A PRACTICAL GUIDE TO DIFFERENTIAL POWER ANALYSIS OF USIM CARDS

ANSSI/SDE/ST/LS{C,F}

CONTEXTE

- Black Hat 2015 : article « Small Tweaks do Not Help… »
  - Attaque de MILENAGE (authentification 3G/4G)
- Extraction des secrets d'authentification de cartes USIM
  - Attaque par canaux auxiliaires sur MILENAGE
  - Suppose la connaissance du code PIN
- Conséquences :
  - Capture passive et déchiffrement du trafic de l'abonné
  - Usurpation du réseau auprès de l'abonné (attaque de homme du milieu)
  - Usurpation de l'abonné auprès du réseau

SCÉNARIO

- Vol du téléphone portable de l'abonné ciblé
- Hypothèse : code PIN trivial (0000/1234) ou désactivé
  - En France : trois opérateurs sur quatre offrent des cartes avec PIN trivial
- Extraction des secrets de la carte USIM par l'attaquant
  - Attaque par corrélation de la consommation de courant
- Restitution du téléphone à l'abonné

OBJECTIFS

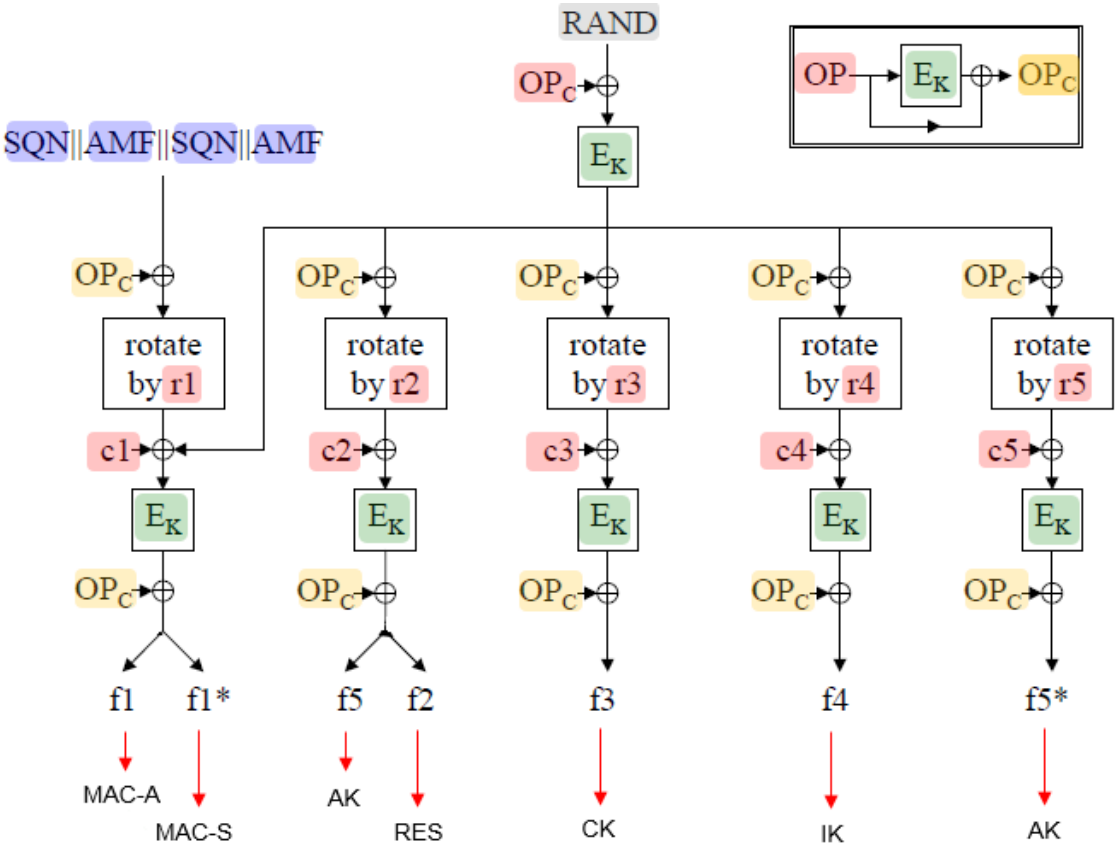
- Reproductibilité des résultats précédents
- État des lieux : existe-t'il des modèles français vulnérables ?
- Etablir le niveau de difficulté de l'attaque
  - Combien de temps pour extraire les secrets ?
  - Quels moyens matériels/logiciels ?

RÉSULTATS

- 9 cartes USIM testés (dont 5 françaises)
  - Travail se poursuivant sur plus de cartes
- 1 carte vulnérable identifiée
  - Implémentation standard de MILENAGE (AES-128)
  - Entité concernée notifiée en janvier 2018
- Les diapositives suivantes présentent son attaque

MILENAGE

Ek = AES-128

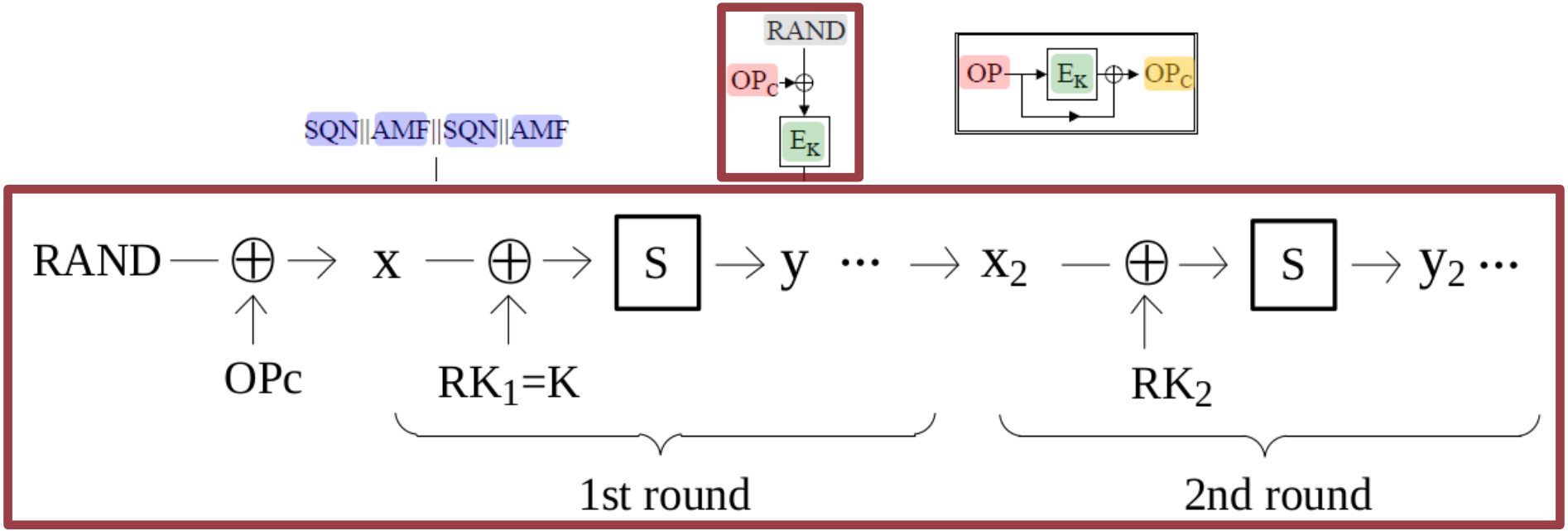


L'attaquant contrôle RAND

L'attaquant cible K et OPc

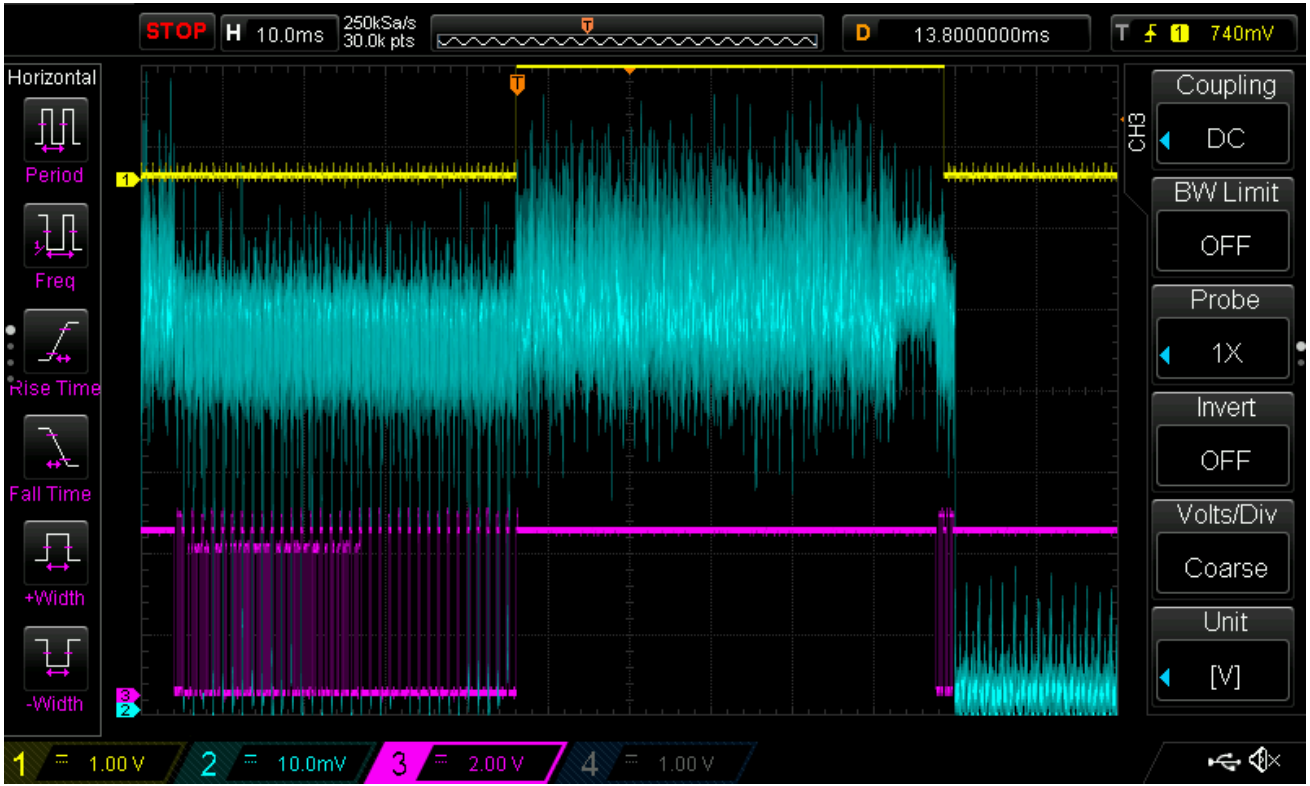
Source : sharetechnote.com

MILENAGE



Source :
https://ubm.io/1IRRhqX

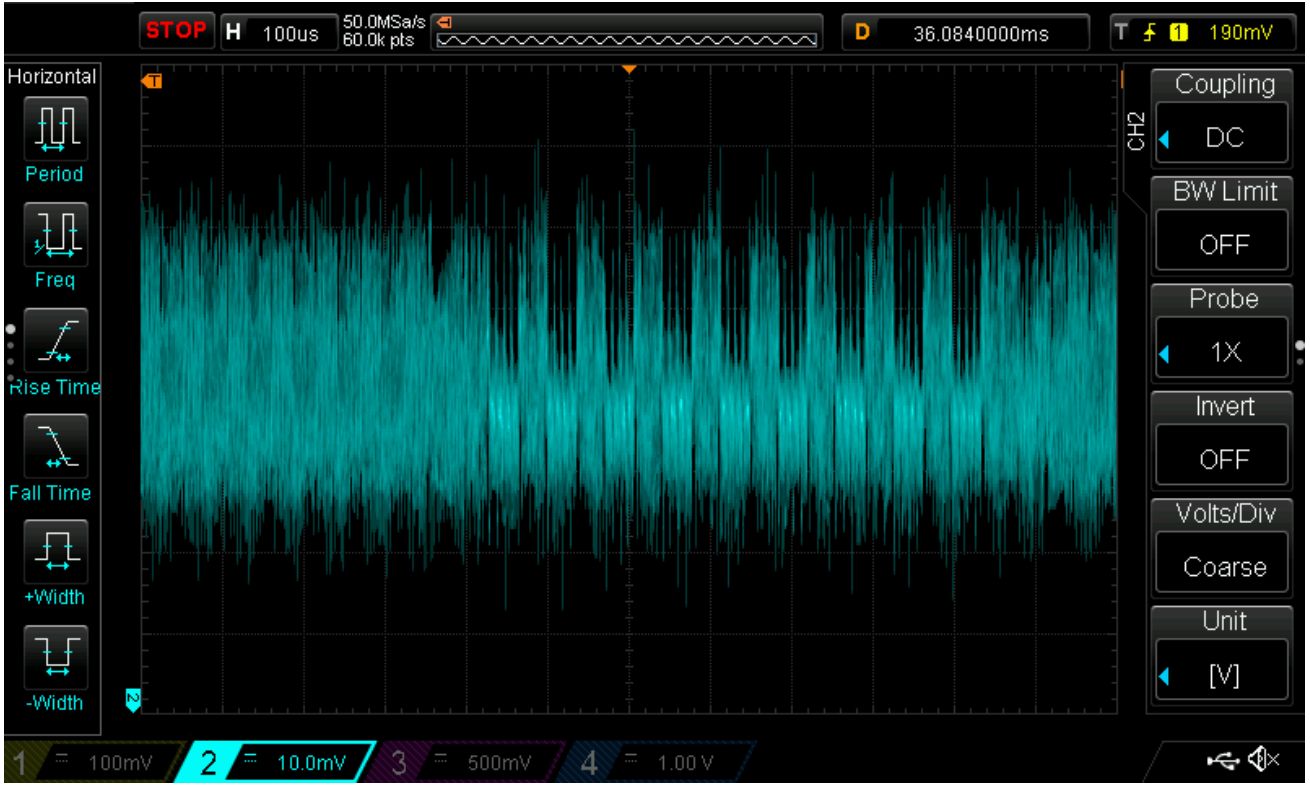
VUE D'ENSEMBLE



ZOOM 20X


STOP
H 500us
10.0MSa/s
60.0k pts
D 38.4200000ms
T 188mV
Horizontal
Period
Freq
Rise Time
Fall Time
+Width
-Width
CH2
Coupling
DC
BW Limit
OFF
Probe
1X
Invert
OFF
Volts/Div
Coarse
Unit
[V]
1 100mV
2 10.0mV
3 500mV
4 1.00 V

ZOOM 100X


STOP
H 100us
50.0MSa/s
60.0k pts
D 36.0840000ms
T 190mV
Horizontal
Period
Freq
Rise Time
Fall Time
+Width
-Width
CH2
Coupling
DC
BW Limit
OFF
Probe
1X
Invert
OFF
Volts/Div
Coarse
Unit
[V]
1 100mV
2 10.0mV
3 500mV
4 1.00 V

ZOOM 1000X


STOP
H 10.0us
250MSa/s
60.0k pts
D 35.9280000ms
T 190mV
Horizontal
Period
Freq
Rise Time
Fall Time
+Width
-Width
CH2
Coupling
DC
BW Limit
OFF
Probe
1X
Invert
OFF
Volts/Div
Coarse
Unit
[V]
1 100mV
2 10.0mV
3 500mV
4 1.00 V

CAPTURE DES TRACES

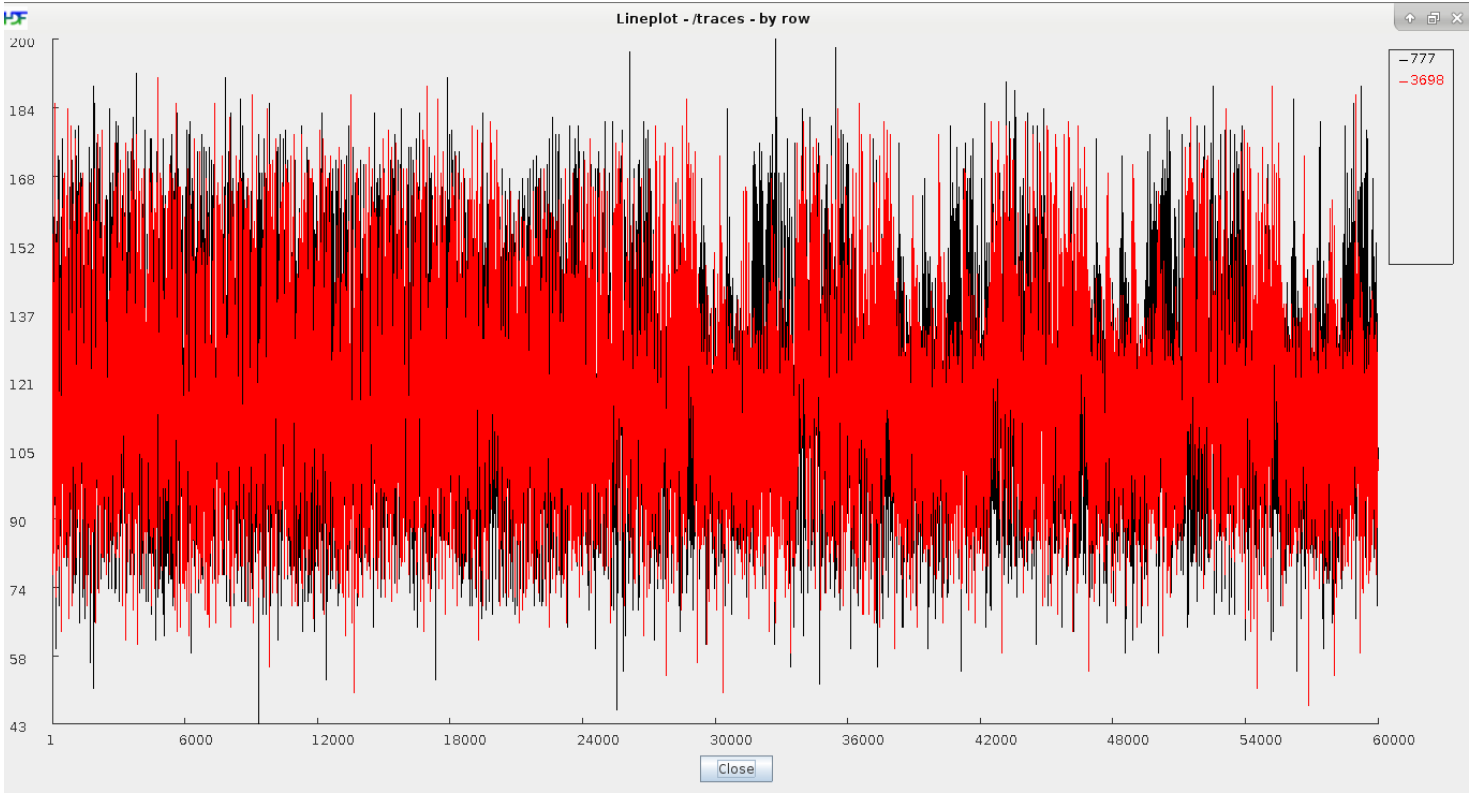
- Problème du bruit
  - Interférences radio : GSM, Bluetooth, CPL, etc.
    - Solutions : cage de Faraday / éloignement des sources d'émission
  - Interférences venant du PC de mesure
    - Solutions : optocoupleur / filtrage / changement de PC

DÉROULÉ DE L'ATTAQUE

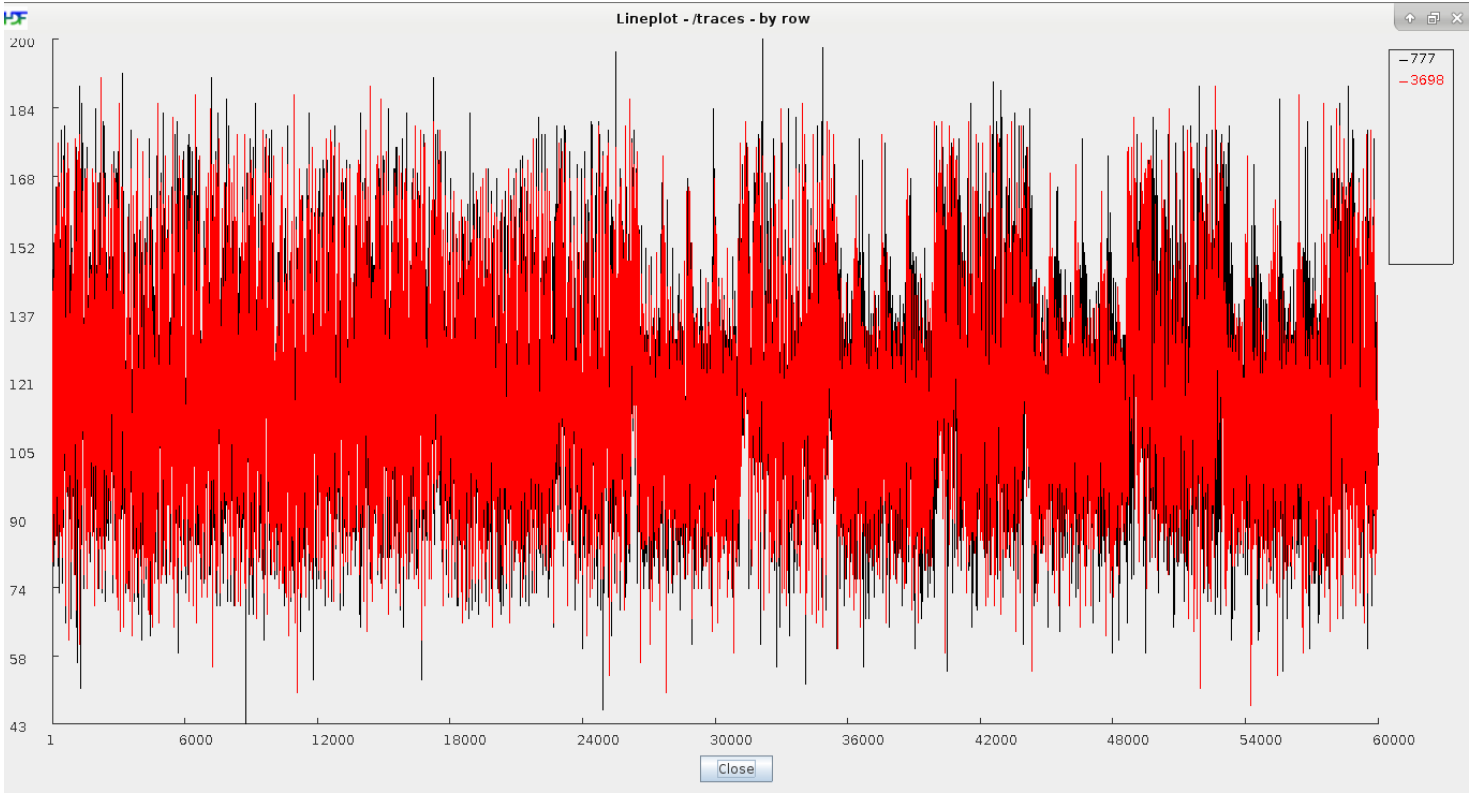
Hypothèse de base : la donnée manipulée influe la consommation

1. Capturer n traces de consommation du courant
   - Matrice des traces T : n traces * m points
   - Ici : 4000 traces, 60000 points par traces
2. Synchroniser temporellement les traces
3. Pour chacun des 16 octets du secret attaqué (OPc$\oplus$K puis RK2) :
   1. Calculer la matrice P des 256 prédictions à partir de RAND
      en l'occurrence de taille 256 * 4000
   2. Calculer la corrélation de P contre T
   3. Retenir l'hypothèse la plus probable

AVANT SYNCHRONISATION



APRÈS SYNCHRONISATION

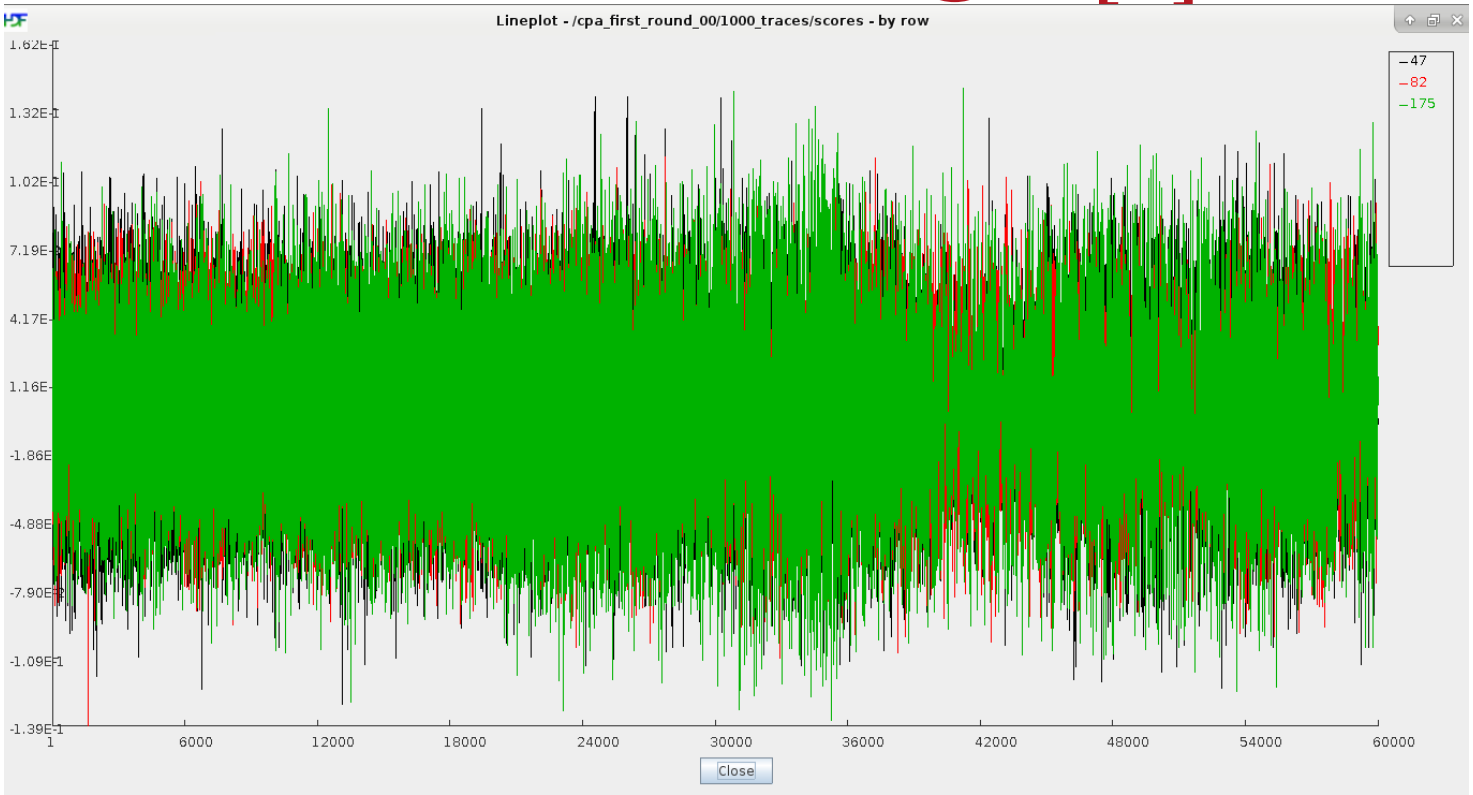


DÉROULÉ DE L'ATTAQUE

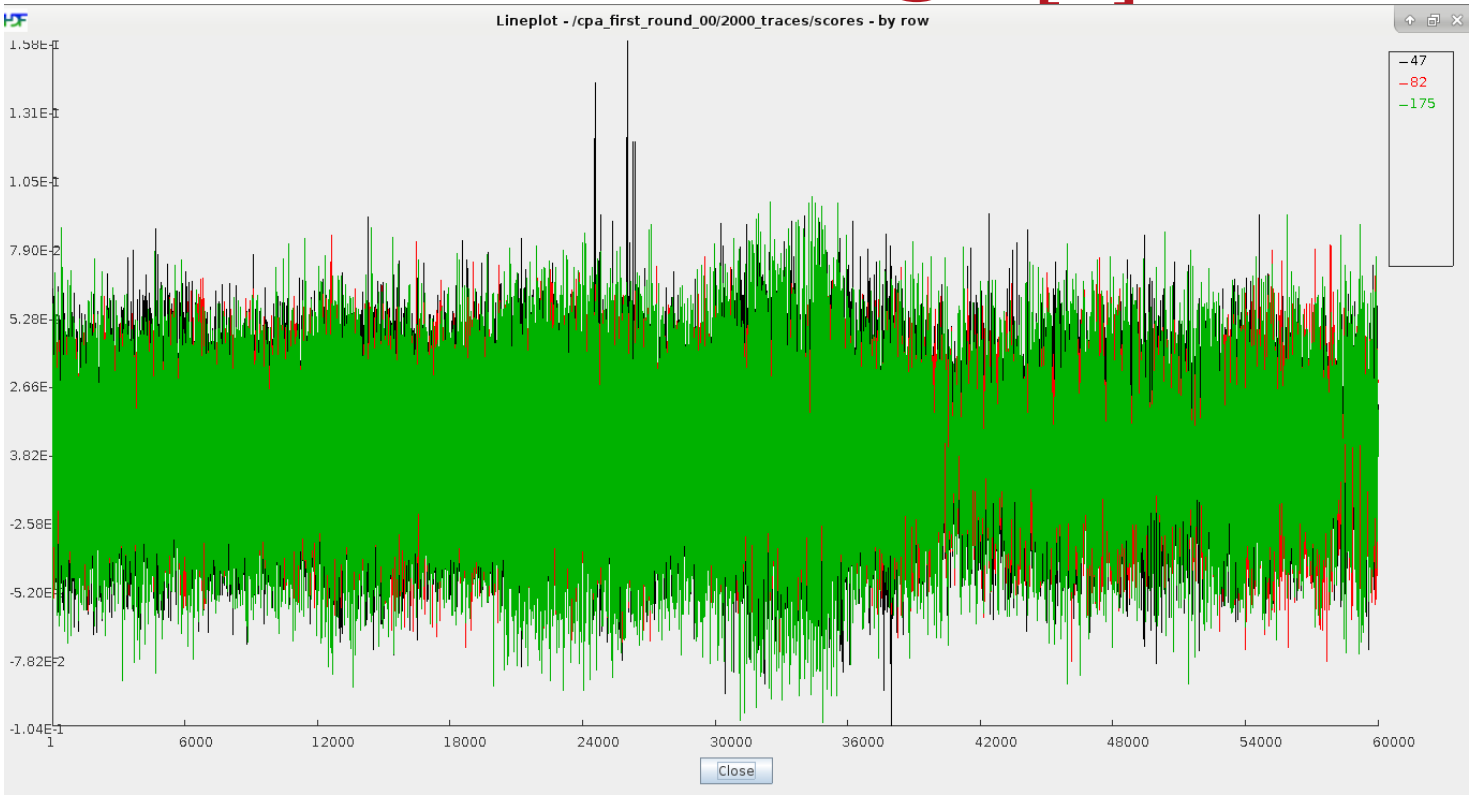
Hypothèse de base : la donnée manipulée influe la consommation

1. Capturer n traces de consommation du courant
   - Matrice des traces T : n traces * m points
   - Ici : 4000 traces, 60000 points par traces
2. Synchroniser temporellement les traces
3. Pour chacun des 16 octets du secret attaqué (OPc$\oplus$K puis RK2) :
   1. Calculer la matrice P des 256 prédictions à partir de RAND
      en l'occurrence de taille 256 * 4000
   2. Calculer la corrélation de P contre T
   3. Retenir l'hypothèse la plus probable

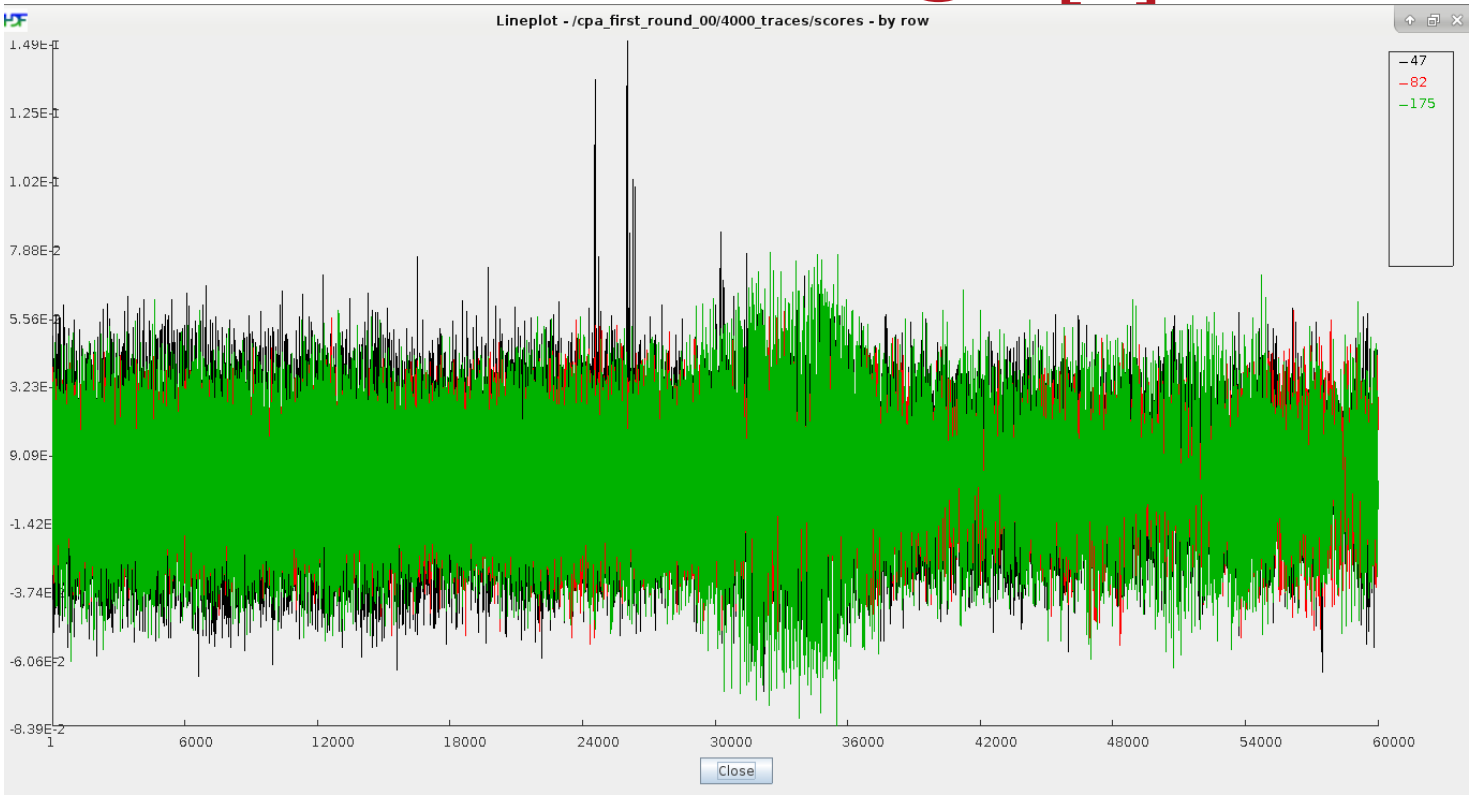
1000 TRACES : OPC⊕K [0]=?



2000 TRACES : OPC⊕K[0]=47?



4000 TRACES : OPC⊕K[0]=47



RÉCAPITULATIF

- Temps nécessaire pour capturer 4000 traces : ~80 minutes
- Temps nécessaire pour resynchroniser et corréler : ~20 minutes
- Matériel nécessaire
  - Rigol DS1054Z (400 euros)
  - Lecteur de carte à puces « custom »
- Logiciels nécessaires :
  - Scripts Python (NumPy)
  - https://github.com/pklaus/ds1054z

CONCLUSION

- L'attaque ne nécessite pas forcément des moyens importants
- Abonnés : changer le code PIN s'il est trivial (et ne pas le désactiver)
  - Afin de ralentir l'attaquant
- Opérateurs : utilisation de composants certifiés
  - Carte vulnérable : entité concernée notifiée en janvier 2018
  - https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/produits-certifies-cc/
- Travaux prospectifs
  - Utilisation de SCARE (Side-Channel Analysis for Reverse-Engineering)[1]

1 Attaques par canaux auxiliaires pour l'ingénierie à reculons

Q&A

- Merci pour votre attention !