés corrects et fautés, on obtient une des valeurs de M_9 et ensuite :

$$K_{10} = \text{SR} \circ \text{SB} (M_9) \oplus C$$

Nouvelle DFA élargie

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



Jusqu'à présent, attaques en entrée de la dernière ronde, c'était du monobit

Mais, avec cette nouvelle DFA élargie :

- Fautes libres constantes (sans contrainte sur le nombre de bits)
- Plusieurs octets en parallèle
- Fautes en ronde 10 acceptées sans limite

✓ Atteinte partielle du 3ème objectif

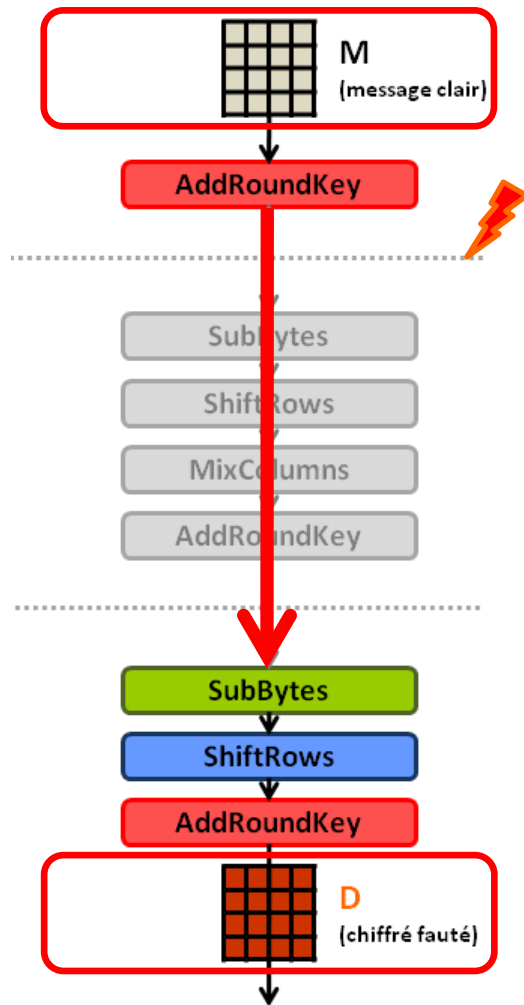


RMA : Round Modification Analysis – Analyse de modification de rondes

H. Choukri et M. Tunstall	Y. Monnet et al.	J.H. Park et al.
FDTC 2005	FDTC 2006	ETRI Journal, juin 2011
RR	RR	RR
AES	DES	AES
PIC16F877 à 8-bit	2 cryptoprocresseurs ASIC asynchrones	Atmega128 à 8-bit
Attaque sur le CR : R1→R10	Attaque sur le CR multi-rail de 17 lignes	Attaque sur le CR : R2→R10
1 rondes	rondes différentielles	2 rondes
Pic de courant sur V_{CC}	laser	laser

Scénarios d'attaque sur notre AES

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



START

$C \leftarrow M$

$C \leftarrow C \oplus K$

FOR ($CR \leftarrow 1$; $CR < R_{\max}$; $CR++$)

{

$C \leftarrow \text{SBOX}(C)$

$C \leftarrow \text{SR}(C)$

$C \leftarrow \text{MC}(C)$

$C \leftarrow C \oplus K_{CR}$

}

$C \leftarrow \text{SBOX}(C)$

$C \leftarrow \text{SR}(C)$

$C \leftarrow C \oplus K_{CR}$

END

1

sur CR

2

sur $R_{\max}$

Scénario 1 - Attaque sur le compteur de rondes



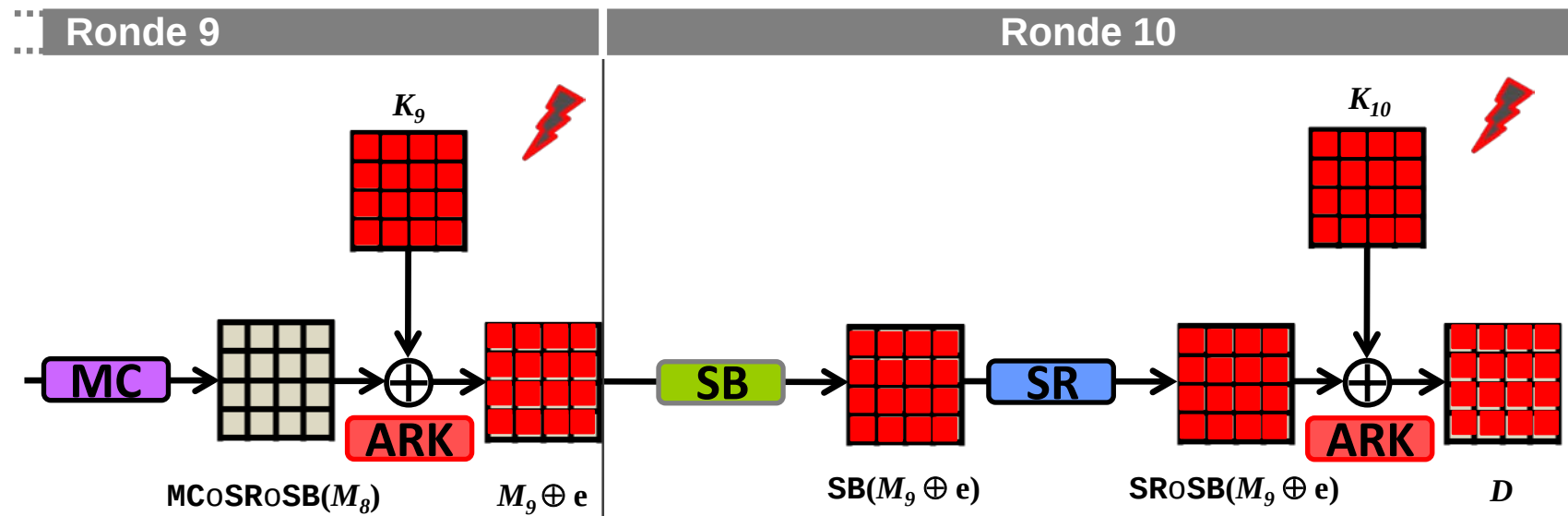
INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Instant d'attaque : CR = 9 [SB, SR, MC]

Exemple de faute = {0x10}

R_9 ARK : CR = ~~9~~ 25 $\Rightarrow R_{m=25}$

R_f ARK : CR = ~~10~~ 26 $\Rightarrow R_{f=26}$



$$C_{\text{(chiffré correct)}} = SR \circ SB (MC \circ SR \circ SB(M_8) \oplus K_9) \oplus K_{10}$$

$$D_{\text{(chiffré fauté)}} = SR \circ SB (MC \circ SR \circ SB(M_8) \oplus K'_9) \oplus K'_{10}$$

Avec 3 paires de chiffrés corrects et fautés, on obtient une des valeurs de M_9 et ensuite :

$$K_{10} = SR \circ SB (M_9) \oplus C$$

Scénario 1 - Attaque sur le compteur de rondes

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



- Plusieurs attaques exploitables sont faisables
- Mais, notre algorithme AES recherche des valeurs de clef de rondes non existantes
- Donc, exploitations plus complexes ; mais, toujours faisable avec cryptanalyses légères pour 8 attaques

Scénario 2 - Attaque sur la référence du nombre de rondes



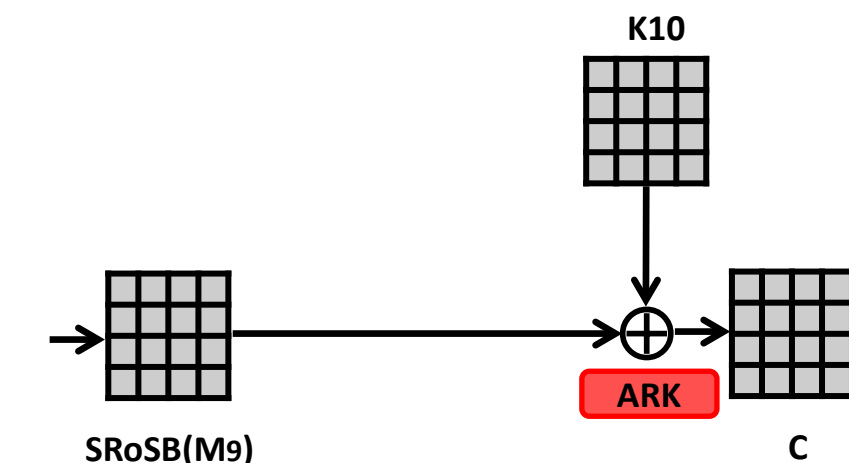
INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Instant d'attaque : entre CR=0 et CR=10 FOR

$R_{\max}=10$, faute = {01} $\Rightarrow R_{\max}=11$

$\Rightarrow R_{f=10} + R_{f=11}$

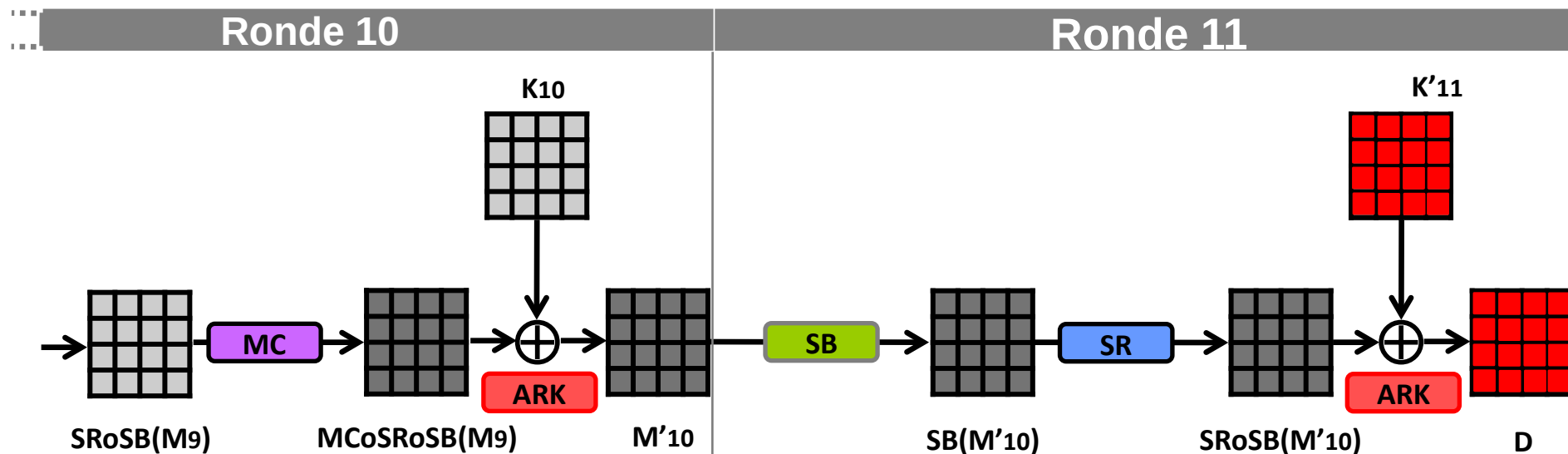
Exécution de l'algorithme : $R_0-R_1..R_9-R_{m=10}-R_{f=11}$



$$C = SR \circ SB (M_9) \oplus K_{10}$$

$$D = SR \circ SB (MC \circ SR \circ SB(M_9) \oplus K_{10}) \oplus K'_{11}$$

K_{10} retrouvée avec trois paires de chiffrés.



RMA sur AES - Conclusions

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



- En plus des attaques de RR, des attaques d'augmentation de rondes sont également faisables sur AES.
- Dans le contexte de notre circuit, une quinzaine d'attaques sont théoriquement exploitables avec un temps de calcul acceptable.
- 8 attaques ont été réalisées par l'injection de fautes mono-bits par laser et exploitées.

✓ Atteinte du 3ème objectif



- Validation expérimentale des modèles classiques d'injection de fautes mono-bit et mono-octet par laser
- Extrapolation aux technologies avancées et proposition des modèles d'injection de fautes élargies par laser
- Contribution à l'état de l'art sur les attaques matérielles :
 - Nouvelle attaque en DFA
 - Attaques d'analyse de modification de rondes



- Autres mécanismes d'injection de fautes sur microcontrôleur
 - fautes sur l'unité logique arithmétique (ALU)
 - fautes sur les bus
 - fautes sur l'opération d'expansion de clef
- Études de la vulnérabilité des mémoires flash
 - modification du programme chargé.
 - fautes sur les valeurs initiales
- Implémentation et validation de contremesures



- Validation expérimentale des modèles classiques d'injection de fautes mono-bit et mono-octet par laser et extrapolation
 - M. Agoyan, J.M. Dutertre, A.P. Mirbaha, D. Naccache, A.L. Ribotta et A. Tria, "Single-byte laser faults using large spots", *2nd PACA Security Trends In Embedded Security Workshop (PASTIS'2010)*, Gardanne, 2010.
 - M. Agoyan, J.M. Dutertre, A.P. Mirbaha, D. Naccache, A.L. Ribotta et A. Tria, "How to flip a bit?", *IEEE International Online Testing Symposium (IOLTS'2010)*, Corfu, 2010, pp. 235-239.
 - J.M. Dutertre, A.P. Mirbaha, D. Naccache et A. Tria, "Reproducible single-byte fault injection", *IEEE Conference on PhD Research in Microelectronics and Electronics (PRIME'2010)*, Berlin, 2010, pp. 1-4.
- Attaques d'analyse de modification de rondes
 - J.M. Dutertre, A.P. Mirbaha, D. Naccache et A. Tria, "Round modification analysis", En cours de préparation.



- Extrapolation et proposition des modèles d'injection de fautes élargies par laser
 - M. Agoyan, J.M. Dutertre, A.P. Mirbaha, D. Naccache, A.L. Ribotta et A. Tria, "Single-bit DFA using multiple-byte laser fault injection", *IEEE Homeland Security Technologies Conference (HST'2010)*, Waltham, 2010, pp. 113-119.
 - M. Agoyan, J.M. Dutertre, A.-P. Mirbaha, D. Naccache, A.-L. Ribotta et A. Tria, "Single-bit DFA vs. single-byte DFA: When the harder method becomes the more practical", En attente de soumission.
- Autres travaux sur injection de fautes par laser
 - A. Tria, B. Robisson, J.M. Dutertre, et A.P. Mirbaha, "Fault attacks from theory to practise: what is possible to do?", *2nd Canada-France Workshop on Foundations & Practice of Security*, Grenoble, 2009.
 - J.M. Dutertre, A.P. Mirbaha, A. Tria, B. Robisson et M. Agoyan. "Revue expérimentale des techniques d'injection de fautes", *Journée Sécurité GDR SoC-SiP*, Paris, 2010.
 - J.-M. Dutertre, J. J.A. Fournier, A.-P. Mirbaha, D. Naccache, B. Robisson et A. Tria, "Review of fault injection mechanisms and consequences on countermeasures design", *IEEE Design and Technology of Integrated Systems (DTIS'2011)*, Athens, 2011, pp. 1-6.

Contributions – suite

INSPIRING INNOVATION | INNOVANTE PAR TRADITION



- Autres contributions

- J.M. Dutertre, A.P. Mirbaha, D. Naccache et A. Tria, “Very close to perfect solutions against power attacks”, *EuroCrypt’2010*, Monaco, 2010.
- B. Chung, S. Marcello, A.-P. Mirbaha, D. Naccache et K. Sabeg, “Operand folding hardware multipliers”, *ArXiv e-prints*, cs.MS, 1104.1533.
- J.M. Dutertre, A.P. Mirbaha, D. Naccache et A. Tria, “A photovoltaic countermeasure against power attacks on smart cards”, En attente de soumission.
- A.P. Mirbaha et al., “A novel deterministic primality test based on Dirichlet’s theorem”, En attente de soumission.



Merci pour votre attention

mirbaha@emse.fr