WISG16
WORKSHOP INTERDISCIPLINAIRE SUR LA SÉCURITÉ GLOBALE

ANR

utt
université de technologie Troyes

ies l'institut d'électronique

LIRMM

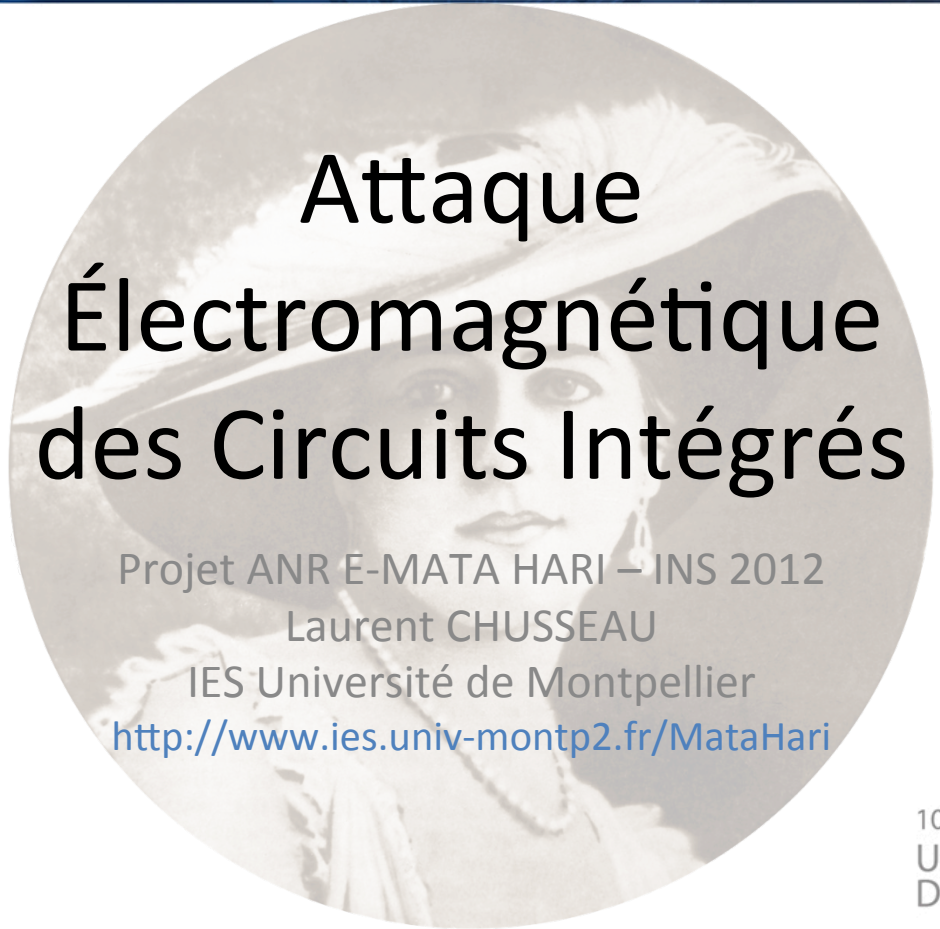
LAAS-CNRS

freescale

SAFRAN Morpho

cea

Ecole Nationale Supérieure des Mines SAINT-ETIENNE



Attaque Électromagnétique des Circuits Intégrés

Projet ANR E-MATA HARI – INS 2012
Laurent CHUSSEAU
IES Université de Montpellier
http://www.ies.univ-montp2.fr/MataHari

10 ET 11 FÉVRIER 2016
UNIVERSITÉ DE TECHNOLOGIE DE TROYES

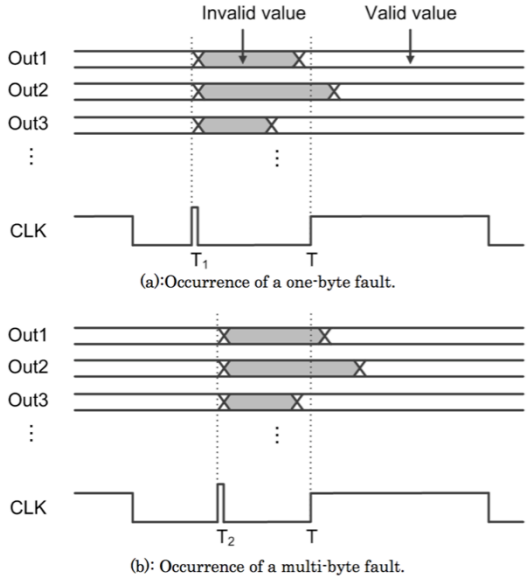
Cryptanalyse par canal auxiliaire

- La sécurité logicielle n'est rien si il existe des vulnérabilités matérielles
- Problématique du système embarqué: difficile à protéger matériellement
- "Ecouter" ou perturber le fonctionnement du circuit
  - Analyse de consommation SPA/DPA
  - Analyse d'émanations EM
  - Générer des attaques par création de faute dans le circuit
    - Laser (invasif) : crée des impulsions de courant localisées dans les zones de charge d'espace des transistors
    - EM : crée des impulsions de courant ou de tension sur les lignes d'un circuit
    - …

➔ Permet de remonter aux clés secrètes par analyse statistique

Types de fautes

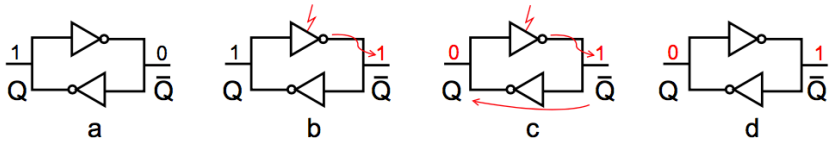
“Glitch” ou faute de timing



Dépendant de la fréquence d’horloge

Bit-set
Bit-reset
Bit-flip

SRAM

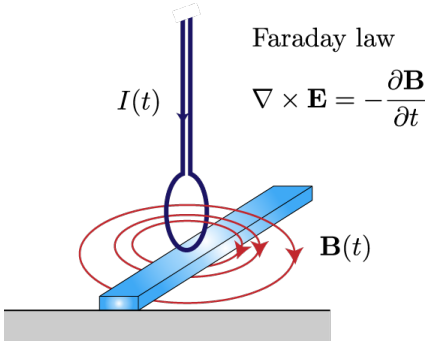


Indépendant de la fréquence d’horloge

➔ Le plus dangereux, même smartcards

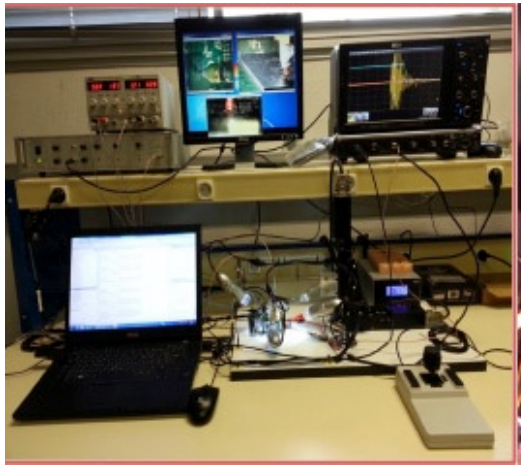
Attaques Électromagnétiques

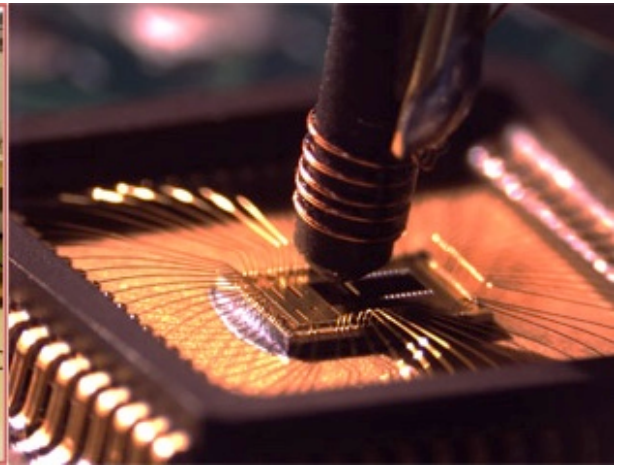
Principe



- Induction d'un champ local
- Modification de la tension et du courant sur la ligne

Application pratique

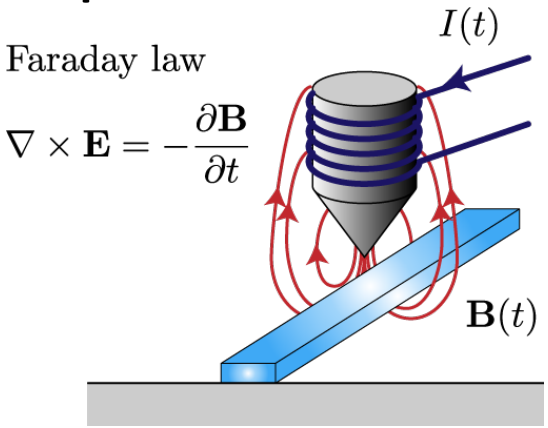




Comment optimiser ces attaques et s'en prémunir ?

Sondes dédiées aux attaques EM

Exemple: Sondes à ferrite

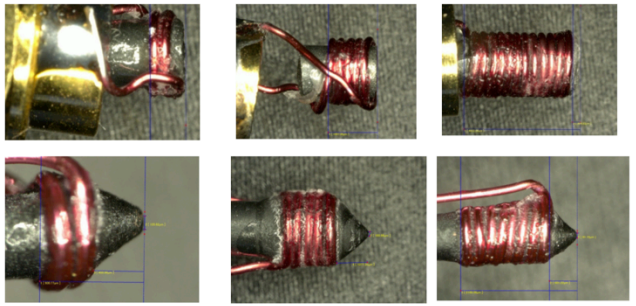


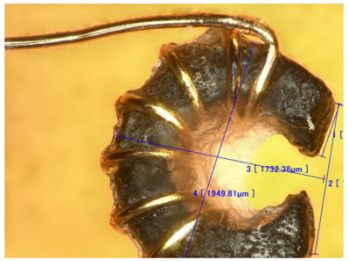
Dissocier la production de **B** et son intensité
- Résolution 400µm
- Indépendant du nb de tours

Modèle:
- Comportement physique de la ferrite
- Modèle électrique en *f*

Réalisations et autres sondes…

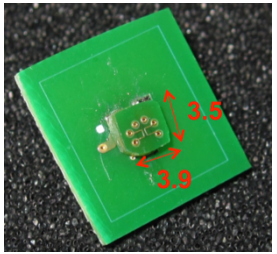
Sondes à ferrite appointées ou non





Sonde en U

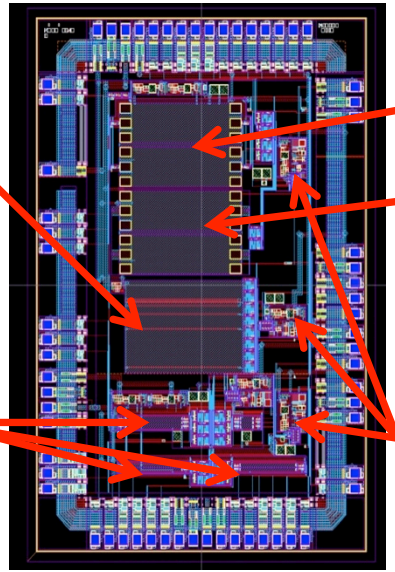
Sonde interférométrique à boucles multiples sur PCB



Circuits dédiés pour le test

- Technologie Freescale 0.25 µm SMARTMOS
- Inclus beaucoup de structures interconnectées avec des capteurs de tension on-chip (**OVS**)
- CQFP64 package sans couvercle

Chip#1
3mmx4.5mm



50Ω lines

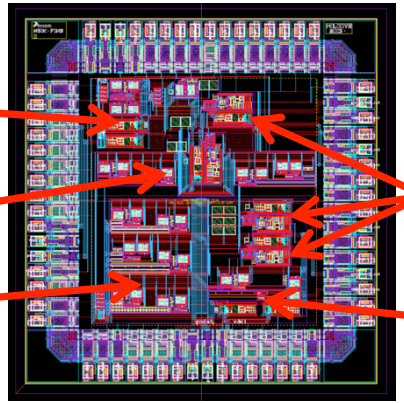
Buses

Die-to-die bonding between buffers

Die-to-die bonding between 50Ω loads

OVS

Chip#2
3mmx3mm



Power rail above logic blocks

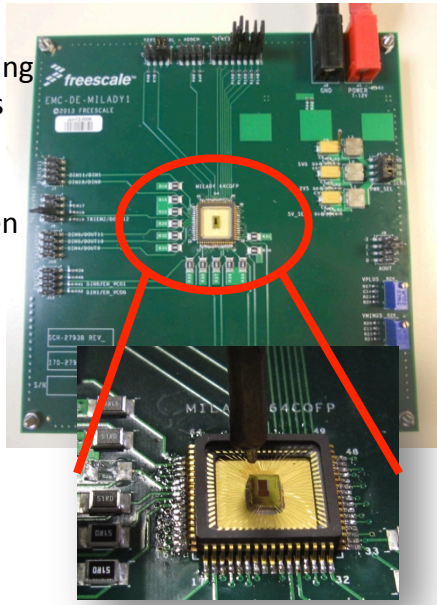
Power rails above power grid and logic blocks

Wide power rails

OVS

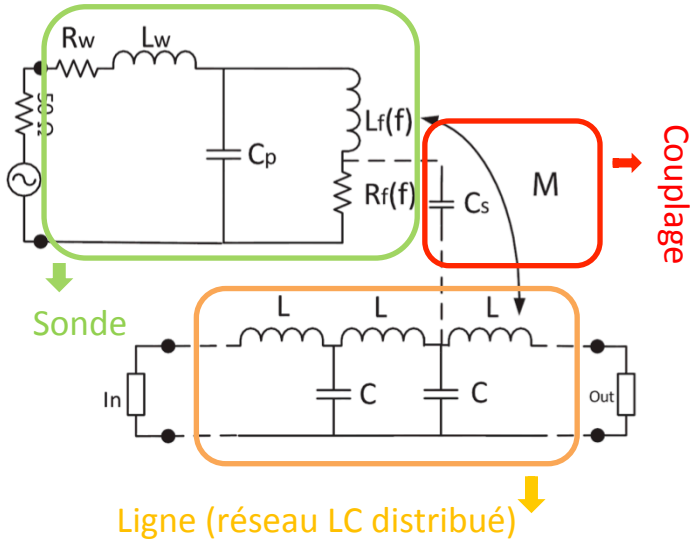
Power rails above analog blocks

PCB control card



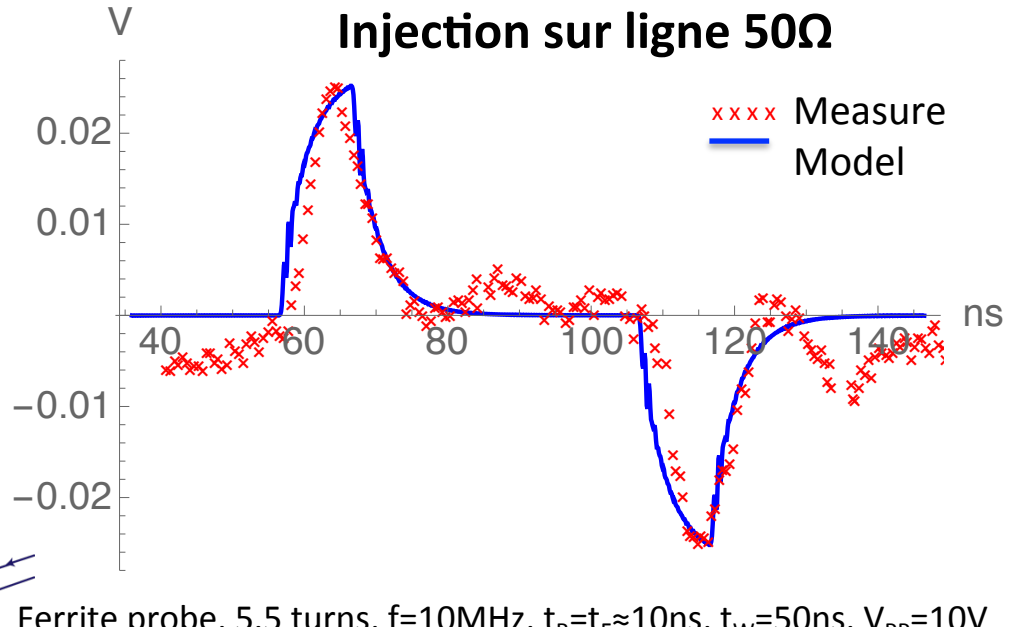
Couplage électromagnétique sur circuit

Modèle de couplage type SPICE



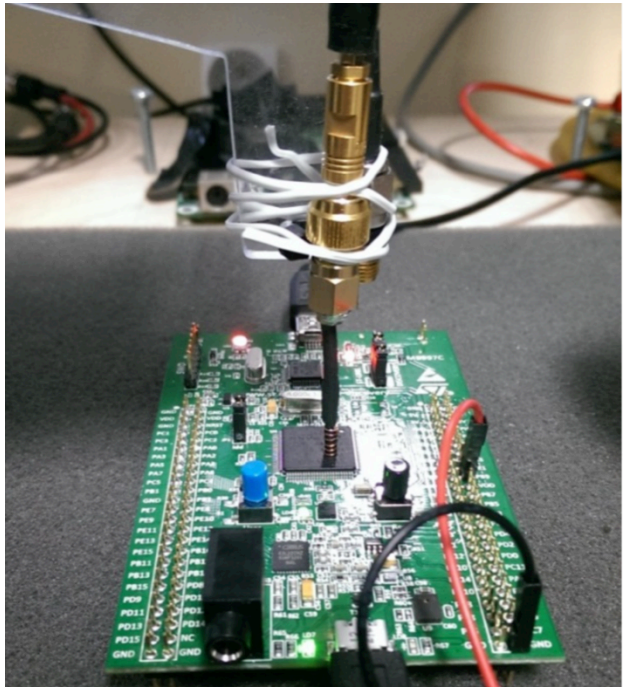
- Basé sur des mesures paramètres S
- Hypothèse validée: couplage par mutuelle inductance

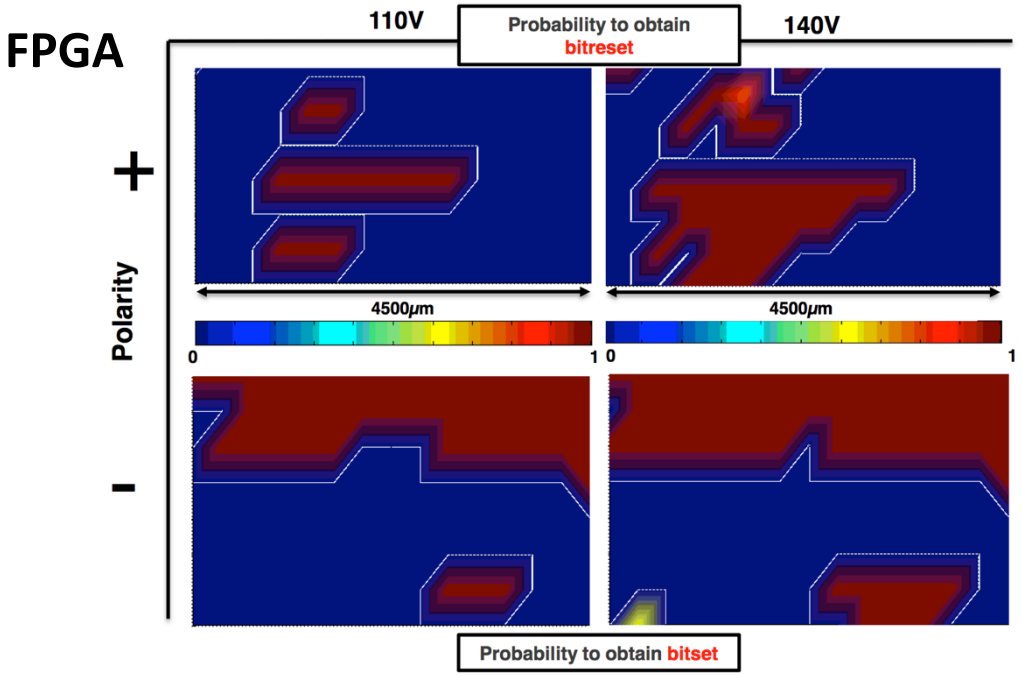
Injection sur ligne 50Ω



Ferrite probe, 5.5 turns, f=10MHz, $t_R=t_F\approx10$ns, $t_W=50$ns, $V_{PP}=10$V

Exemples d'injection de fautes EM





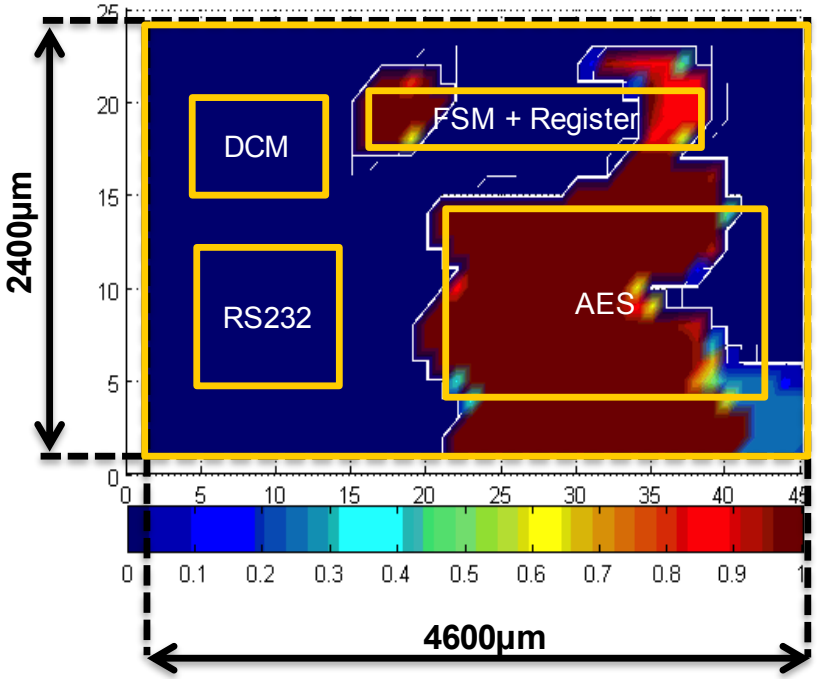
Bit-set & bit-reset observés

Application: AES sur FPGA

Chiffrement AES 128 bits sur FPGA

Attaque EM par scanning du circuit

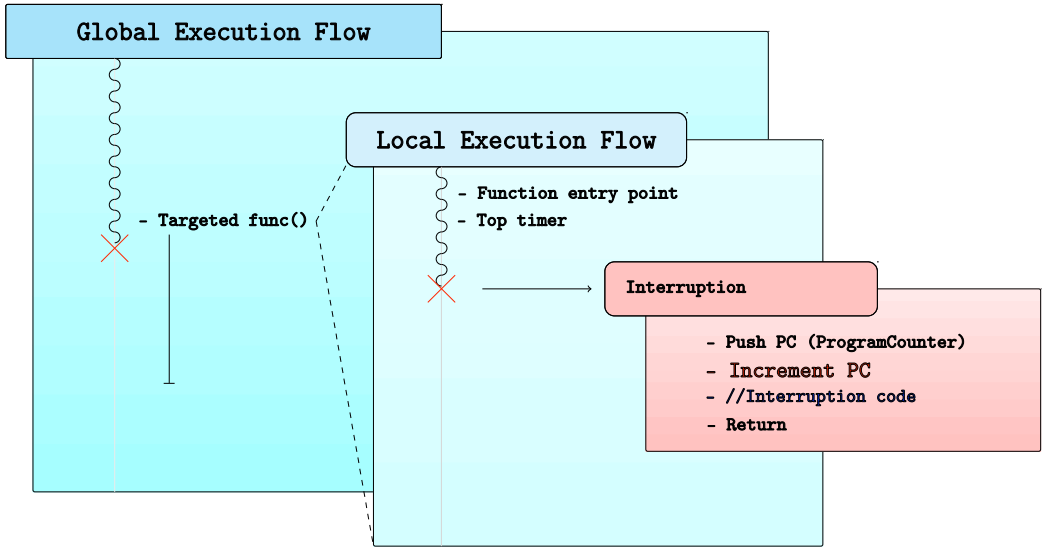
➔ fautes obtenues à 100% sur l'AES
➔ attaques locales
➔ une bonne exploitation de ces attaques permet de remonter à la clé de cryptage



Propagation des fautes dans les circuits

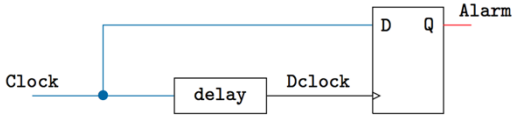
Simulateur de faute embarqué sur smartcard

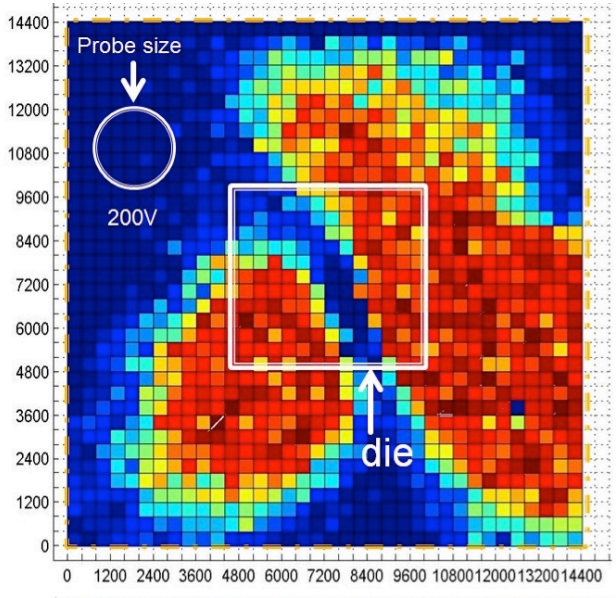
- Concept
  - Inclure la possibilité d'interruption et de modification de contexte
    ➔ variables, adresses, registres, compteurs,….
- Résultats
  - Reproduit les modèles de faute
    ➔ saut d'instruction, modification de mémoire
  - Application sur des software embarqués réels
    ➔ Identification des vulnérabilités



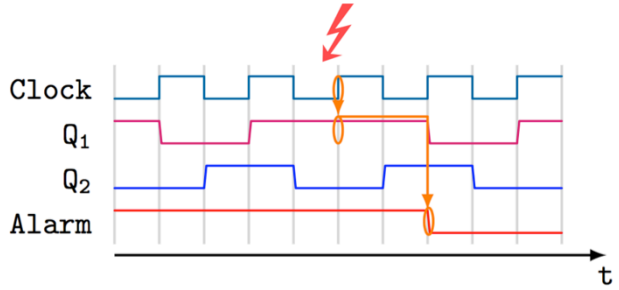
Contremesures

Capteur de « glitch »

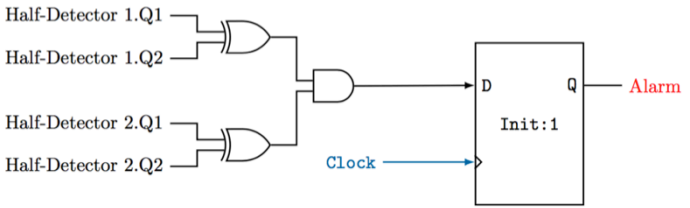




Capteur « bit-set » ou « bit-reset »



Le pulse EM induit une faute sur Q1 ↗ qui est détectée



Conclusion

E-MATA HARI a fait progresser les attaques EM sur circuits

- ✓ Des sondes dédiées et optimisées ont été conçues, réalisées et testées
- ✓ Le couplage EM a été quantifié grâce à des circuits spécifiques
- ✓ Un modèle précis du couplage a été établi
- ✓ Tous types de fautes ont été démontrées avec une menace accrue
- ✓ Un outil de modélisation de la propagation des fautes a été mis en place
- ✓ Des premières contremesures efficaces ont été proposées et testées