Laboratoire Informatique Robotique Microélectronique Montpellier

UNIVERSITÉ MONTPELLIER 2 SCIENCES ET TECHNIQUES

POLYTECH MONTPELLIER

cnrs dépasser les frontières

Sécurité Numérique

Pascal Benoit, L. Torres, F. Bruguier

INVESTISSEMENTS D'AVENIR

cnfm GIP IDEFI finmina

Contact : Pascal.Benoit@lirmm.fr

Technologies Numériques…

Sécurité…

Un hacker insultait un bébé via un moniteur

PIRATAGE — Des parents ont
à Houston (Texas) en découvr
dans la chambre de leur peti

Vos appareils connectés aussi vulnérables

Par Fabien Soyez

Virus, malwares : la cigarette

Karo
pirat

Par Fabier

3 comment

Karotz.

Vot

Par Fab

Sécuriser L'IoT : un défi commun à tous les acteurs de la chaîne

le 2 octobre 2014 |

Internet des objets | Tendances

Les entreprises commencent à investir pour la sécurité de leurs smart objects. Et pour les experts, sécuriser l'IoT doit aussi s'entendre sur le long terme, sur l'ensemble du cycle de vie des réseaux, des produits et des services.

commentez | J'aime 19 | Tweet 34 | g+1 4 | imprimer

Ces cinq prochaines années, nos voitures seront de plus en plus connectées. Avec tous les risques que cela comporte pour vos données.

Attention, votre "smart TV" est piratable, autant que votre smartphone ou que votre PC. Pour les experts en sécurité, une télévision connectée est même "la cible parfaite" pour un pirate souhaitant espionner son prochain...

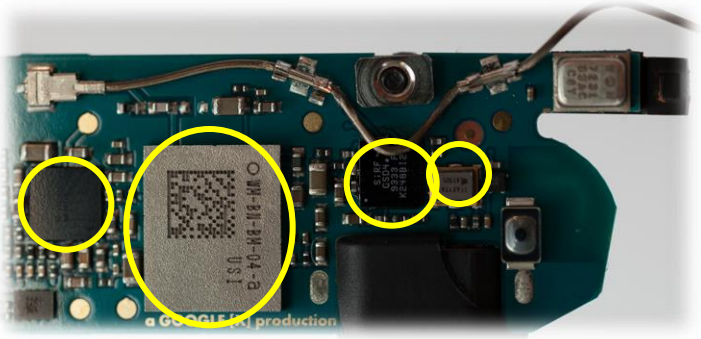
Objectifs d’un attaquant

- Espionnage : avoir accès a l'information stockée sur le matériel (si possible sans l'ouvrir).
- Interruption : empêcher le matériel de fonctionner normalement.
- Modification : pouvoir corrompre les valeurs stockées dans le matériel.
- Fabrication : pouvoir cloner ou contrefaire le matériel sécurisé.

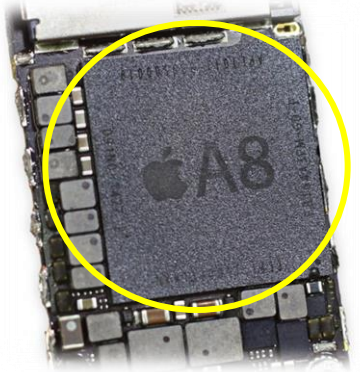
Avec l’IoT, la sécurité doit s’envisager dès la conception de l’objet

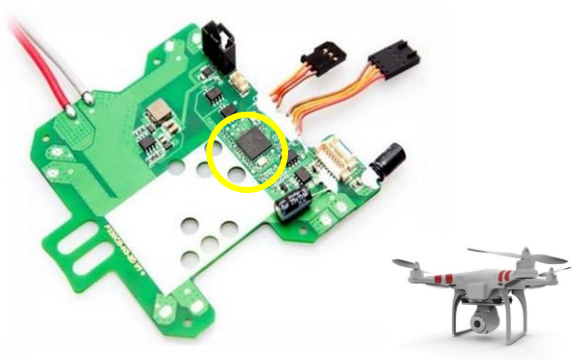
Derrière l'objet…

Google Glass



iPhone 6



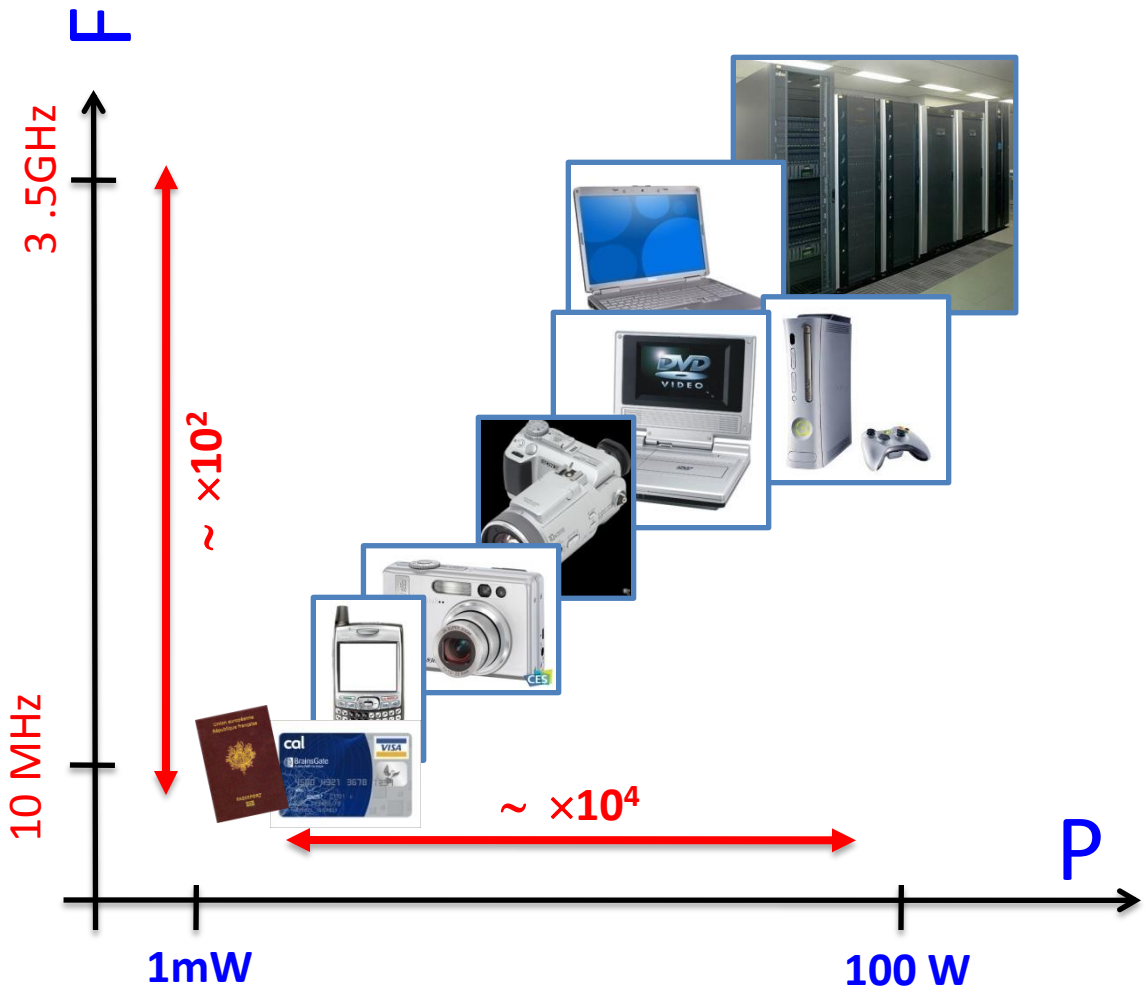


Phantom

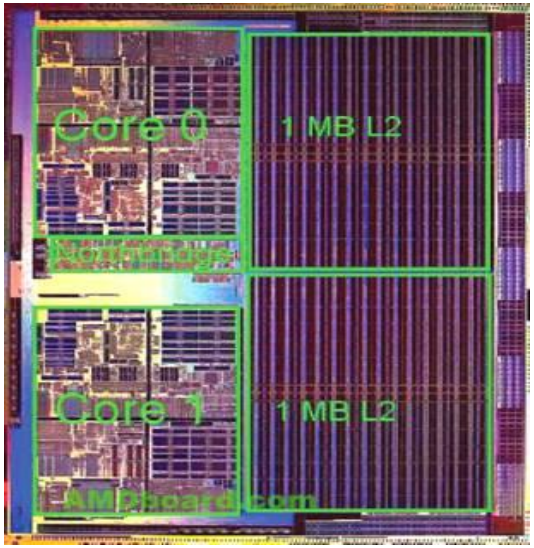
Sphero

Circuits intégrés numériques

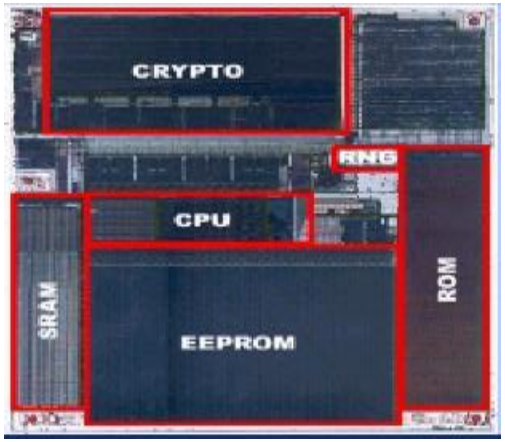
Circuits sécurisés



2,20 GHz, 65W , 85 mm²



30MHz, 10mW , 6mm²



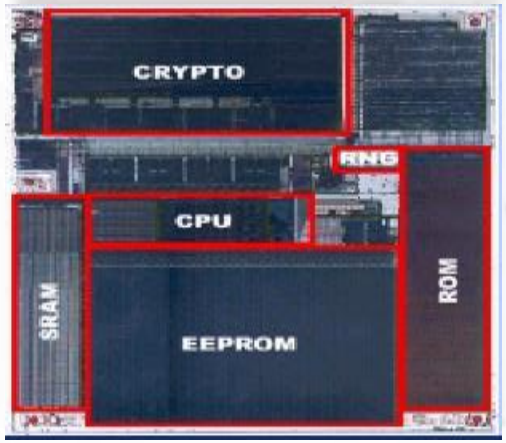
Circuits sécurisés

PERFORMANCE

CONSOMMATION

SURFACE

SECURITE



Comment sécuriser?

Plaintext Message

Message

Ciphering

Cipher Key

Encrypted Message

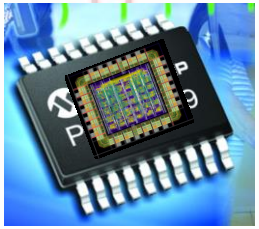
Xbkjzge dvsd,vb sdhfgdf jsldkvh evgsdv

Deciphering

Decipher Key

Message

SECRET



FUITES!!!

Angela Merkel espionnée par la NSA

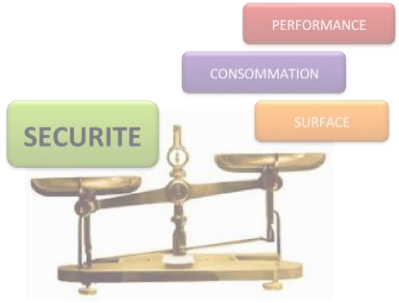
LE MONDE | 24.10.2013 à 12h31 |

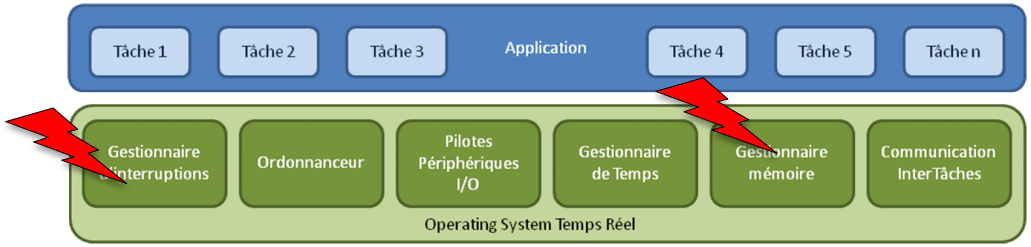
Par **Frédéric Lemaître** (Berlin, correspondant)

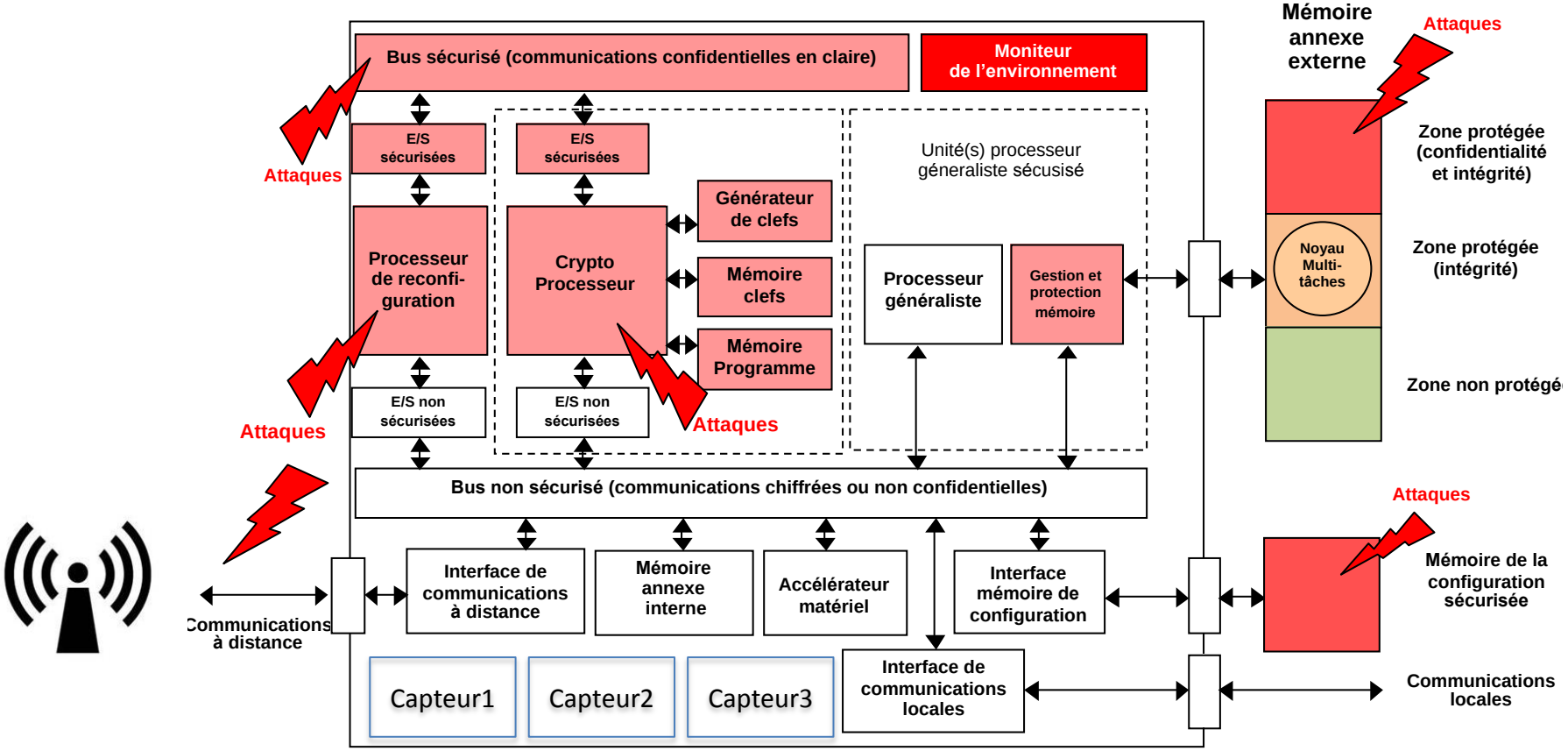
Réagir Classer Partager

Recommander Partager 29 personnes recommandent ça. Soyez le premier parmi vos amis.

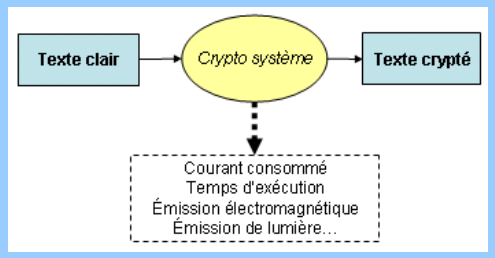
Que faut-il sécuriser?

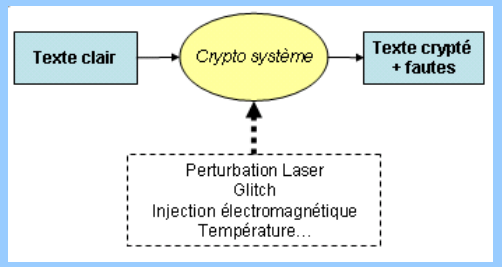






Les attaques matérielles

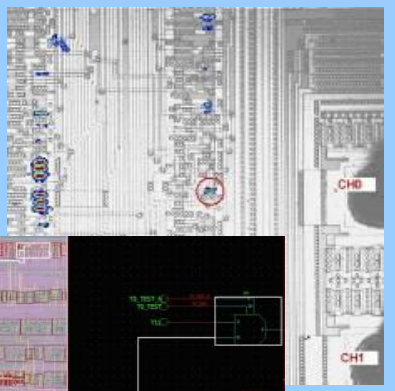


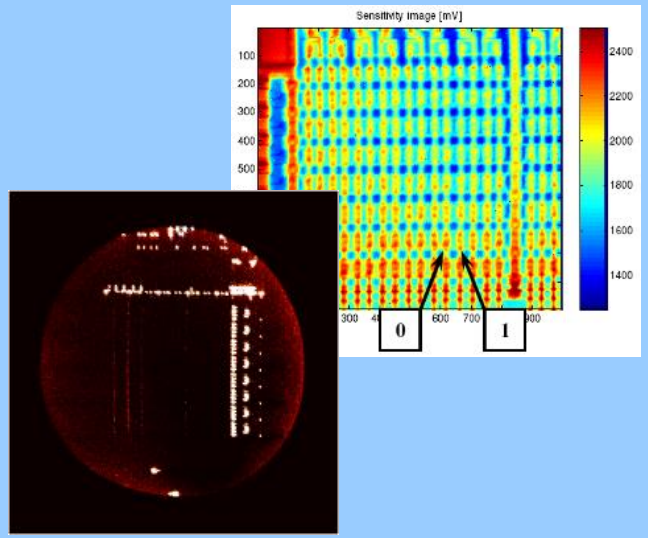


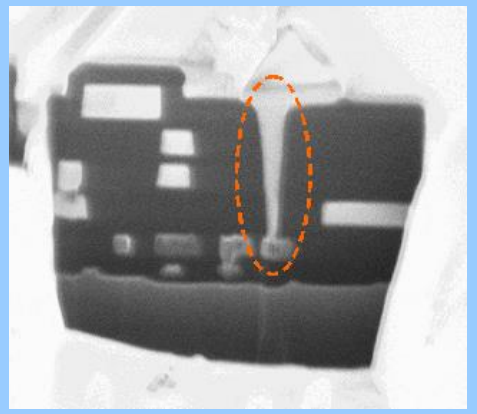
Attaques non-invasives
- Canaux auxiliaires
- Fautes / glitch
- Force brute

Attaques semi invasives
- Fautes laser
- Sondage laser
- Emission de lumière

Attaques invasives
- Reverse engineering
- Attaque en « probing »
- FIB





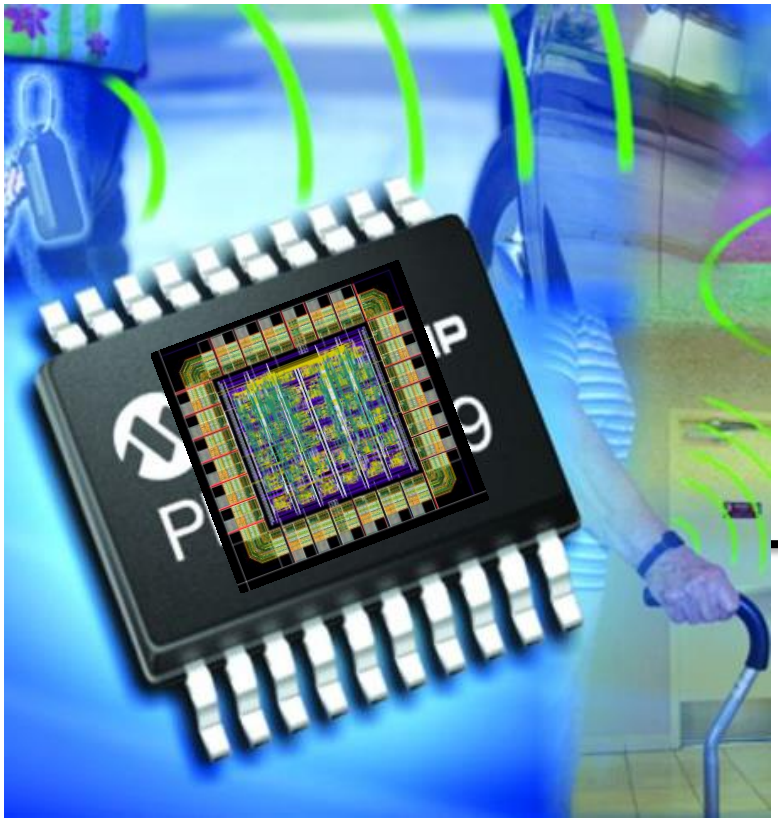


- Efficacité +

- Coût +

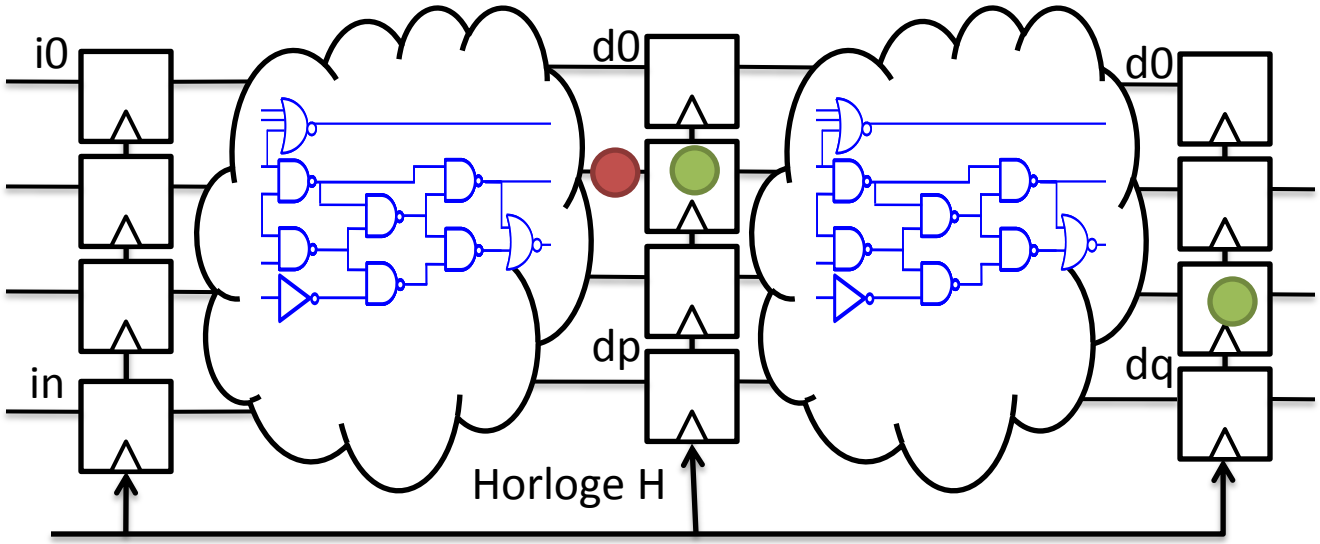
Attaques par canaux cachés

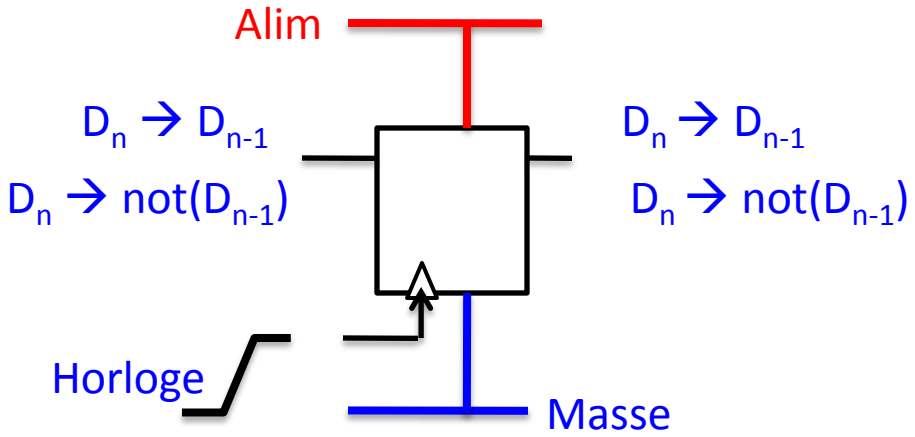
Idée : connaissant l'algorithme effectué par un dispositif matériel, extraire des informations secrètes par traitement d'une grandeur physique émise ou altérée par son fonctionnement

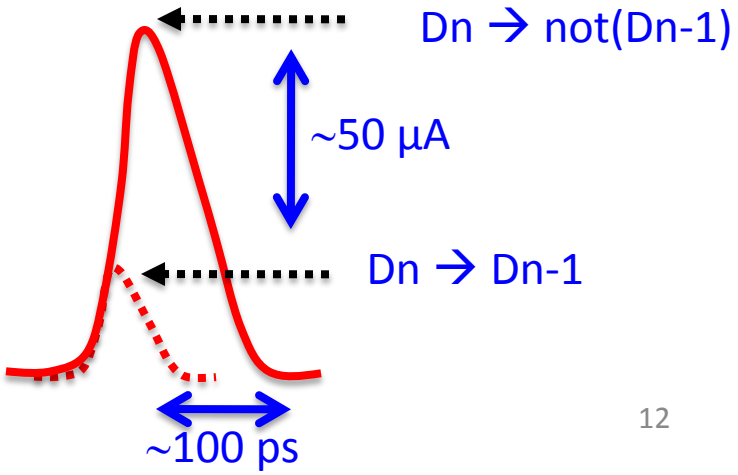


Temps de calcul ---> (Kocher 1996)
Courant ---> (Kocher 1998)
Emissions EM ---> (Gemalto 2001)

Origine des fuites physiques

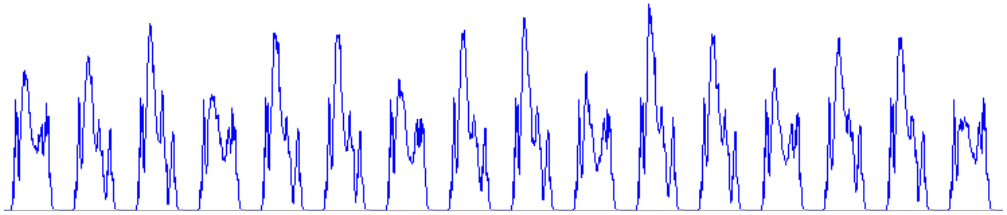




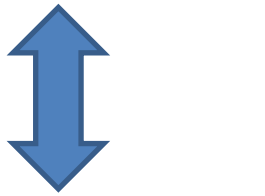


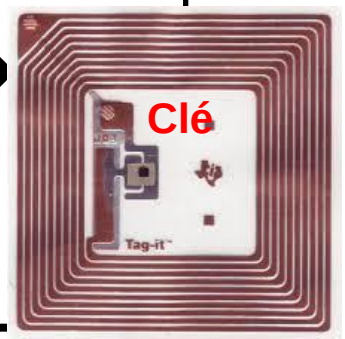
Attaque sur le DES

Etape 1 : Mesure de la consommation ou EM



Consommation/traces EM d'un DES





Message clair

64

64

Message crypté

Horloge

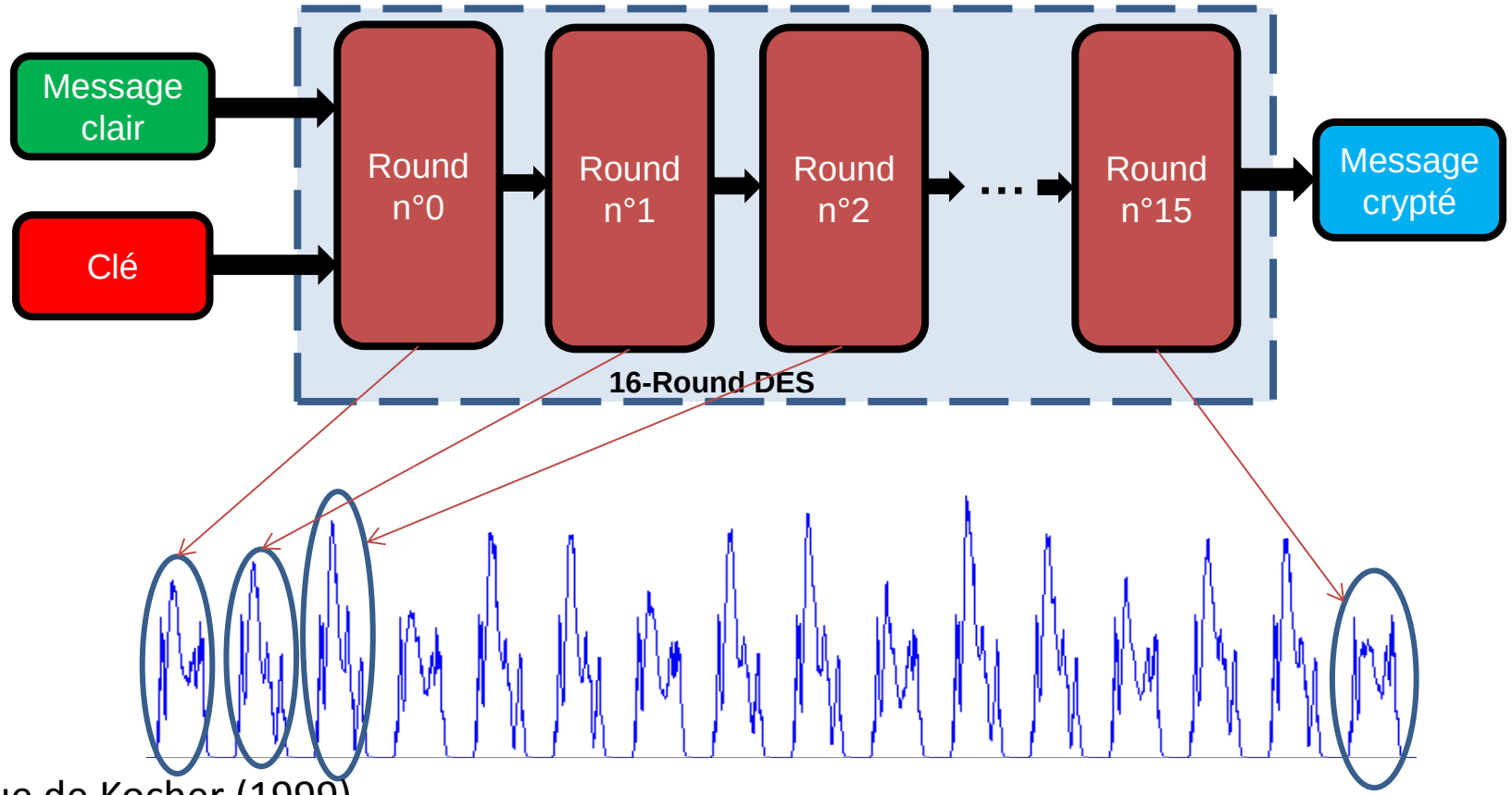
Sonde de courant

Attaque de Kocher (1999)

Attaque sur le DES

Etape 2 : Attaque et déduction d'information

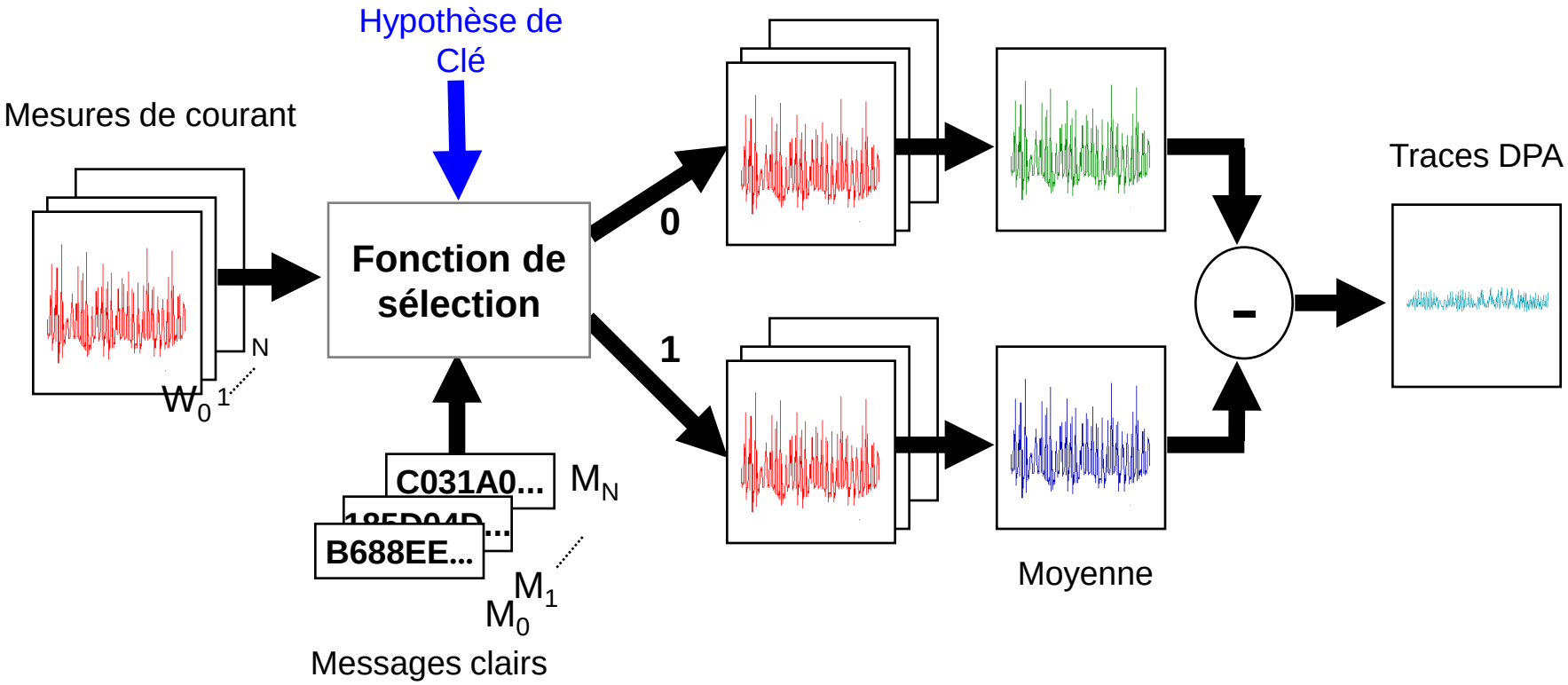
Mise en évidence du lien entre l'activité et la consommation



Attaque de Kocher (1999)

Attaque sur le DES

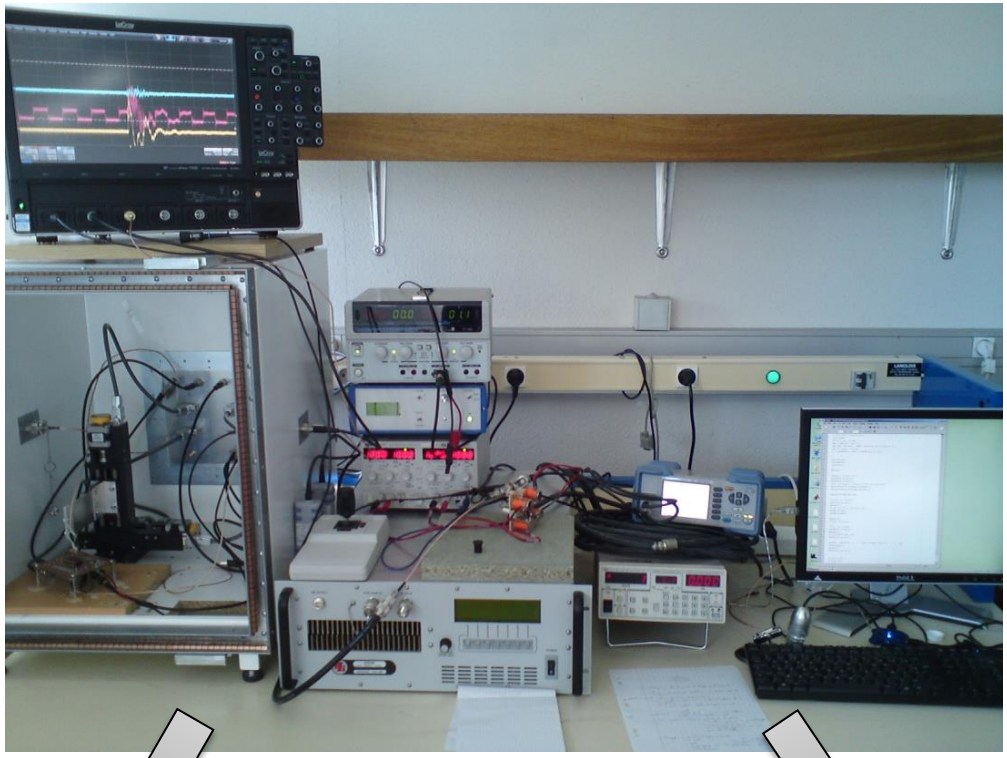
Etape 3 : Analyse statistique basée sur un modèle avec des mesures réelles



Référence : Pascal Paillier, “SPA and DPA attacks” Gemplus ARSC/STD/CRY

Référence : Paul Kocher, Joshua Jaffe, and Benjamin Jum, " Differential Power Analysis"

SECNUM



PA
(Power Analysis)
- simple
- differential

EMA
(ElectroMagnetic Analysis)
- simple
- differential

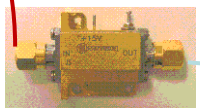
SECNUM

3.5GHz LeCroy Oscilloscope

EM waves probing

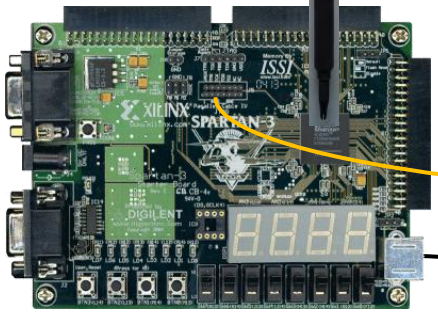
EM Probe

XYZ Table Stage
accuracy: 1µm



60dB Low-Noise Amplifier

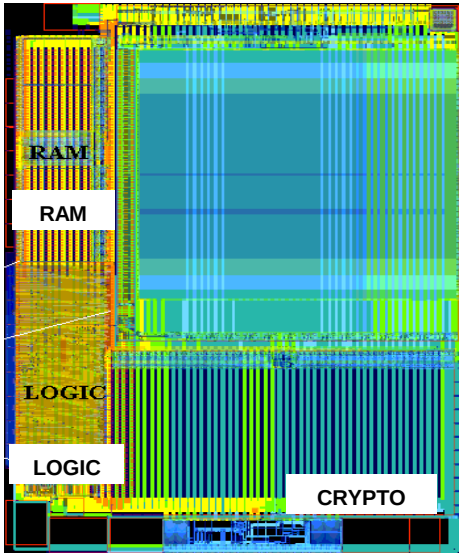
EM waves plotting



100MHz –> 1GHz circuit

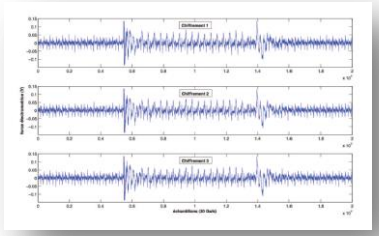
plaintext message

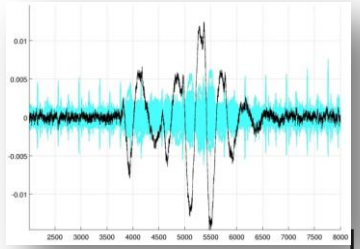
data acquisition



EM Analysis

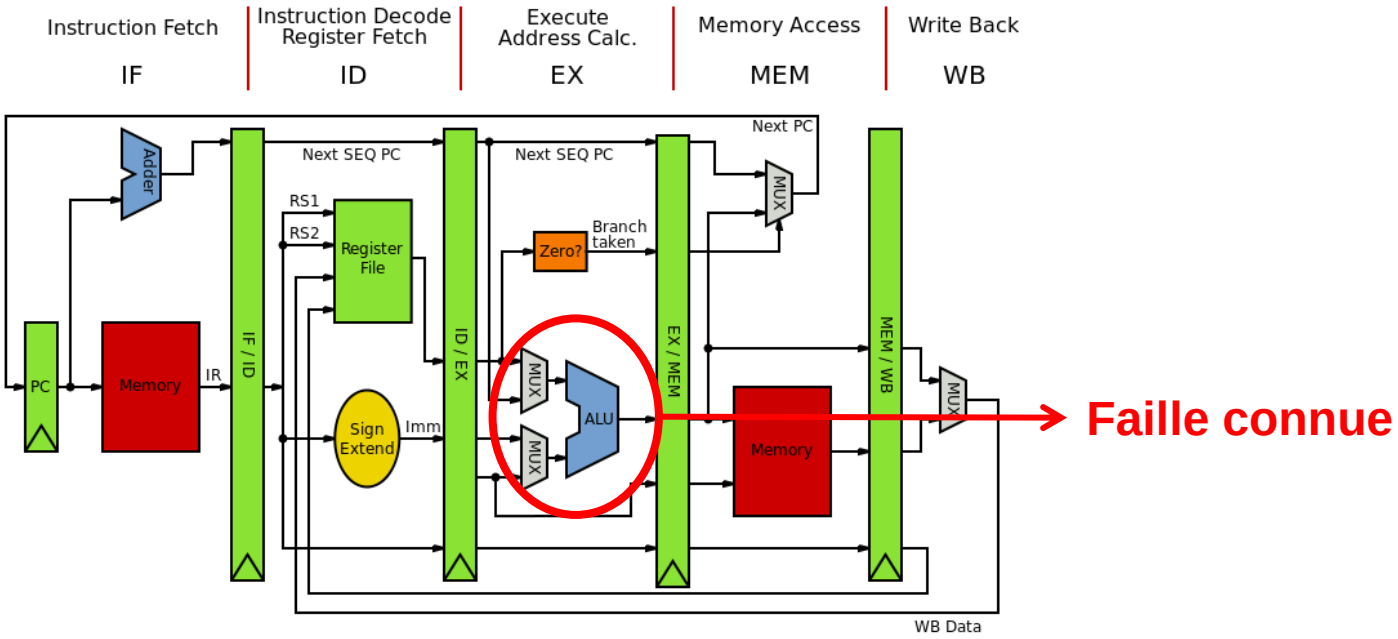
Power Supply





SECNUM: Evaluation d'un processeur RISC

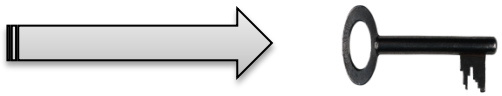
- Architecture RISC



- Evaluation SECNUM

→ Mise en évidence d'une nouvelle faille: le **pipeline**!

Attaque: 15mn



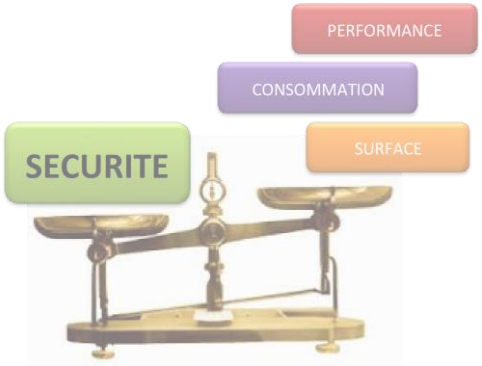
Clé secrète < 20mn
=> Rapide & peu coûteux

Acquisition: **100 traces, 4mn**

SECNUM: Conception d'un processeur sécurisé

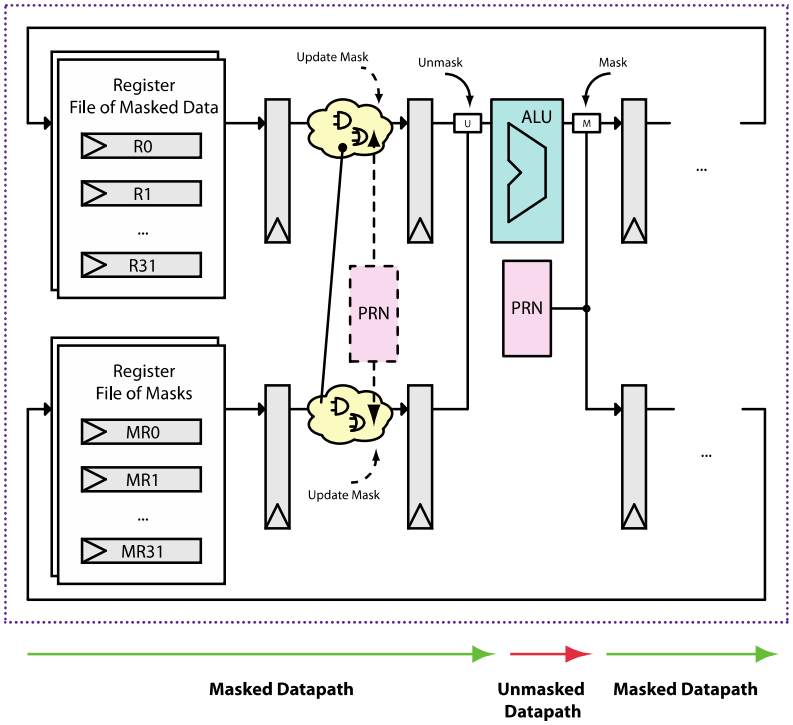
Mise en œuvre de contremesures

MASKING

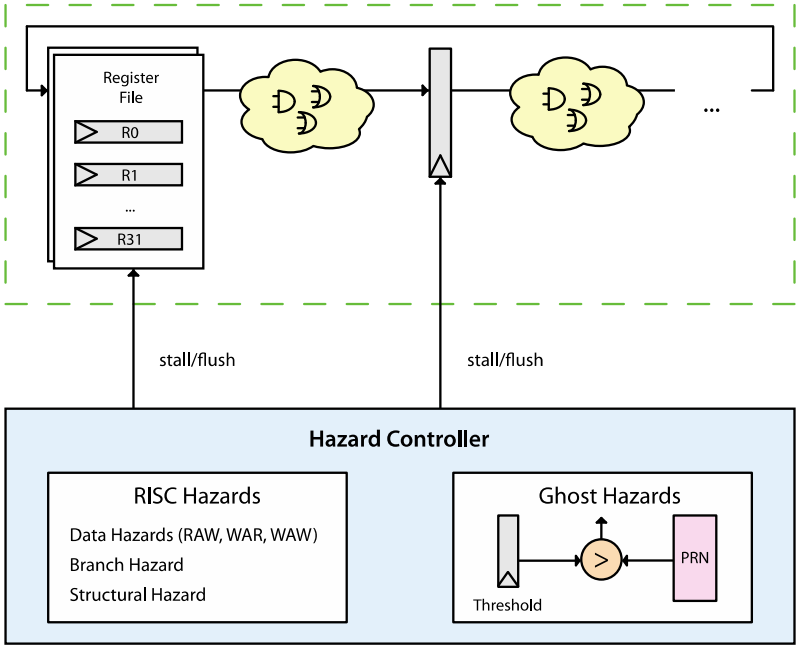


HIDING

Core



Pipeline



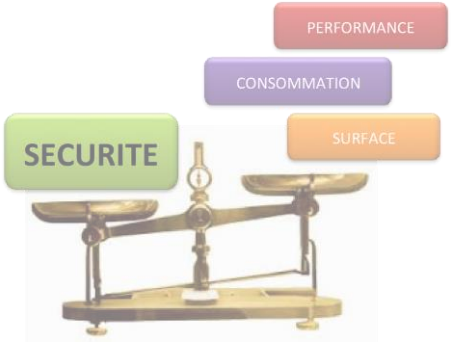
SECNUM: Conception d'un processeur sécurisé

SecretBlaze

Side-Channel Resistant

- Conception d'un processeur RISC sécurisé

Processeur sécurisé (www.lirmm.fr/ADAC)



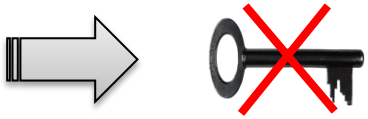
- Evaluation de la robustesse des contremesures

Processeur RISC

→ Acquisition: **100 traces – 4 minutes**
→ Attaque: **15 minutes**

SecretBlaze

→ Acquisition: **200000 traces – 1 semaine**
→ Attaque: plusieurs semaines



Publication FPL – Best Paper:
"Investigation of a Masking Countermeasure against Side-Channel Attacks for RISC-based Processor Architectures"
Authors: Lyonel Barthe, Pascal Benoit, Lionel Torres.

En conclusion: De nombreux défis

Modélisation

Flot de simulation

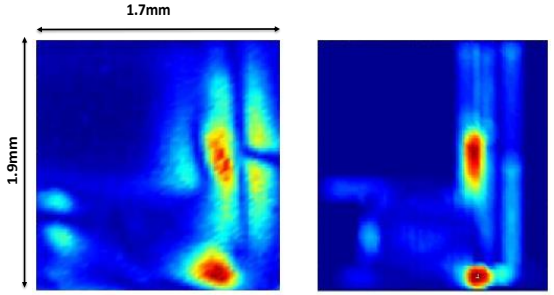
Compréhension phénomènes ϕ

Contremesures

- Logique équilibrée
- Brouillage électromagnétique
- randomisation spatiale à grain fin
- ….

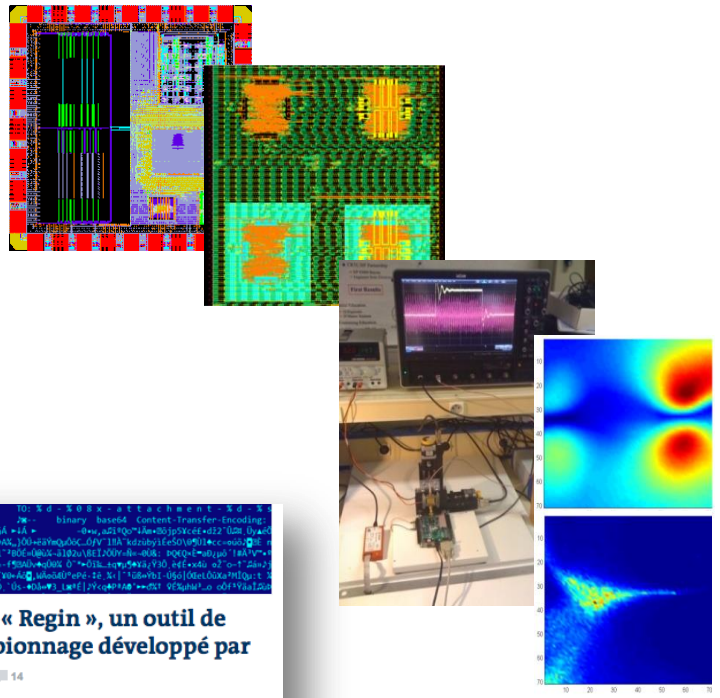
Les attaques

- Flot d'attaques (DEMA, CEMA, DGMSI)
- Méthode de pré-traitement des données
- Méthode de localisation (cohérence spectrale)
- Méthodes de Test
- Injection électromagnétique de fautes



Measured Pk2Pk map of the magnetic field (IC1)

Simulated Pk2Pk map of the magnetic field (IC1)



M PIXELS CHRONIQUES DES (R)ÉVOLUTIONS NUMÉRIQUES | VIE EN LIGNE

Après son piratage, la base de donnée de Domino's Pizza publiée sur Internet

Le Monde.fr | 21.11.2014 à 13h09 • Mis à jour le 24.11.2014 à 18h51 |

Par Martin Untersinger

Réagir Classer Partager

Le virus « Regin », un outil de cyberespionnage développé par un Etat 14

Deux entreprises de sécurité informatique affirment avoir découvert un nouveau virus, d'une telle complexité qu'il ne peut avoir été développé qu'avec le financement et les moyens techniques d'un Etat.

SECNUM

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier

LIRMM

ies l'institut d'électronique

cnfm GIP

Started 2009

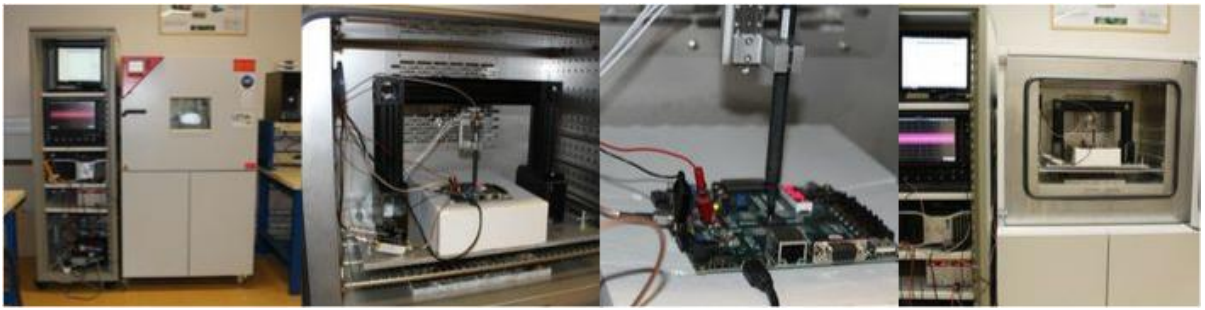
SECNUM

POLYTECH MONTPELLIER

Recherche

Industriels

Education



ST

THALES

INVIA Secure Semiconductor IP

Netheos CONFIDENTIALITÉ & SÛRETÉ NUMÉRIQUE

BULL

CROCUS Technology Blossoming future

Agence Nationale de la Recherche ANR

DGA

cea

cnrs www.cnrs.fr

la Région Languedoc Roussillon