Attaques sur les ressources cryptographiques

DGA Maîtrise de l'information

F.VALETTE

Plan

- Quelques attaques sur les ressources cryptographiques:
  - Les canaux auxiliaires
  - L'injection de faute
- Quelques contre-mesures
  - Les protections génériques
  - Les protections spécifiques
- Des problématiques

Les attaques sur ces composants

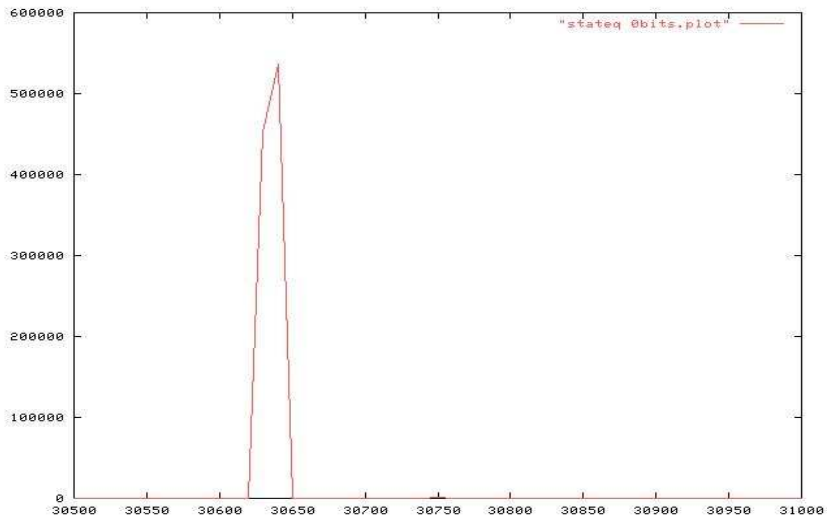
- Attaques intrusives
  - Attaques par observation :
    - MEB, AFM, …
    - Retro-conception partie hardware
    - Relecture de mémoire (ROM, ...)
  - Attaques par modification
    - FIB, …
    - Probing, …
- Attaques non intrusives
  - Attaques logicielles :
    - Détournement de commande
    - Débordement de mémoire…
  - Attaques par canaux auxiliaires
  - Attaques par fautes

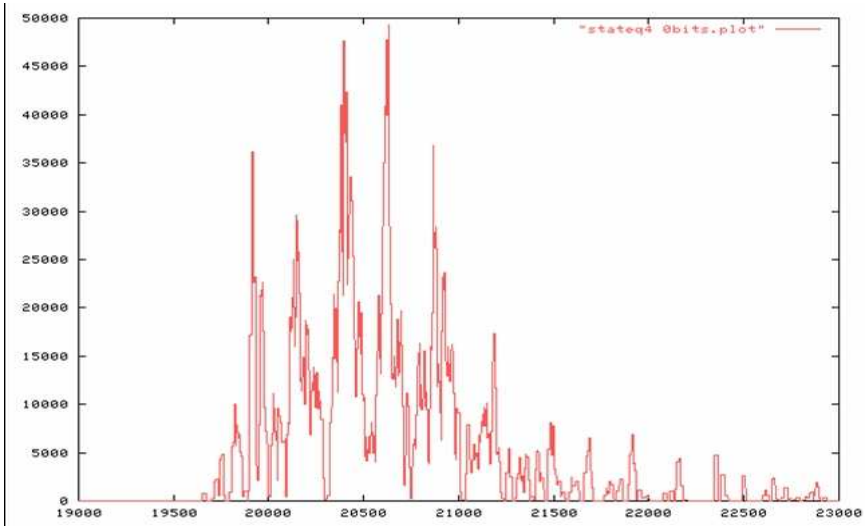
Les attaques par canaux auxiliaires

- Les sources d'informations
  - Le temps de calcul
    - Information globale
    - Profilage temporel parfois possible (hyperthreading)
  - La consommation de courant
    - Bande passante ~ centaine de Mhz
    - Information globale sur le fonctionnement du composant
  - Le rayonnement électromagnétique
    - Bande passante ~ qq Ghz
    - Profilage spatial
  - L'émission de photons
    - …

Temps de calcul

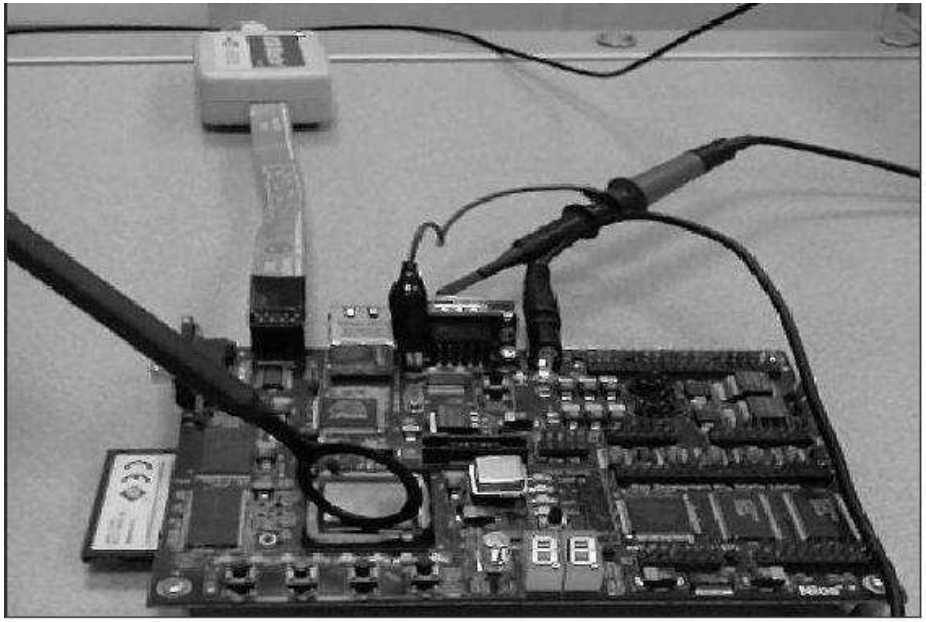
- AES implémenté en logiciel sur P3 et P4
  - Temps constant « au niveau assembleur »
  - Effet des optimisations hardware du processeur





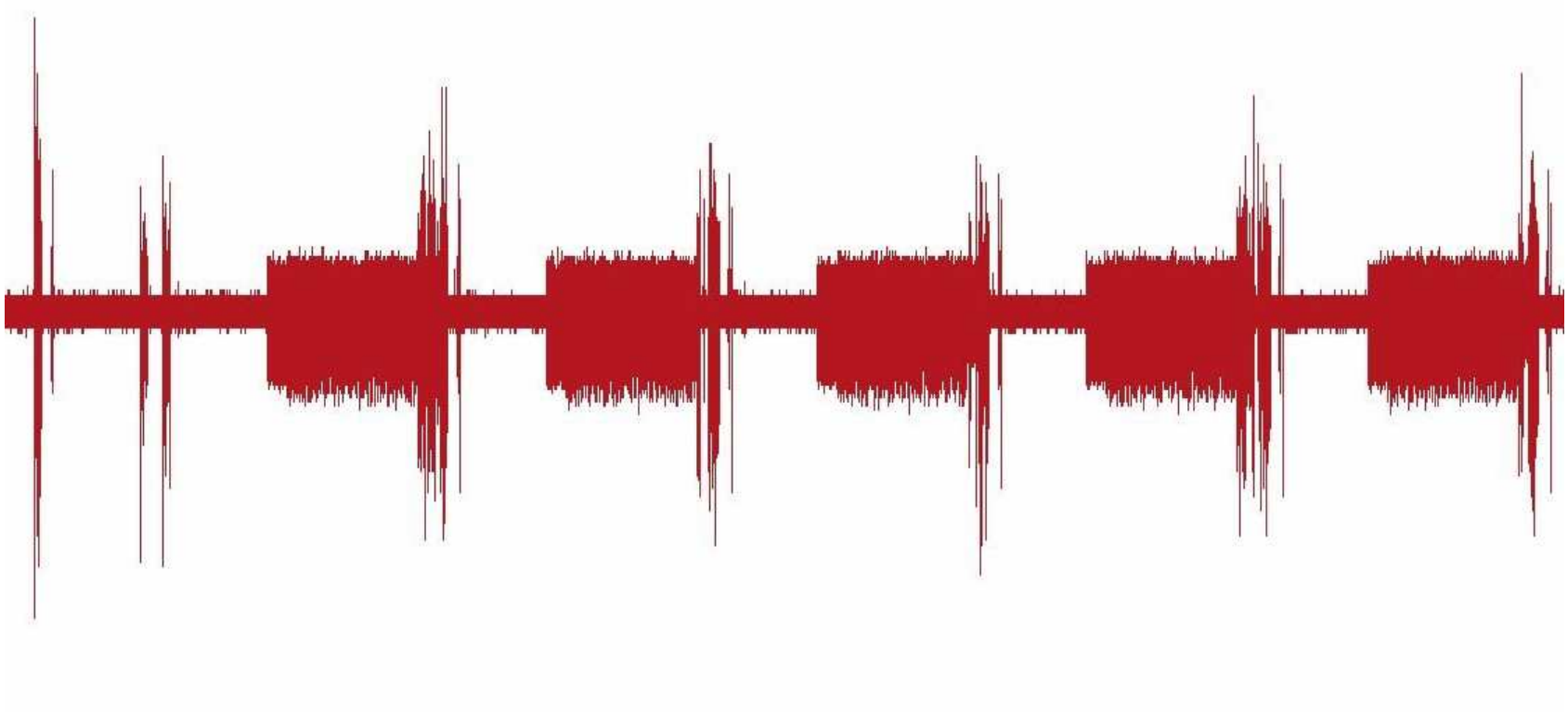
Mesure de courant / Rayonnement électromagnétique global

- Comparaison courant / EM
  - Bande passante
    - Basse -> courant
    - Elevée -> EM
  - Facilité de mise en œuvre
    - EM
- Exemple de mise en œuvre



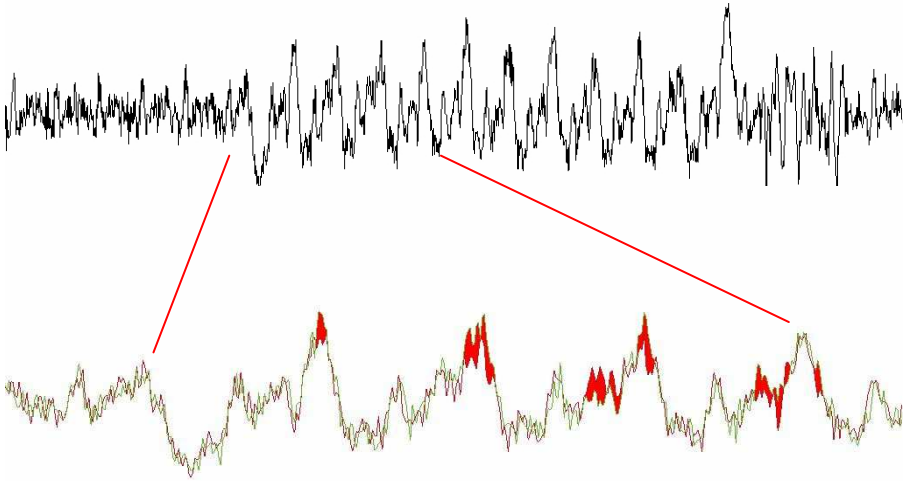
Exemple de mesure EM globale

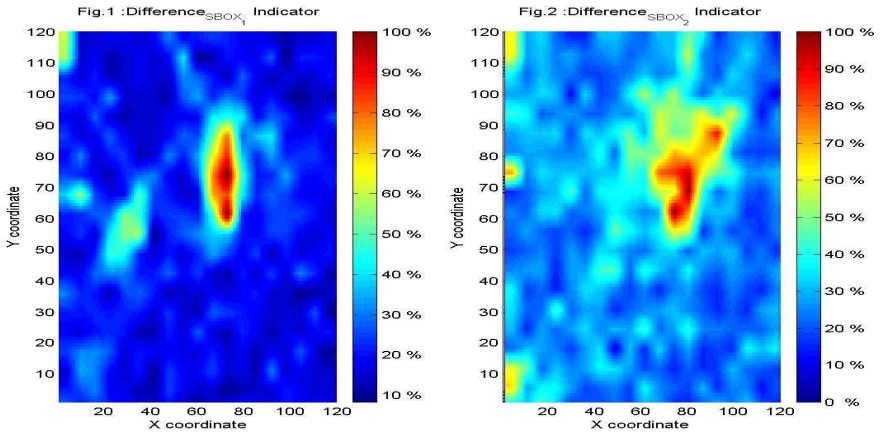
- HMAC implémenté en logiciel sur NIOS sur STRATIX



Rayonnement EM localisé

- AES implémenté en Hardware sur STRATIX
  - En haut : 1 mesure d'un chiffrement complet
  - En bas : zoom sur 2 mesures avec des messages différents en entrée de l'AES
- Exemple de cartographie :
  - Image 20x20 du FPGA
  - Différence entre deux mesures réalisée en chaque point.



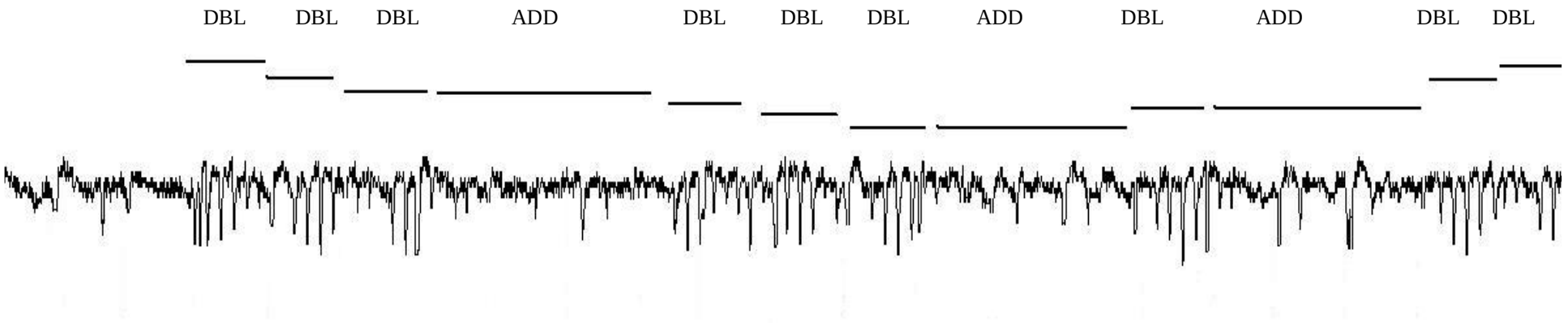


Les méthodes d'exploitation

- Deux techniques :
  - Par comparaison :
    - Simple Power Analysis, Collision Attacks, Template Attacks…
  - Par distingueur :
    - Differential Power Analysis, Correlation Power Analysis, DPA d'ordre supérieur…
    - DEMA, CEMA,...

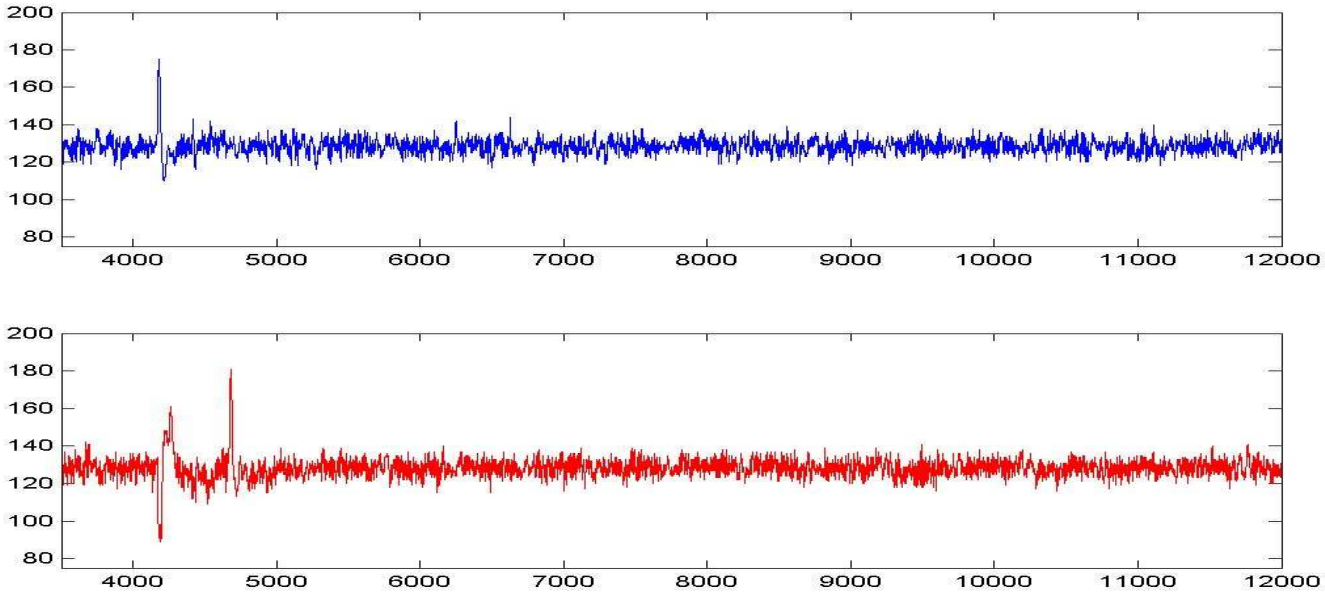
Exemple d'attaque SEMA

- Mesure EM globale d'un produit scalaire sur courbe elliptique
- Bande passante du signal réduite à qq dizaines de Mhz



Exemple de distingueur CEMA

- Distingueur en canaux auxiliaires:
- Fonction qui dépend :
  - Paramètres de la fonction crypto (entrée, …)
  - Mesures effectuées
- Qui permet de distinguer deux composants
  - Le premier contenant l'implémentation visée
  - Le second contenant la même implémentation mais avec des entrées aléatoires (clef + message).
- Ex de distingueur CPA sur les entrées d'un Feistel :
  - En haut partie gauche
  - En bas partie droite



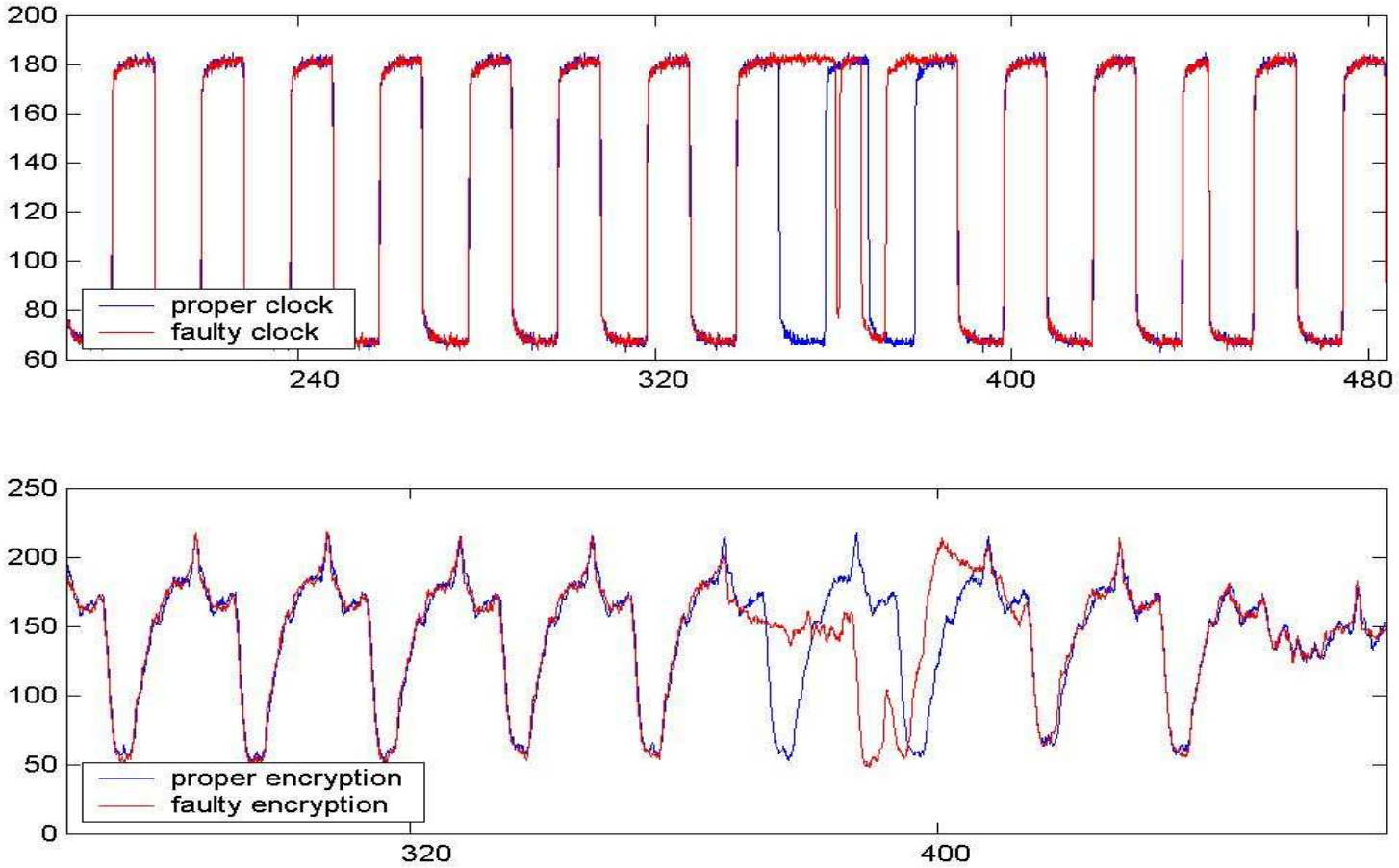
Transformation d'un distingueur en cryptanalyse

- Technique classique en cryptanalyse de chiffrement par bloc :
  - Hypothèse : un distingueur sur n-1 tours :
    - Entrées+ sorties + valeurs intermédiaires au tour n-1
  - Attaque sur n tours :
    - Deviner une partie de la sous clef du dernier tour
    - Calculer les valeurs intermédiaires au tour n-1
    - Calculer l'indicateur associé à cette valeur de sous-clef
    - Identifier pour quelle sous-clef le distingueur fonctionne. (Pour les mauvaises clefs, il ne fonctionne pas)
  - Permet de retrouver une partie de la sous-clef
- Même technique utilisée en canaux auxiliaires :
  - Construire un distingueur :
    - À partir des données de l'algorithme (sortie premier tour ou entrée dernier tour par exemple)
    - Prenant en compte l'implémentation (modélisation du lien implémentation / mesure réalisée)
  - Deviner les bits de clef et calculer le distingueur

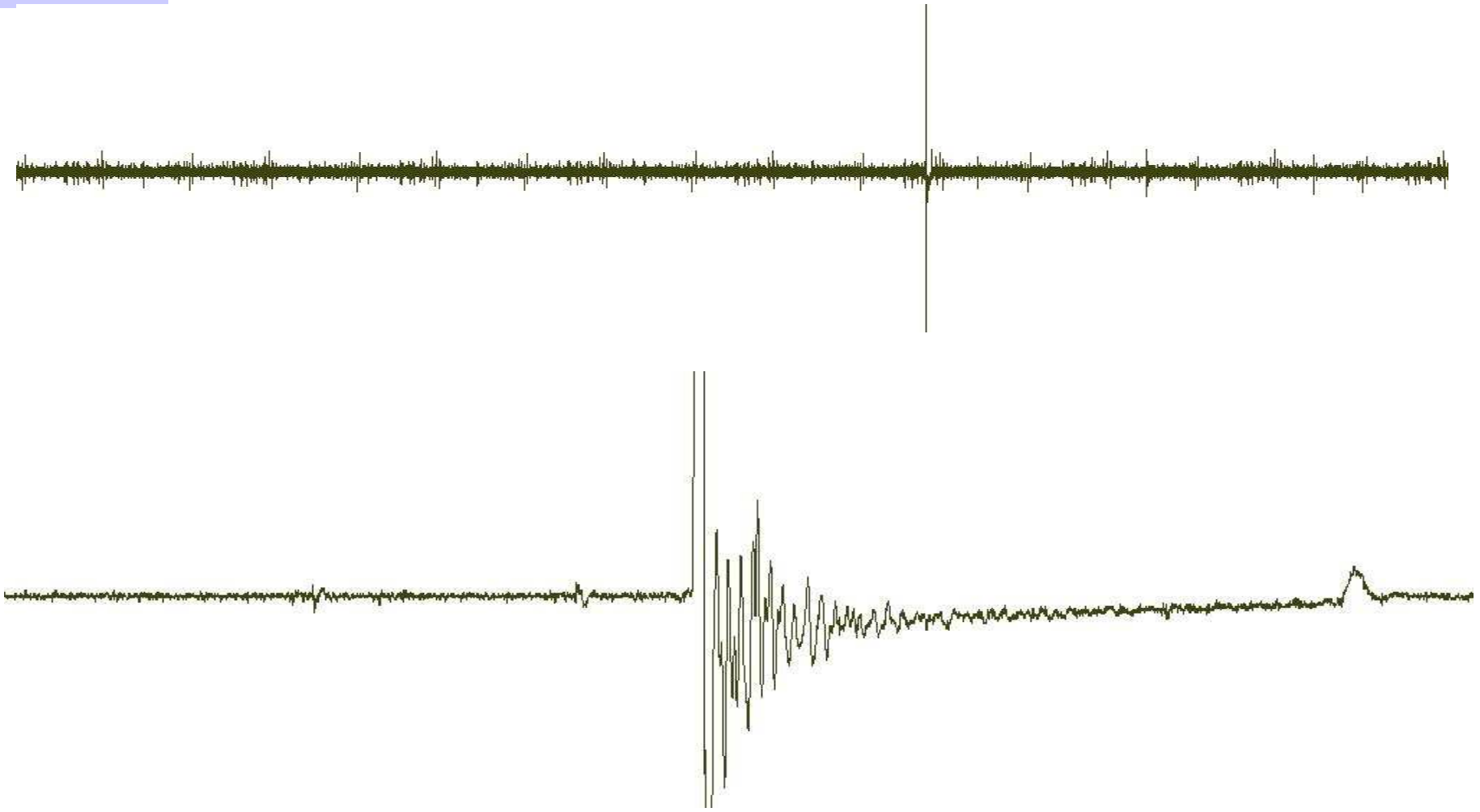
Attaques par fautes

- Méthodes d'injection
  - Horloge :
    - Accélérer l'horloge sur un ou deux cycles
    - Effet global
  - VCC
    - Surtension/sous-tension
    - Effet global
  - Laser :
    - Apport d'énergie par un faisceau laser
    - Effet local qui dépend de la taille du spot laser
    - Préparation du composant nécessaire
  - EM :
    - Injection d'une impulsion électromagnétique de courte durée
    - Effet local
  - ...
- Effet des fautes :
  - Transitoire généralement
  - Rémanent : modification configuration d'un FPGA par exemple

Exemple de fautes sur l'horloge



Exemple d'injection EM

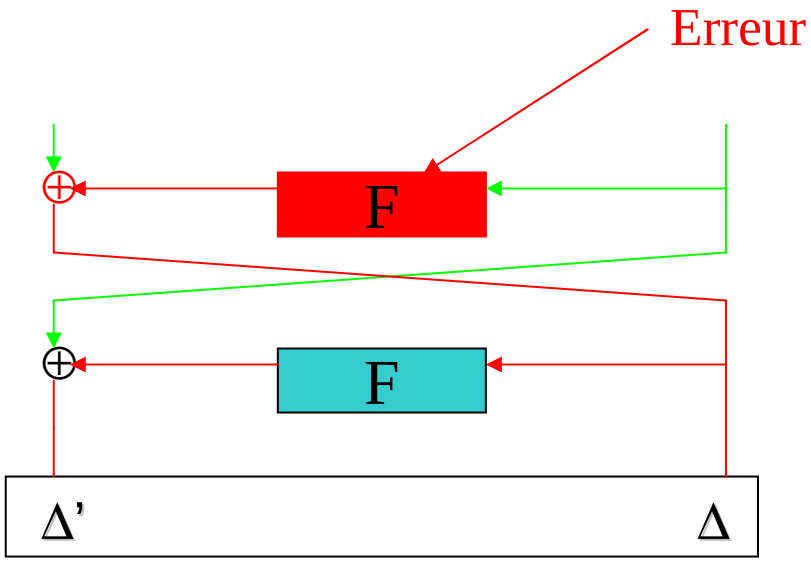


Attaques par faute : exploitation des résultats

- Deux techniques :
  - Par comparaison avec un résultat correct (obtenus sur le composant ou calculé)
    - Differential Fault attack
    - Attaque sur le RSA –CRT
  - En utilisant uniquement le fait que le résultat soit fauté :
    - Safe errors
    - Differential Behavior Analysis

DFA sur le DES

- Application pratique de la cryptanalyse différentielle sur le DES



Les contre-mesures

- Deux grandes familles de contre-mesures :
  - Génériques
  - Spécifiques à un algorithme
- Efficacité des contre-mesures :
  - Combinaison de plusieurs techniques souvent nécessaire
  - Effets collatéraux possible :
    - Protection qui engendre de nouvelles attaques, ex:
      - CRC sur la mémoire de clef pour éviter les fautes peut permettre de faire une attaque par canaux auxiliaires sur cette zone
- Coût :
  - Approximativement un facteur 2 en temps ou en place
  - Cryptographie symétrique et asymétrique se comportent différemment

Les contre-mesures génériques

- Canaux auxiliaires :
  - Désynchronisation :
    - Ajout de délai aléatoire
    - Alternance des calculs avec la clef et des « fausses clefs »
  - Diminution du rapport signal / bruit
    - Équilibrage : précharge, dual rail, asynchrone,...
    - Génération de bruit en parallèle des calculs à protéger
- Faute :
  - Détecter la conséquence :
    - Redondance temporelle ou spatiale
    - Utilisation code correcteur
  - Détecter la cause
    - Capteurs de lumière
    - Capteur de surtension ...

Les contre-mesures spécifiques

- Canaux auxiliaires :
  - Protection contre la SPA en équilibrant tous les chemins
    - Ex : sur courbe elliptique, on fait systématiquement une addition entre deux doublements
  - Techniques de masquage sur les algorithmes symétriques :
    - Au lieu de manipuler A, on manipule A⊕R et R
    - Très coûteux pour passer d'une opération à une autre
  - Technique de masquage sur les algorithmes asymétriques :
    - Utiliser les propriétés des objets manipulés pour rendre les calculs aléatoires
    - Ex :
      - pour calculer $M^d \bmod N$,
      - on calcule $((M.A^e)^{d+ B.\varphi(N)} /A) \bmod N$ où A et B sont des nombres aléatoires
    - Peu coûteux
- Fautes :
  - Utilisation de la fonction inverse :
    - Ex pour le RSA:
      - On calcule $S=M^d \bmod N$ et on vérifie que $M=S^e \bmod N$
  - Intéressant si la fonction inverse :
    - est différente de la fonction
    - est plus rapide que la fonction

Quelques problématiques

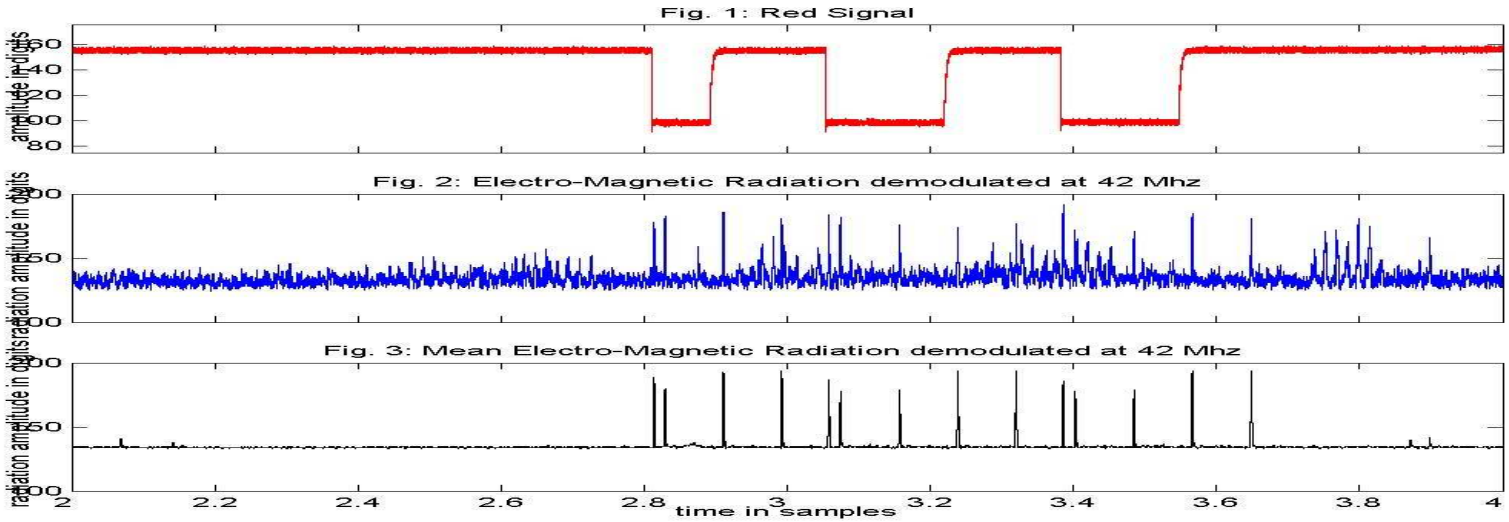
- La génération d'aléa
- Les attaques à distance
- SCARE

Génération d'aléa

- Conception respectant les critères définis par l'ANSSI
  - Modèles théoriques pour le générateur physique
    - Aspect qualitatif (entropie) plus que quantitatif (débit)
  - Retraitements prouvés et performants
- Attaques :
  - Sur la génération physique
    - Cf CHES 2009
  - Sur le retraitement

Les attaques à distance

- Attaques de type SEMA :
  - Exemple : signal clavier modulant une porteuse à 42Mhz
- Mener des attaques de style DEMA, CEMA à plusieurs mètres :
  - synchronisation
  - Bruit
  - Bande passante



SCARE

- Rétro-conception par canaux auxiliaires :
  - dans le cas d'algorithmes cryptographiques propriétaires
  - Dans le cas de code embarqué inconnu
- Protections :
  - Utilisation de protection allégées contre les canaux auxiliaires

Dispositifs DGA

- Appels d'offre :
  - Code des marchés publics
- Dispositifs d'aide à l'innovation :
  - REI
  - RAPID
- Thèse DGA
  - Financement de bourses de thèse pour des sujets intéressant la DGA