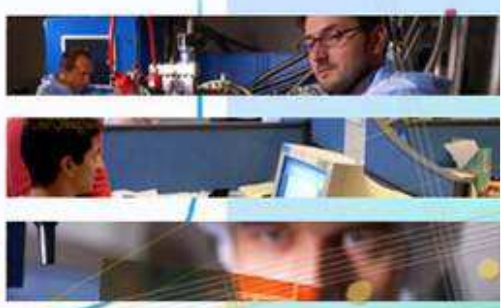
micro et nanoélectronique
microsystèmes
intelligence ambiante
biologie et santé
chaîne de l'image

2008

# La cryptographie au CESTI


Cécile Canovas

Mel : cecile.canovas@cea.fr

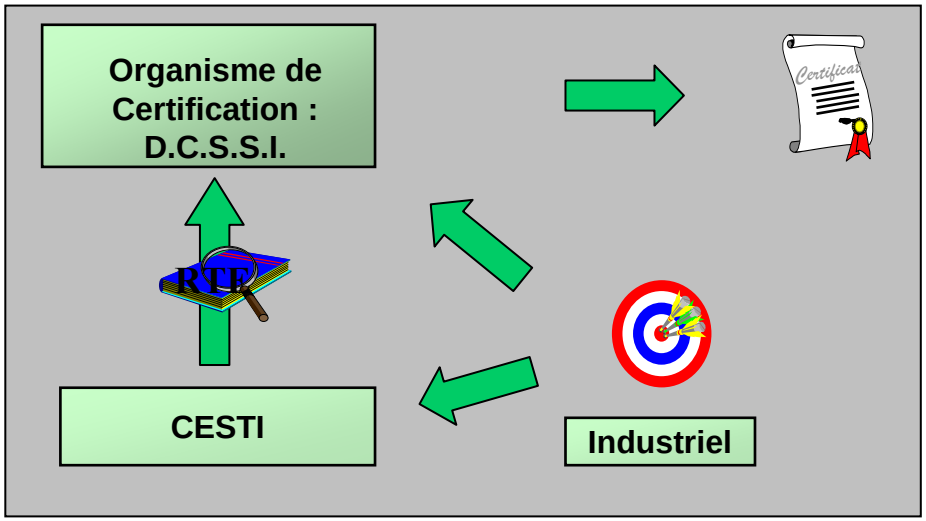



leti MINATEC INSTITUT CARNOT CEA LETI

cea

# Centre d'Évaluation de la Sécurité de l'Information

- Centre agrée dans le schéma français de certification



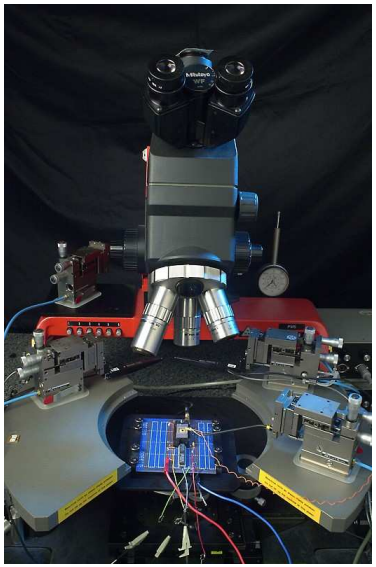

- Domaine : objets portables sécurisés
  - Carte à puce
  - Matériel et logiciel

# Les atouts du LETI

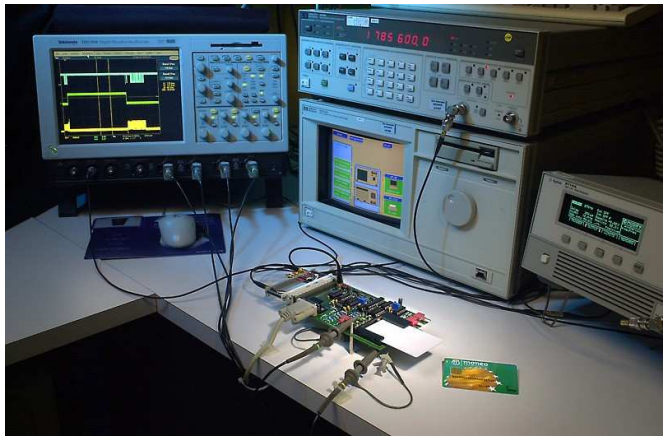
- Moyens lourds en micro-électronique
- Savoir faire sur les cartes à puce
- Aspects multi-compétences
- Stabilité et indépendance du CEA

# Équipement

Micro électronique



Bancs de tests



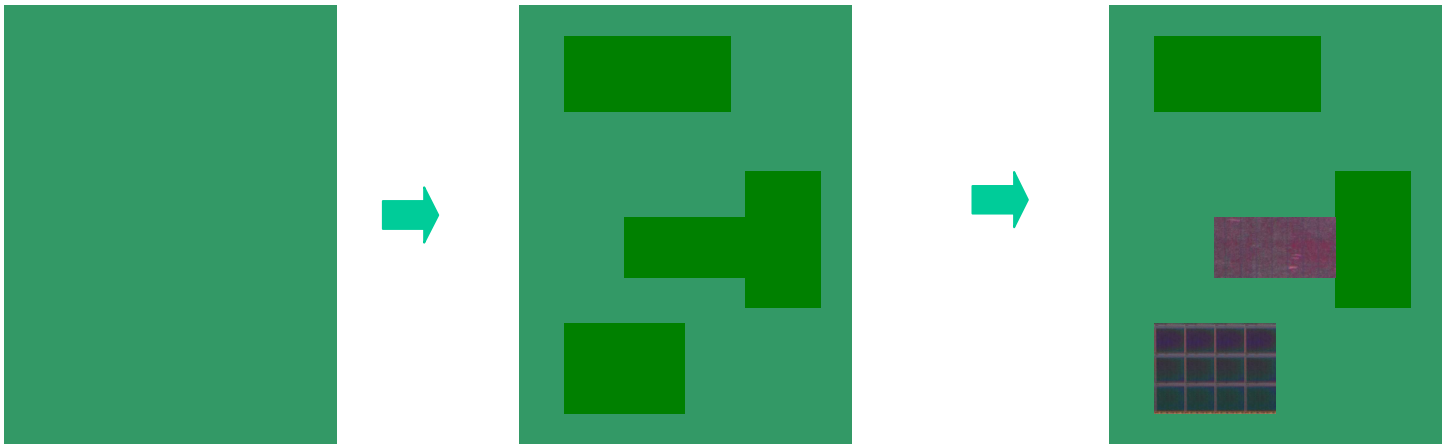
# CESTI LETI

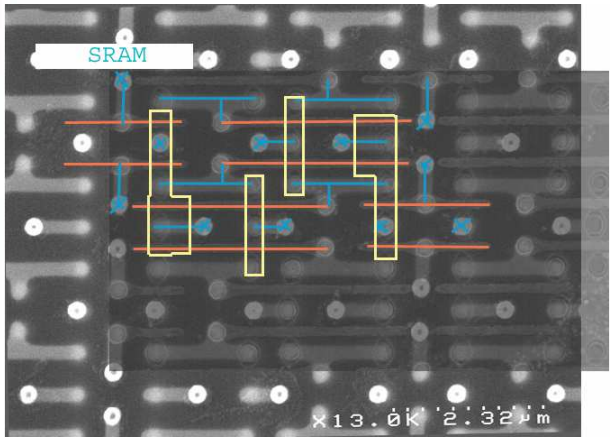
- Crée en 1999
- Personnel
  - 10 permanents
  - 2 doctorants
- Locaux dédiés sécurisés
- Ciblage : excellence technique
  - Circuits intégrés
  - Attaques

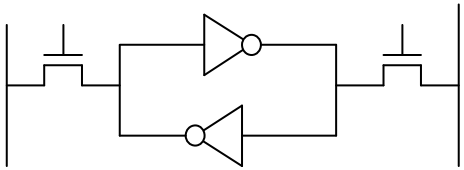
# Compétences (circuits intégrés)

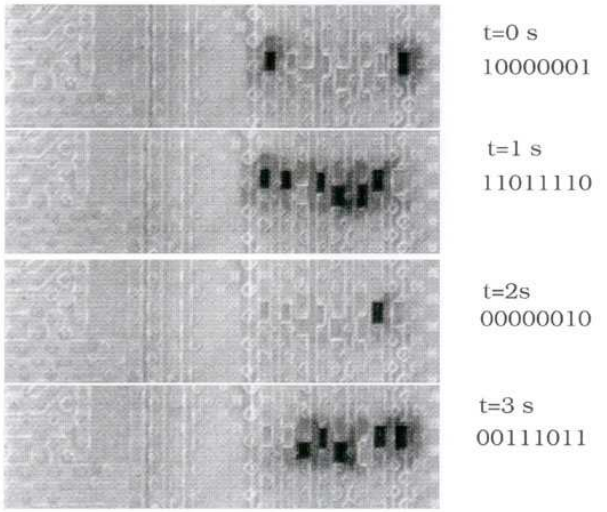
- Analyse interne
  - Préparation (chimie, plasma, polissage)
  - Retro-conception
- Analyse externe
  - Cartographie (laser, EM)
  - Susceptibilité aux perturbations
  - Attaques cryptographiques
- Attaques physiques
  - Modification, probing, extraction de fils

# Déprocessing et rétroconception



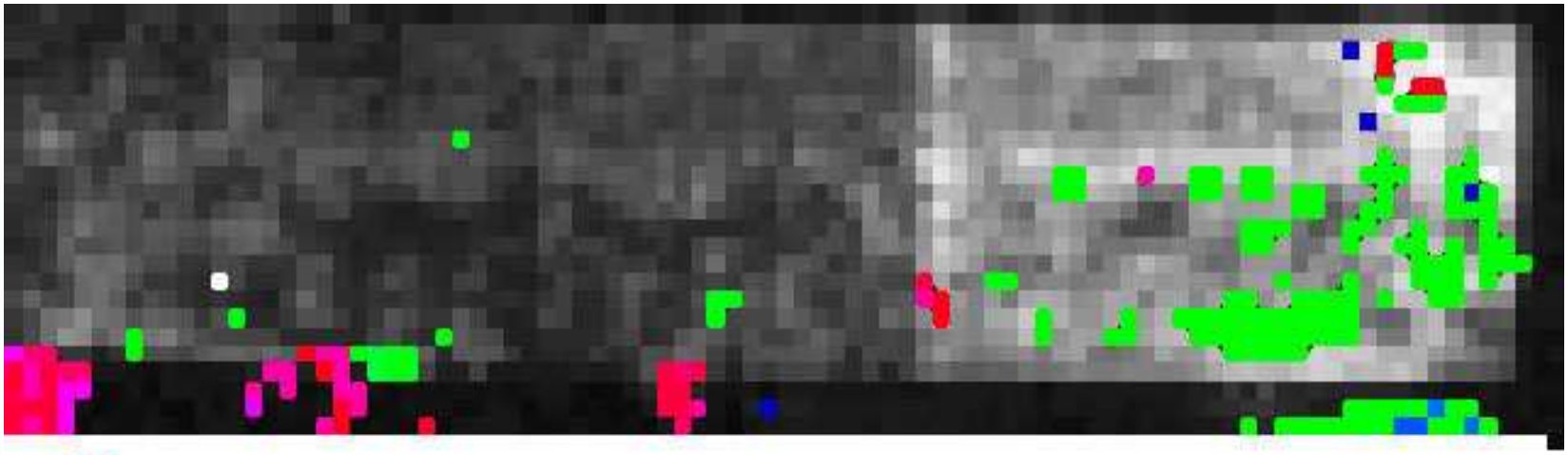





Contraste de potentiel en fonction du temps.

# Cartographie



# Cryptographie embarquée

- Chiffrement de données
- Signature
- Génération de clés
- Échange de clés
- …
  - ➔ Algorithmes symétriques et asymétriques
  - ➔ Générateur de nombres aléatoires

**Sécurité des fonctions cryptographiques ?**

# Sécurité des algorithmes

- Utilisation d'algorithmes sûrs d'un point de vue cryptographique (TDES, AES, RSA, …)

…mais…

- Vulnérabilités du composant
  - Déroutements, modifications de la mémoire
  - Observation de signaux

➔ Attaques physiques

# Attaques par perturbation

- Écrasement de clés
  - La clé devient 0xFF…FF

- Altération de l'algorithme
  - Niveau de sécurité plus faible
  - Differential Fault Analysis
    - Modélisation des fautes
    - Exploitation du calcul erroné
    - ➔Information sur les secrets

# Attaques simples par observation

## SPA/EMA

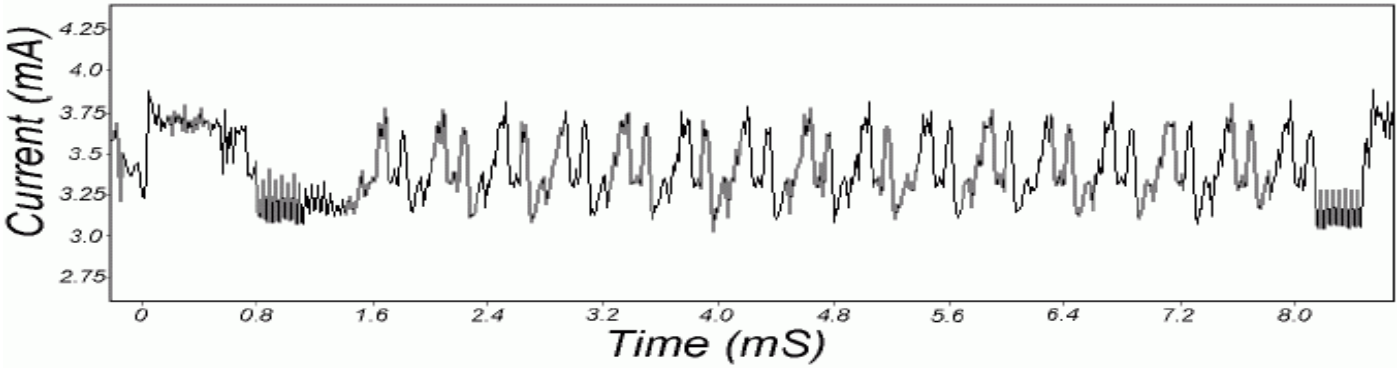



**Figure 1:** SPA trace showing an entire DES operation.

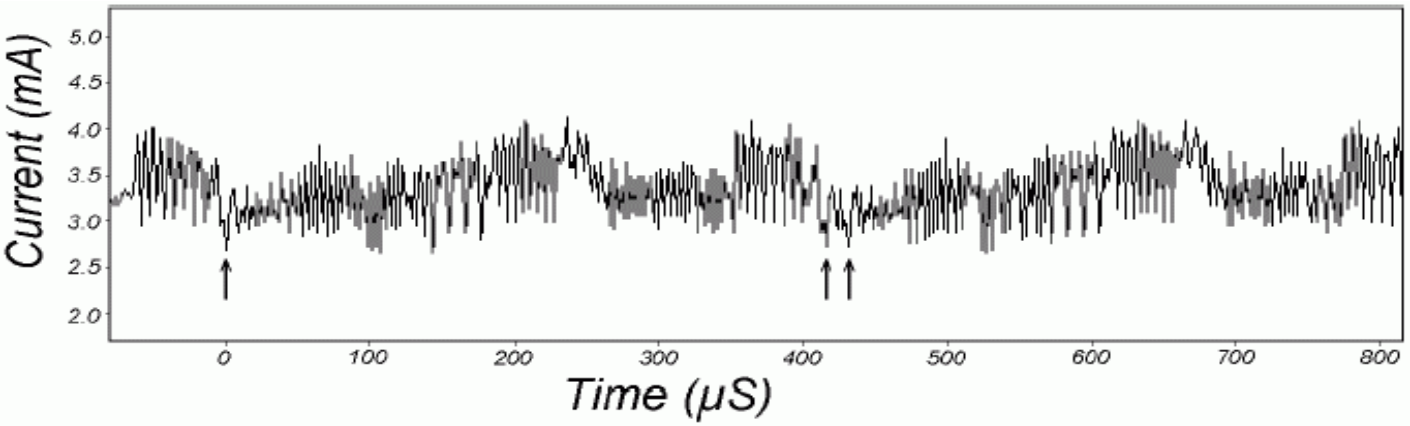


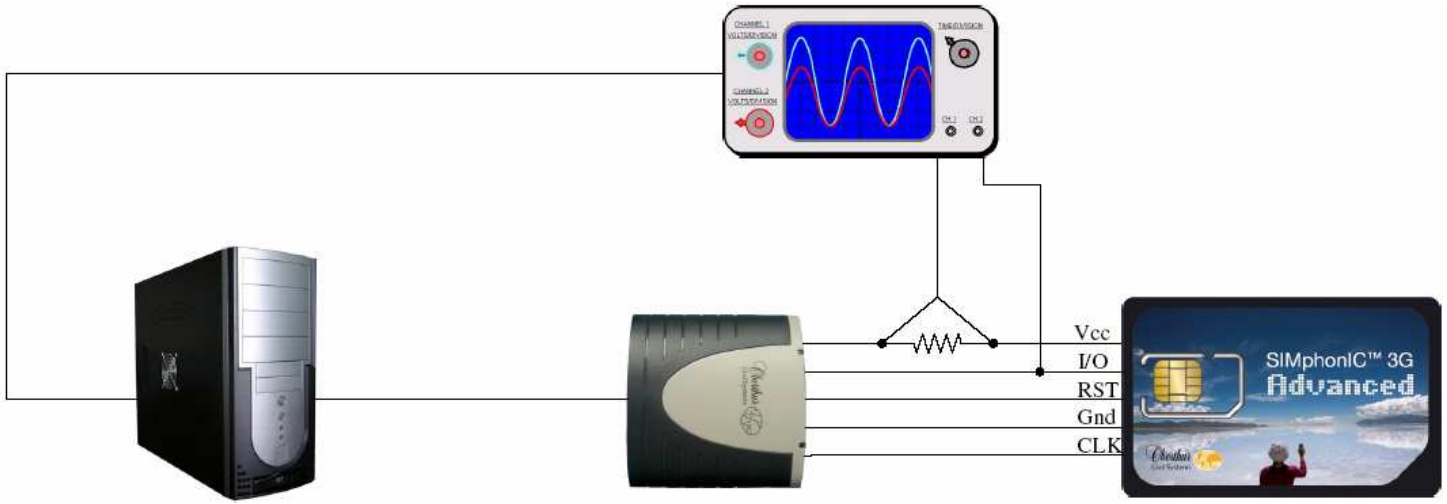

**Figure 2:** SPA trace showing DES rounds 2 and 3.

# Attaques statistiques par observation

DPA/CPA =

Mesure des signaux compromettants

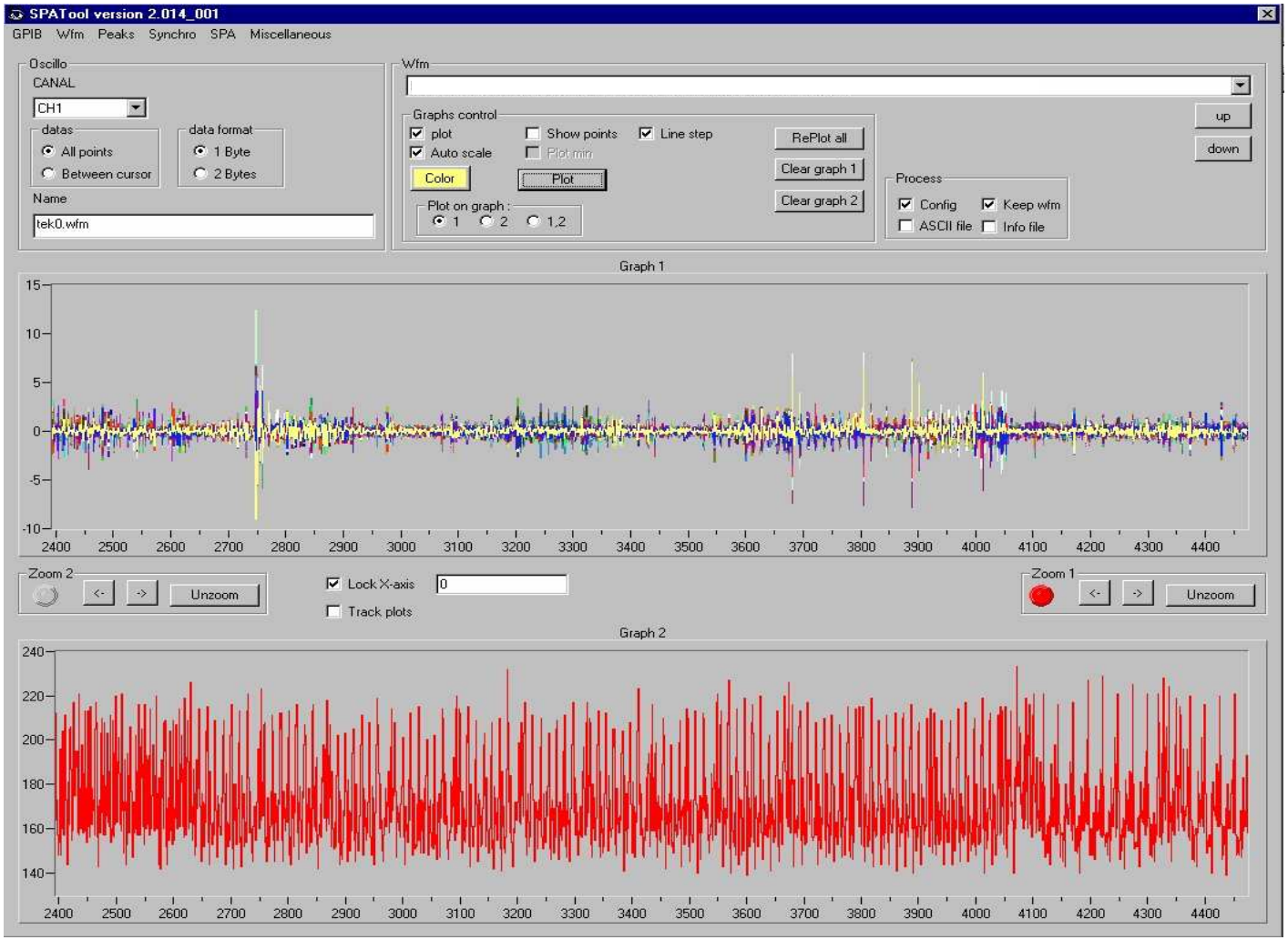
+ Analyse statistique




➔Information sur les secrets

Source: C. Giraud, *Attaques de cryptosystèmes embarqués et contre-mesures associées*, rapport de thèse - 2007

# Attaques statistiques par observation



# Sécurité des générateurs d'aléas

- Générateur physique
  - ➔ Tests statistiques
- Retraitement algorithmique
  - ➔ Étude cryptographique

# Travaux de recherche en cours

- Évaluation / tests
  - Adaptation des attaques connues à d'autres algorithmes :
    - courbes elliptiques
    - algorithmes propriétaires
  - Étude des contre-mesures propriétaires
- ODYSSEE - projet ANR
  - Algorithmes de chiffrement par flots

# Thèses en cours

- Berzati Alexandre
  - Analyse cryptographique des altérations d'algorithme
- Canivet Gaëtan
  - Implémentation d'algorithmes cryptographiques sur FPGA et vulnérabilités associées


# Merci de votre attention

leti

MINATEC

INSTITUT CARNOT CEA LETI

cea