THALES

EMA DEMA vs SPA DPA : Avantages et inconvénients

Plan

- Introduction
- Quelques Rappels
- Setup
- SEMA
- DEMA

Introduction

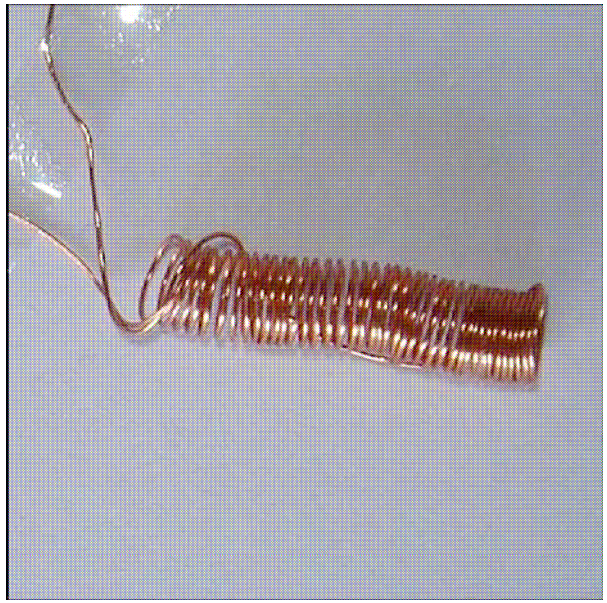
- Fin des années 90 : apparition des Sides Channel Attacks (Kocher & Al)

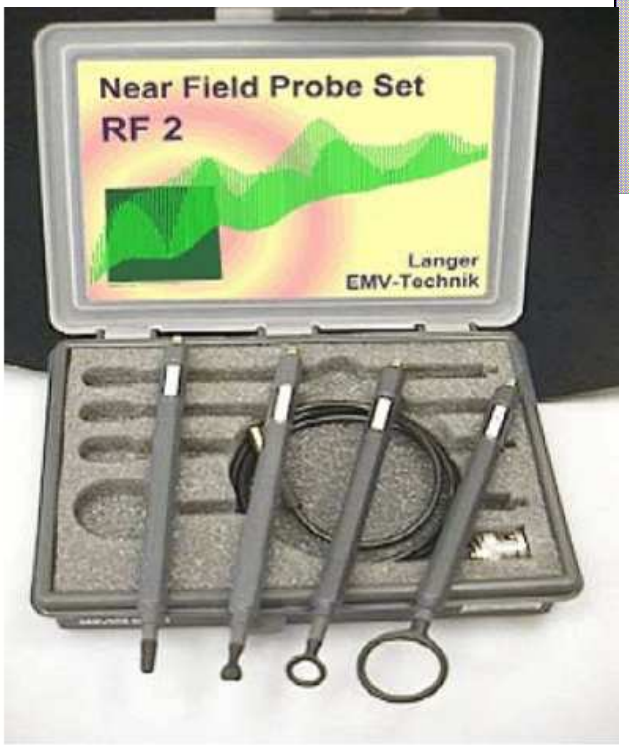
- Début des années 2000 : Introduction de l'EMA
  - J.J. Quisquater et D Samyde « a new tool for non intrusive analysis of smart cards based on electro-magnetic emissions, the SEMA and DEMA methods » Presented at the rump session of EUROCRYPT'2000
  - K. Gandolfi, C. Mourtel et F. Olivier «Electromagnetic Analysis : Concrete Results » CHES 2001

Principe

- Tout mouvement de porteur s'accompagne d'une émission de champ électromagnétique.
  - Champ électrique proportionnel au courant
  - Champ magnétique proportionnel aux variations de courant.
- Meilleurs résultats sur circuits type carte à puce : mesures du champ magnétique

Les détecteurs :



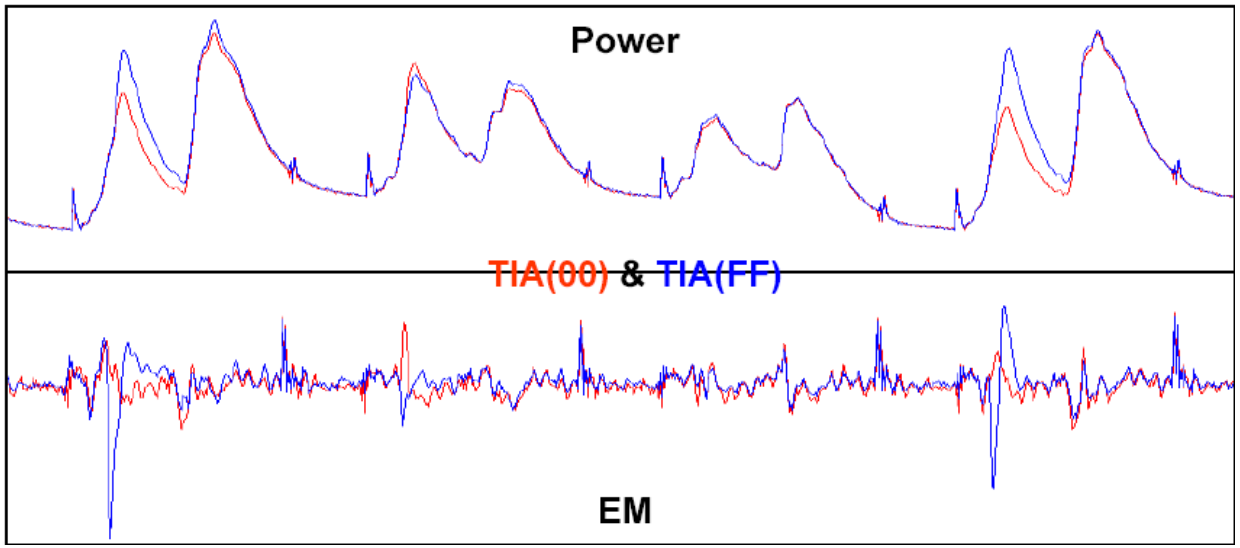


La chaîne d'acquisition :

- PB champ magnétique très faible => signal de mesure très faible
- Nécessité d'amplifier le signal au plus prêt de la source pour diminuer le bruit (amplificateur large bande faible bruit)
- Possibilité de trouver des détecteur avec amplificateur intégré.
- Numérisation du signal avec un oscilloscope numérique ou une carte d'acquisition

•Avantages :

- Bande passante plus élevée
- Possibilité d'avoir une information locale
- Plus grande sensibilité

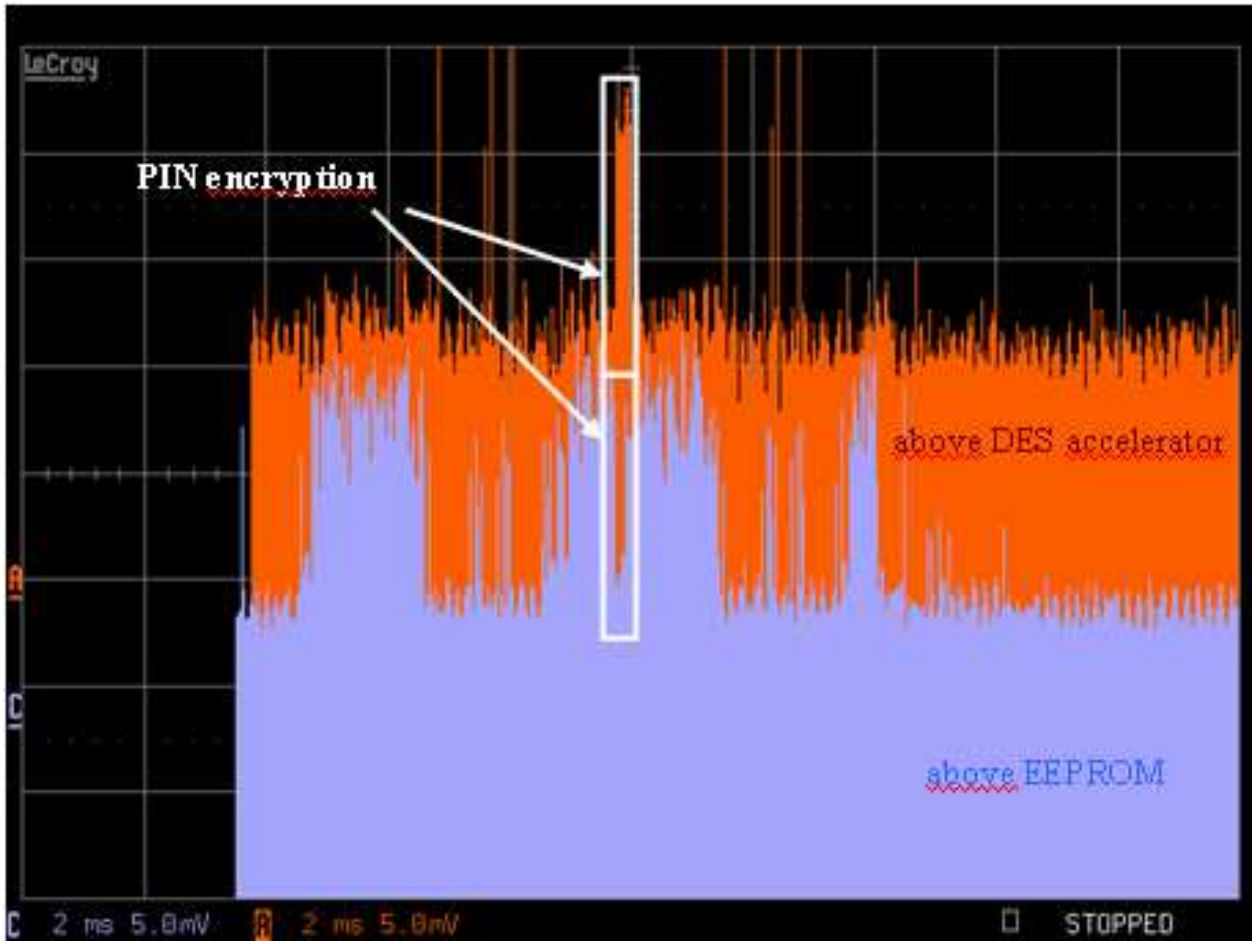


Localisation

Informations très différentes en fonction

- De la région mesurée
- Des dimensions de la sonde
- De l'orientation de la sonde
- De la hauteur de mesure
- …

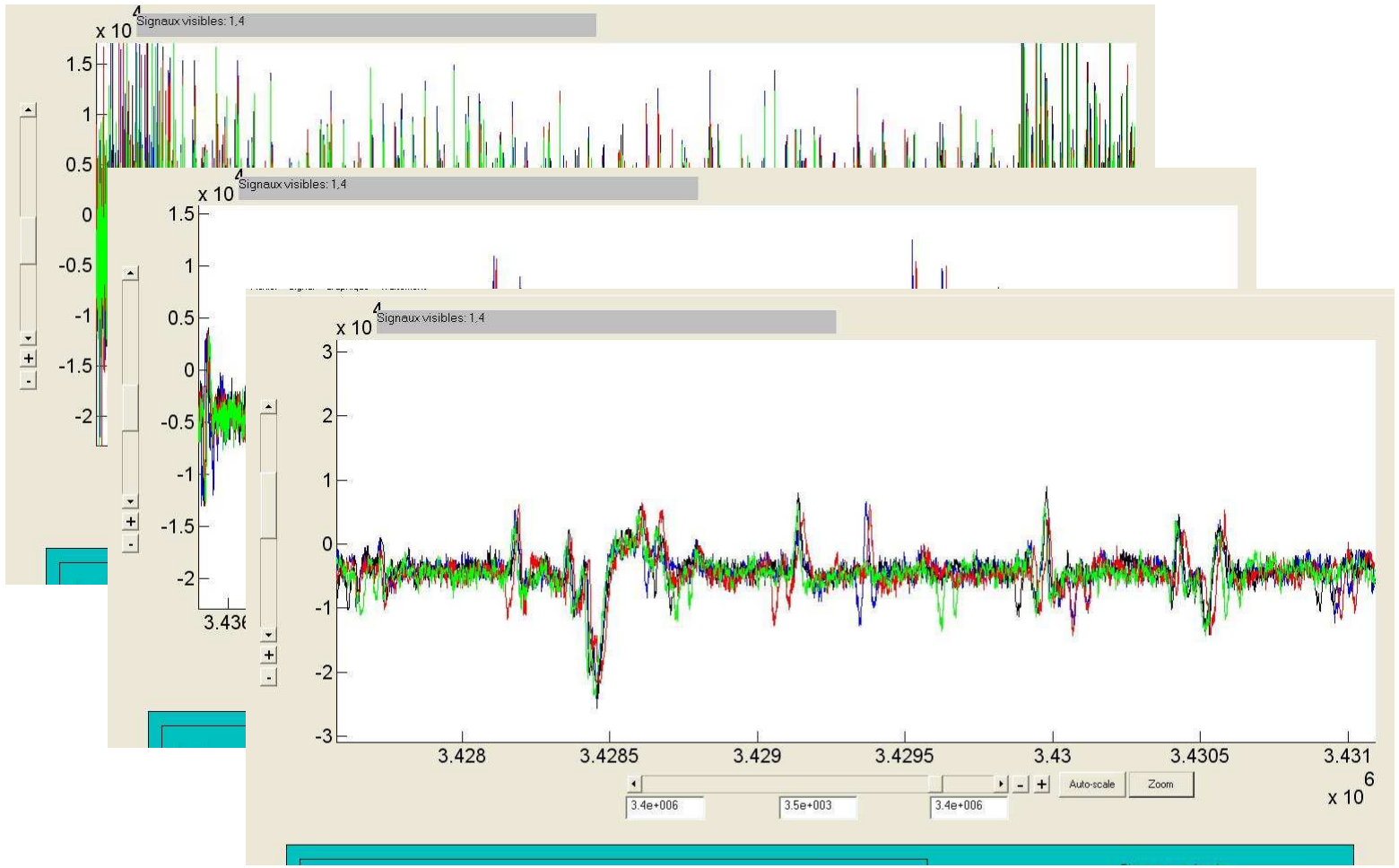
Localisation d'un crypto processeur



QUESTION : Comment trouver les meilleures conditions d'acquisition

- Signal le plus fort
- Différences les plus significatives
- …

Zoom sur les différences

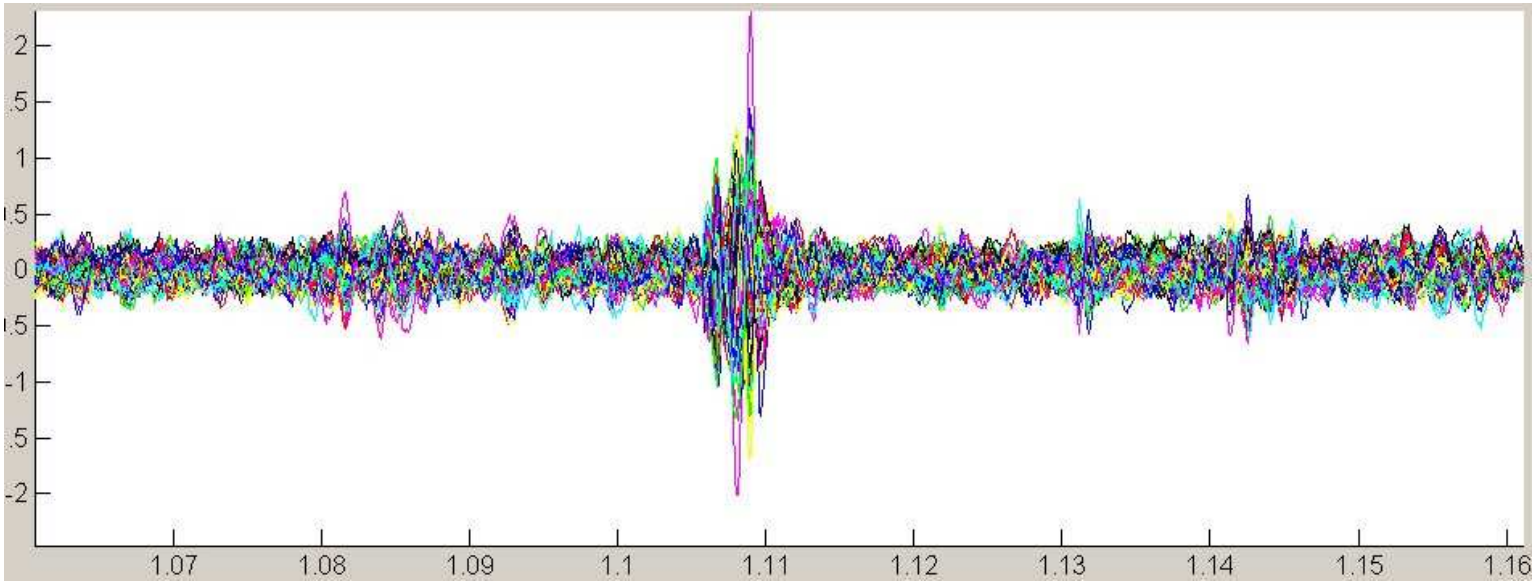


Mêmes problèmes que pour la SEMA :

- Comment choisir la meilleure sonde ?
  - Taille
  - Orientation
- Comment trouver la meilleure position ?
  - Maximise le signal
  - Maximise les différences
  - Autres traitement : WGMSI (Weighted Global Magnitude Squared Incoherence)

- Même principe que pour les analyses en courant avec mêmes outils

- Possibilité d'optimiser en appliquant le switching distance model de Eric Peeters, François-Xavier Standaert, Jean-Jacques Quisquater.



Conclusion

Analyses Electro-magnétiques :

- Plus riches que la simple analyse en courant
- Pas besoin d'accès direct (intérêt pour les mesures sur cartes FPGA, Processeurs …)
- Plus complexe (plus de degrés de liberté)