Titre : Attaque par canaux auxiliaires

Auteurs :
Khadija Boukaffa
Théo Depoizier

Introduction :

Une attaque par canaux auxiliaires est une attaque informatique dans le but d'obtenir des informations sur un message crypté sans attaquer la sécurité mathématique d'un code. Généralement, les attaques par canaux auxiliaires s'intéressent à l'implémentation physique d'une procédure de cryptologie.
La première attaque par canaux auxiliaires connue a été implémentée par m. Kocher en 1998 sur une analyse différentielle de la consommation électrique des crypto-processeurs(cf. attaque par analyse de la consommation). depuis cette époque, les attaques par canaux auxiliaires ont évoluées et se sont fortement diversifiées.

Différents types d'attaques connus:

voici un exemple d'attaques par canaux auxiliaires connues. dans la suite de notre rapport, nous ne traiteront que les quatres premières.

- Attaque temporelle
- Attaque par analyse de consommation
- Attaque par analyse des émanations électromagnétique
- Attaque par fautes
- Fuite photonique
- Cryptanalyse acoustique
- Attaque par analyse du trafic

Présentation précise de certains types d'attaque :

Attaque temporelle: : Timing attaque

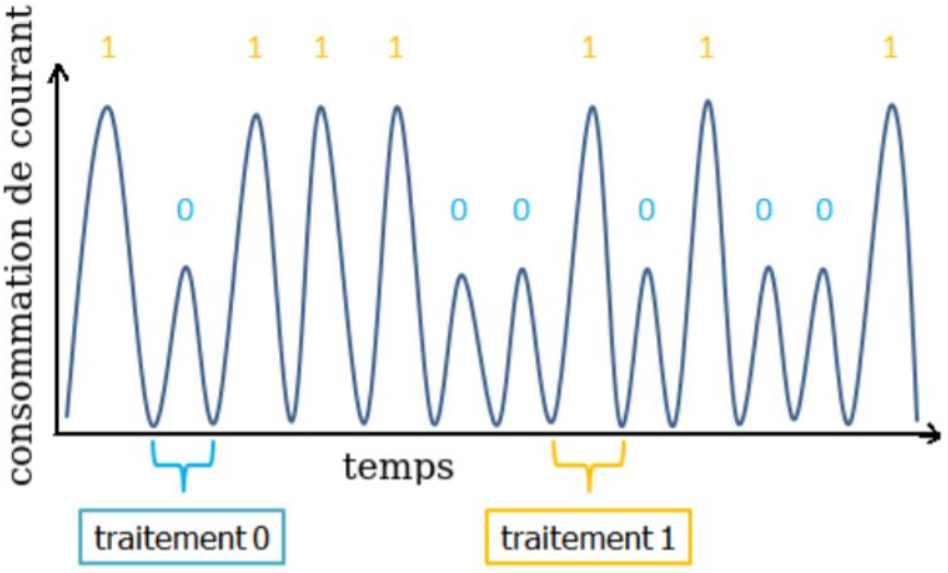
Principe:
une attaque temporelle consiste à estimer et analyser le temps mis pour effectuer certaines opérations cryptographiques dans le but de découvrir des informations secrètes. La mise en œuvre de ce genre d'attaque est intimement liée au matériel ou au logiciel attaqué.
cette attaque peut se faire dans un système est en général soumise à des perturbation aléatoire, ou à distance via un réseau.
cette attaque demande de connaître les détails de l'implémentation.

Exemple:
Prenons l'exemple de calcul de l'exponentiation modulaire, l'algorithme consiste à calculer N puissance B modulo C.
 En fonction de la valeur de B, l'algorithme ne prendra pas le même temps à s'exécuter, plus B est grand, plus l'algo mettra du temps.
grâce à cette différence de temps et donc de consommation d'énergie, il est possible d'attaquer le processeur et de connaître les valeurs N,B et C

Contre mesures:
 les processeurs génèrent un nombre aléatoire qu'ils insèrent dans leurs calculs pour brouiller le temps d'exécution et effectuer des opérations inutile.

Analyse de consommation :

https://www.di.ens.fr/~rossi/docs/rapport-stage.pdf
principe :
Étude de la tension en entrant et en sortant d'un circuit électrique pour en déduire quels types d'actions ont été réalisées ou quelles valeurs sont utilisées.
Analyse simple de la consommation (Simple Power Analysis) :
Le principe est simple, en implémentant le schémas décrit plus bas, on obtient un graphique sur l'oscilloscope où il devient aisé de trouver les 1 (correspondant aux à une plus grande consommation d'électricité) et les 0 (moins grande consommation), chaque 1 ou 0 étant induit par un courant différent dans le crypto-processeur. Le graphique suivant (extrait de la référence 2 page 4).



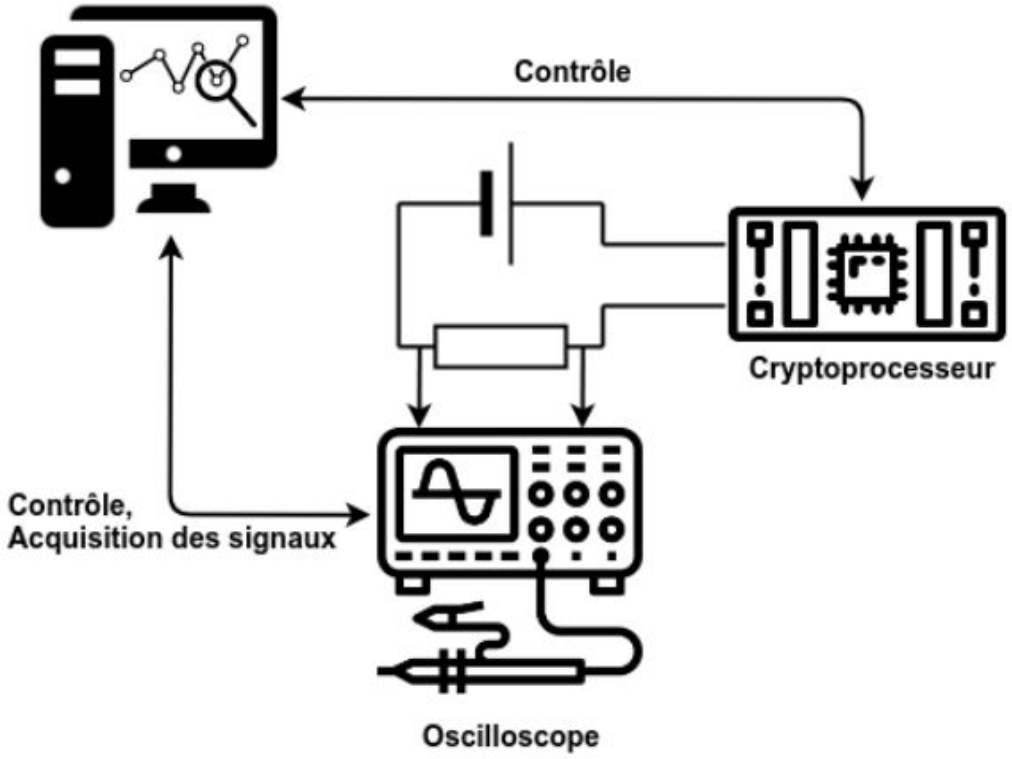
Analyse Différentielle de la consommation (Differential Power analysis) :

Cette attaque, bien que très théorique, combine une analyse de la tension utilisée et une extrapolation des actions exécutées par le processeur à un instant t. avec un grand nombre d'échantillons, on peut extrapoler quelles actions sont exécutées en même temps (et en quel nombre). il devient donc aisé de déchiffrer les valeurs utilisées tels que la clé privée d'un chiffrement asymétrique.

contre mesures :

- Noyer le signal dans un bruit (consommer tout le temps de l'électricité de manière aléatoire et déchiffrer toujours des clés aléatoires qu'elles soient justes ou fausses)
- réduire le courant consommé pour rendre imperceptible la différence de courant entre l'entrée et la sortie (contre mesure à court terme car les outils de mesure sont de plus en plus précis)

schémas d'installation pour une attaque par simple analyse de consommation :



schémas extrait de la référence 1

Références :

1. https://akerva.com/blog/avis-dexpert-securisation-des-systemes-complexes-embarques/
2. https://www.di.ens.fr/~rossi/docs/rapport-stage.pdf

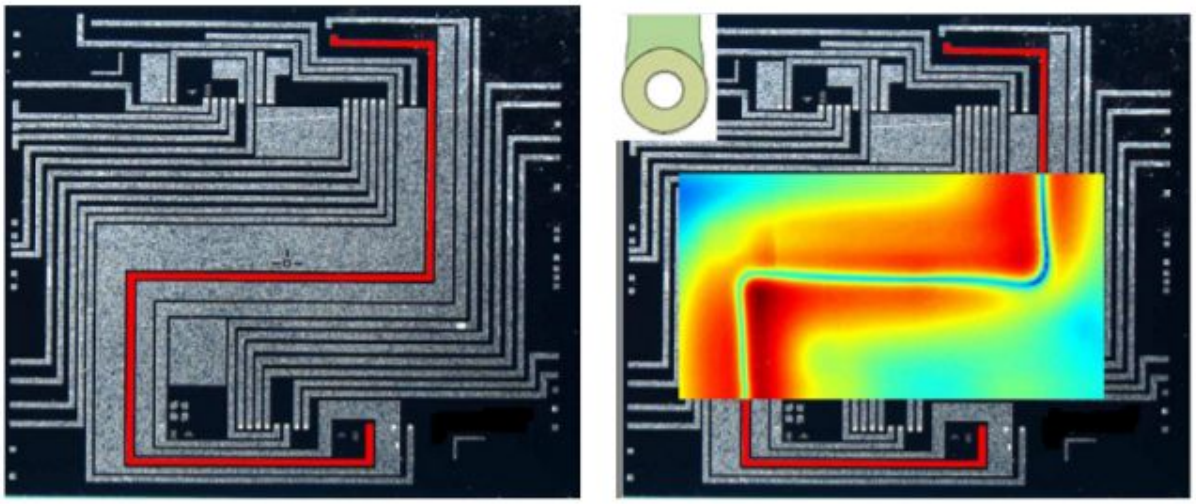
Attaque d'émanation Électromagnétiques :

Principe :

Partons de deux principes de base :

1- Toute particule chargée se déplaçant crée un champ électromagnétique. ceci est un principe de base du l'électromagnétisme.
2- Un processeur, pour réaliser la tâche qui lui est affectée, réalisera un certain nombre d'action logique en déclenchant des portes logiques par signal électrique.

Il devient donc aisé de comprendre que tout circuit électronique ou électrique, de part son fonctionnement, crée un champ électromagnétique modifiant le bruit électromagnétique présent tout autours de nous. Ce principe d'attaque par canaux auxiliaires vise à observer les modifications générées par le fonctionnement d'un processeur. Il s'agit d'une attaque par analyse d'émanation électromagnétique.



Cartographie des rayonnements électromagnétiques émis par des interconnexions (origine : référence 3)
Pour réussir à décrypter un code, le fonctionnement est plutôt simple : tout processeur, pour chiffrer/déchiffrer un message, réalisera certaines actions logiques (portes OU, portes ET…) Or toutes les actions ne sont pas réalisés à chaque tour d'horloge. Analyser le spectre d'émissions électromagnétiques d'un processeur réalisant des actions de chiffrement/déchiffrement permet donc de savoir quels actions sont réalisées, et dans quel ordre. À force de calcul et de beaucoup d'échantillons d'analyse, on peut tout à fait déchiffrer une clé secrète d'un code. ou si on connaît déjà le message que la machine essaye de déchiffrer, on peut trouver la clé secrète en quelques minutes (cf source 1).

schémas de mise en place :
(image de l'article en source 2)
Contres mesures :
en soit il est très difficile de se prémunir de ce genre d'attaques car quoi qu'il arrive les composants émettront toujours des rayonnements électromagnétiques. (principe des corps noirs) pour réaliser des contre mesures il faut donc entourer le processeur d'un matériaux qui protège de tous les rayonnements électromagnétiques.

Référence :

1. https://www.01net.com/actualites/pirater-un-ordinateur-en-captant-les-ondes-emises-par-le-processeur-cest-possible-658703.html
2. https://www.tau.ac.il/~tromer/radioexp/ (origine de la référence 1)

3. https://www.emse.fr/~robisson/These_Nguyen.pdf page 16 à 19

Attaque par fautes k :

I. but:

le but des attaques par fautes est de provoquer un comportement inhabituel des opérations cryptographiques dans le but d'en extraire des informations secrètes comme la clé de chiffrement.

II. Exemple:

1. Attaques sur RSA:

les attaques sur RSA sont certainement ce qu'on appelle les timing attacks(ou bien les attaques temporelles)===> voir l'attaque temporelle.

2. Attaques par fautes impossible:

le but de cette attaque et d'obtenir des états normals impossibles, une attaque de ce type est appliquée contre le chiffrement de flot RC4: introduire une erreur dans le tableau de permutations pour arriver à obtenir l'état interne complet du chiffrement.

3. Attaques par corruption/perturbation:

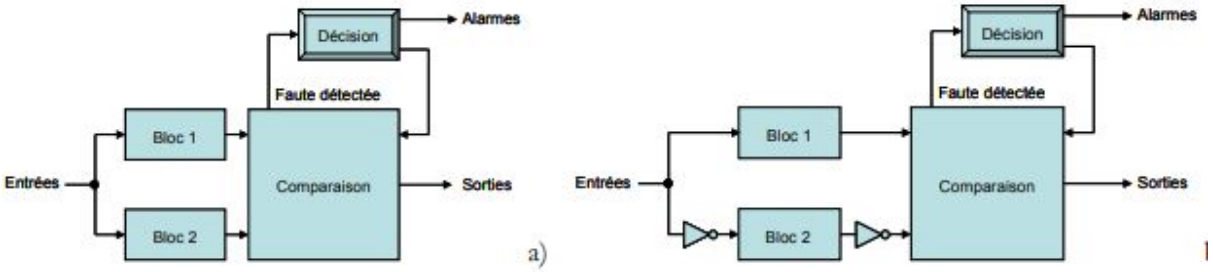
ce type d'attaque est pour principe de créer de valeurs logiques erronées au sein du circuit permettant soit de corrompre les données soit de modifier le flot d'exécution. Ces attaques se réalisent en deux grandes étapes : l'**induction de fautes puis l'analyse de fautes.** L'étape d'**induction de fautes** consiste à obtenir un certain nombre de traces d'exécution en présence ou non de perturbations extérieures.

L'analyse des fautes de ces perturbations sur le comportement du circuit et la déduction d'informations sur la clef à partir des traces obtenues durant la première étape constituent l'analyse de fautes.

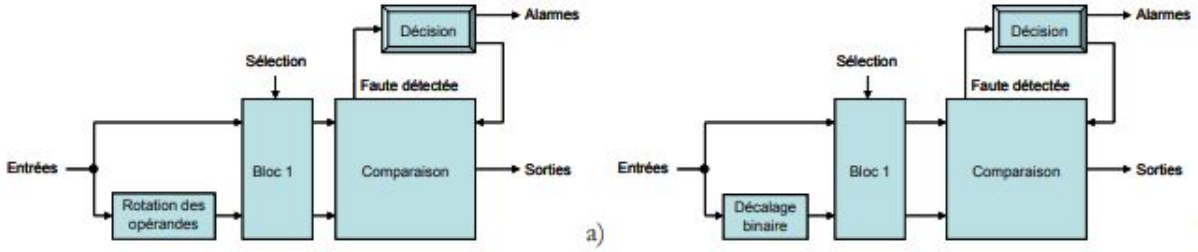
III. Contre mesures:

Pour se prémunir des attaques par injections de fautes, une des contre-mesures les plus efficaces est la redondance qui peut être de trois types : matérielle, temporelle ou d'information. En plus de ces techniques, il est possible de réaliser des calculs de vérification tels que le chiffrement d'une donnée puis du déchiffrement du résultat pour détecter les injections de fautes.

1. Redondance matérielle:
   le principe est de faire la duplication (simple/multiple/dynamique) avec comparaison, il suffit de faire la même opération sur plusieurs copies d'un même bloc de calcul et de comparer les résultats obtenus.



2. Redondance temporelle:
   La redondance temporelle consiste à effectuer le même calcul avec le même bloc matériel mais à des instants différents.



3. Redondance d'information:
   Cette technique utilise par exemple de la parité, des checksums ou les codes de Hamming….

   1.1. Parité:consiste à ajouter un bit en plus à la donnée. La valeur de ce bit dépend de la donnée mais également du type de parité désirée : paire ou impaire. Par exemple, dans le cas de la parité paire, le bit de parité vaut '0' si la somme des bits à '1' de la donnée est paire afin que la somme des bits de la donnée et de la parité soit paire.
   1.2. Les Check sum: consistent à faire la somme de tous les bits d'une donnée et à comparer le résultat obtenu avec une valeur stockée. Dans le cas où les résultats diffèrent alors une faute est présent.
   1.3. les code de hammings : permettent de corriger une et une seule erreur dans une donnée. Le code de Hamming transfère 4 bits de données et 3 bits de parité pour un message de 7 bits, et si l'un de ces 7 bits est modifié alors il existe un algorithme permettant de corriger l'erreur.

Références:

1. https://sebsauvage.net/streisand.me/mangetamain/?20120609_205926_Decouvrez_les_attaques_par_canaux_auxiliaires_sur_cryptoprocesseurs
2. https://tel.archives-ouvertes.fr/tel-00399450/document
3. https://fr.wikipedia.org/wiki/Attaque_temporelle
4. https://fr.wikipedia.org/wiki/Attaque_par_faute
5. https://tel.archives-ouvertes.fr/tel-00422660/document

Bilan

L'attaque par canaux auxiliaires décrit parfaitement le vieil adage : "une chaîne n'est jamais plus forte que son chaînon le plus faible."
En effet, grâce aux attaques par canaux auxiliaires, on montre que malgré une sécurité mathématique "parfaite", avec les moyens appropriés il devient facile de décrypter un code ou d'obtenir des informations relatives à un code.
Même si de nombreuses attaques par canaux auxiliaires restent difficiles à mettre en place (une présence physique près du cryptoprocesseur étant généralement nécessaire), il est

parfaitement envisageable de les appliquer à des cas concrets (personne infiltrée dans l'organisme à infiltrer, accès à un ordinateur piratable proche du cryptoprocesseur...), ce qui a été déjà réalisé à travers l'histoire (espionnage des données échanges à travers un cable éthernet ou VGA).