

# Sécurité des implémentations pour la cryptographie

## Partie 5 : Résistance aux attaques locales non-invasives

---

Benoît Gérard  
16 janvier 2017



# Plan du cours

## Étape 1

Définition du besoin et de l'architecture au niveau système.

## Étape 2

Définition de l'interface carte/terminal : API exposée par la carte.

## Étape 3

Implémentation d'une version résistante aux attaques non-crypto.

## Étape 4

Implémentation d'algo. crypto. résistante aux attaques distantes.

## Étape 5

Implémentation d'algo. crypto. résistante aux attaques locales.

## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures

## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures

# Généralités sur les attaques non-invasives

## Principe



# Généralités sur les attaques non-invasives

## Principe



attaques actives

# Généralités sur les attaques non-invasives

## Principe



attaques actives



attaques passives

# Généralités sur les attaques non-invasives

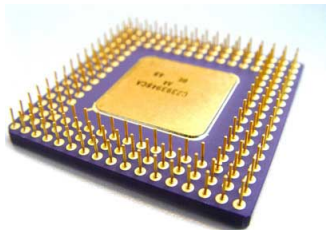
## Principe



attaques actives



attaques passives





# Généralités sur les attaques non-invasives

## Principe



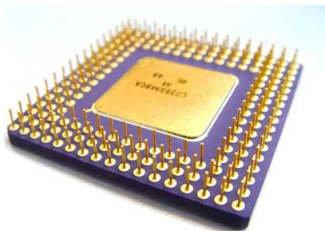
attaques actives



attaques passives



attaques actives



# Généralités sur les attaques non-invasives

## Principe



attaques actives



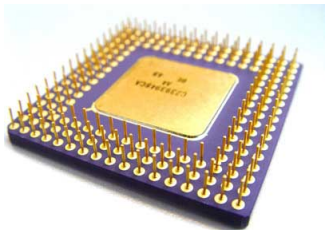
attaques passives



attaques actives



attaques passives

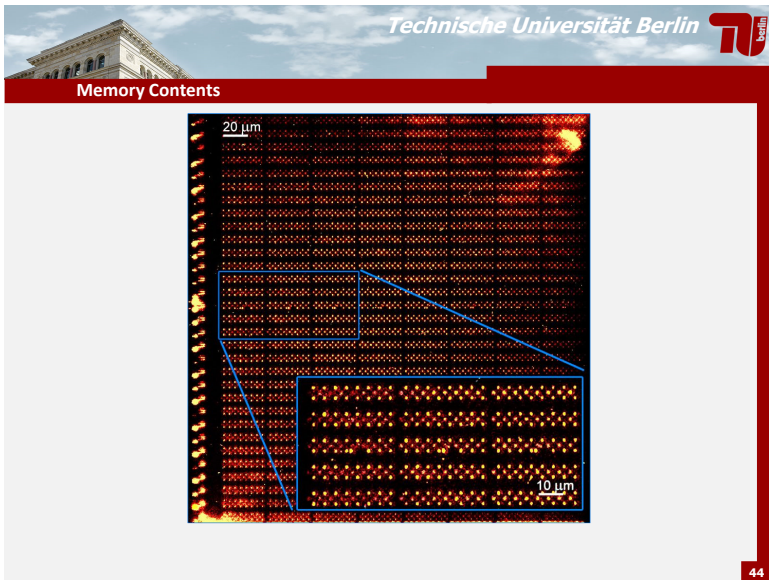


Quelques canaux auxiliaires :

- ▶ temps d'exécution,
- ▶ consommation de courant,
- ▶ rayonnements électromagnétiques,
- ▶ émissions de photons,
- ▶ émissions sonores,
- ▶ température,
- ▶ potentiel électrique d'un corps en contact avec le PC !
- ▶ ...


# Généralités sur les attaques non-invasives

Exemple de l'émission photonique



# Généralités sur les attaques non-invasives

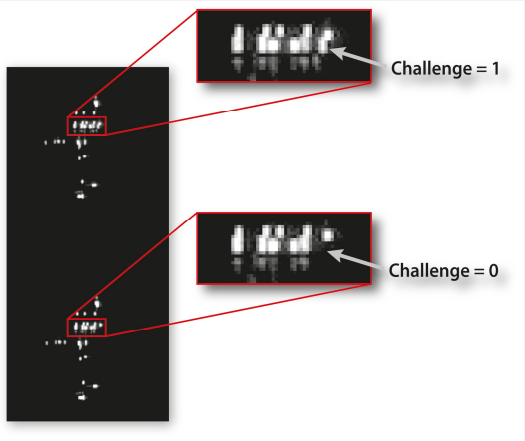
Exemple de l'émission photonique



Technische Universität Berlin

Reading Challenge bits from emissions

- Controlled PUF  
→  
no access to challenges!
- So?
- Simply read challenges from emission patterns.



50

On se protège contre un attaquant borné

- ▶ en temps de calcul,
- ▶ en mémoire,
- ▶ en nombre de mesures.

On peut donc :

- ▶ augmenter la complexité des attaques,
- ▶ diminuer le nombre de mesures disponibles.

La cryptographie n'est pas forcément la seule partie exposée.

## Introduction aux attaques par canaux auxiliaires

Généralités sur les attaques non-invasives

Simple Power Analysis (SPA)

## Cryptographie symétrique

Differential Power Analysis (DPA)

Correlation Power Analysis (CPA)

Autres attaques Divide & Conquer

Contremesures

## Cryptographie asymétrique

Attaques à plusieurs mesures

Contremesures

# Single Power Analysis

## RSA : Square & Multiply

- ▶ Multiplication modulaire
  - ▶ Square & Multiply
- ▶ Multiplication d'un point par un scalaire
  - ▶ Double & Add

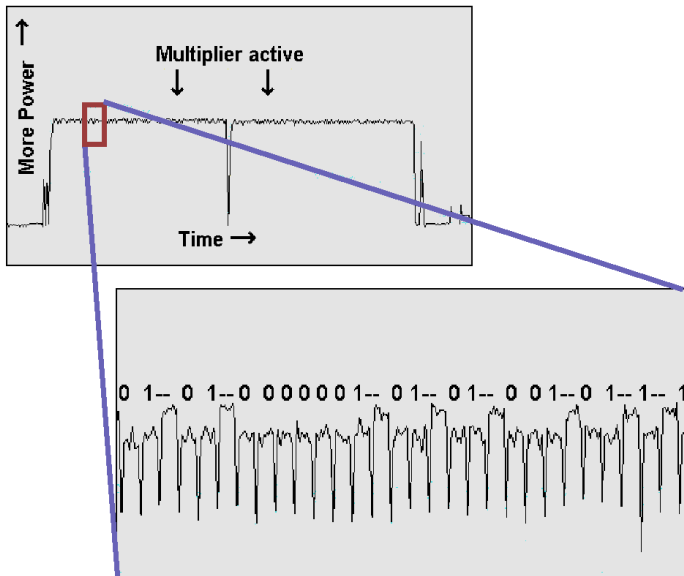
Calcul de  $m^d \bmod n$

```
 $R \leftarrow 1$   
for  $i = k - 1$  to 0 do  
     $R \leftarrow R \times R \bmod n$   
    if ( $d_i == 1$ )  
         $R \leftarrow R \times m \bmod n$   
return  $R$ 
```



# Simple Power Analysis

RSA : exemple de mesure



Utilisation d'algorithmes d'exponentiation réguliers :

- ▶ ajout de multiplications inutiles,
- ▶ algorithmes intrinsèquement réguliers,
  - ▶ Montgomery Ladder,
  - ▶ Multiply Always,
  - ▶ Square Always.

Ajout de bruit :

- ▶ bruit sur la mesure,
- ▶ bruit sur le déroulement temporel de l'algorithme.

Ajout d'opérations inutiles :

- ✓ solution pertinente contre les attaques sur le temps d'exécution,
- ✗ solution potentiellement douteuse contre les attaques locales.

Quelques idées d'attaques :

- ▶ fausses données détectables en SPA ?
- ▶ calculs inutiles non sensibles aux fautes (cf. cours suivant),
- ▶ registre inutile détectable par analyse photonique.

# Simple Power Analysis

## Protections : le Montgomery Ladder

Calcul de  $m^d \bmod n$  :

```
 $R_0 \leftarrow 1$   
 $R_1 \leftarrow m$   
for  $i = k - 1$  to  $0$  do  
     $R_{1-d_i} \leftarrow R_0 \times R_1 \bmod n$   
     $R_{d_i} \leftarrow R_{d_i}^2 \bmod n$   
return  $R_0$ 
```

Sécurité basée sur l'incapacité à distinguer les registres  $R_0$  et  $R_1$ .

L'utilisation d'algorithmes nativement réguliers est à privilégier.

Attention il ne sont pas sécurisés pour autant !

Montgomery Ladder potentiellement :

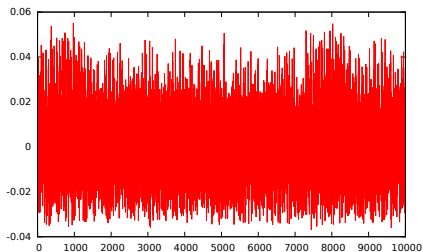
- ▶ sensible à l'analyse d'émissions photoniques,
- ▶ sensible aux fautes.

Mais les attaques sont moins faciles.

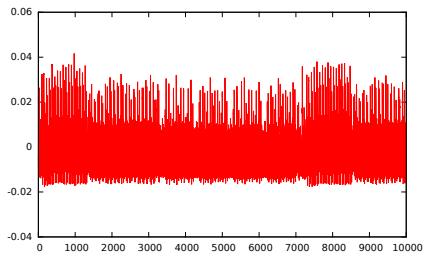
# Simple Power Analysis

Protections : le bruit de mesure

Le bruit rend l'attaque difficile . . .  
mais on peut le réduire en faisant une moyenne.



Mesure brute.



Moyenne de 20 mesures.

## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures

# Differential Power Analysis

## Principe

### DPA : Differential Power Analysis

Terme désignant une attaque en particulier mais souvent utilisé pour parler des attaques par mesure de courant en général.

### Principe

- ▶ pour un grand nombre de clairs,
- ▶ obtenir de l'information sur une variable intermédiaire,
- ▶ en déduire de l'information sur la clef,
- ▶ en général : approche “Diviser pour régner”.

### Vocabulaire

Trace/Courbe : mesures de consommation (ou autre) sur la durée d'un calcul.



## Modèle poids de Hamming

Quand on envoie un signal

- ▶ 0  $\Leftrightarrow$  pas de tension,
- ▶ 1  $\Leftrightarrow$  tension maintenue.

On consomme donc d'autant plus qu'il y a de 1.

## Modèle distance de Hamming

Quand on met à jour une valeur (dans un registre, une mémoire)

- ▶ modifier un bit induit une sur-consommation (changement d'état),
- ▶ ne rien faire n'induit pas de sur-consommation.

On consomme donc d'autant plus que l'on modifie de bits.

On a donc deux modèles.

- ▶ Poids de Hamming  
on envoie  $a$  : on consomme en fonction de  $\text{HW}(a)$ .
- ▶ Distance de Hamming  
on modifie  $a$  en  $b$  : on consomme en fonction de  $\text{HW}(a \oplus b)$ .

Où

$$\text{HW}(\overline{a_{n-1} \dots a_1 a_0}^2) = \sum_{i=0}^{n-1} a_i.$$

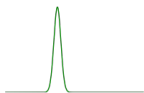
On cible généralement des données intermédiaires mélangeant un secret et une donnée connue.

En cryptographie symétrique on regarde la sortie d'une boîte-S :

$$S(x_i \oplus k_i)$$

# Differential Power Analysis

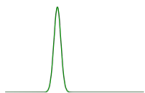
Décomposition d'une mesure



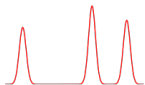
$$S(x_1 \oplus k_1)$$

# Differential Power Analysis

Décomposition d'une mesure



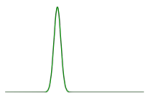
$$S(x_1 \oplus k_1)$$



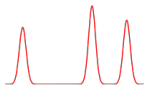
$$S(x_i \oplus k_i), i \neq 1$$

# Differential Power Analysis

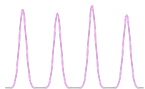
Décomposition d'une mesure



$$S(x_1 \oplus k_1)$$



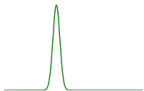
$$S(x_i \oplus k_i), i \neq 1$$



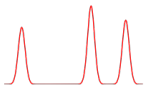
activité proc. (horloge ...)

# Differential Power Analysis

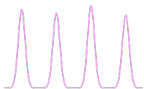
Décomposition d'une mesure



$$S(x_1 \oplus k_1)$$



$$S(x_i \oplus k_i), i \neq 1$$



activité proc. (horloge ...)



bruit de mesure

# Differential Power Analysis

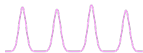
Décomposition d'une mesure



$$S(x_1 \oplus k_1)$$



$$S(x_i \oplus k_i), i \neq 1$$



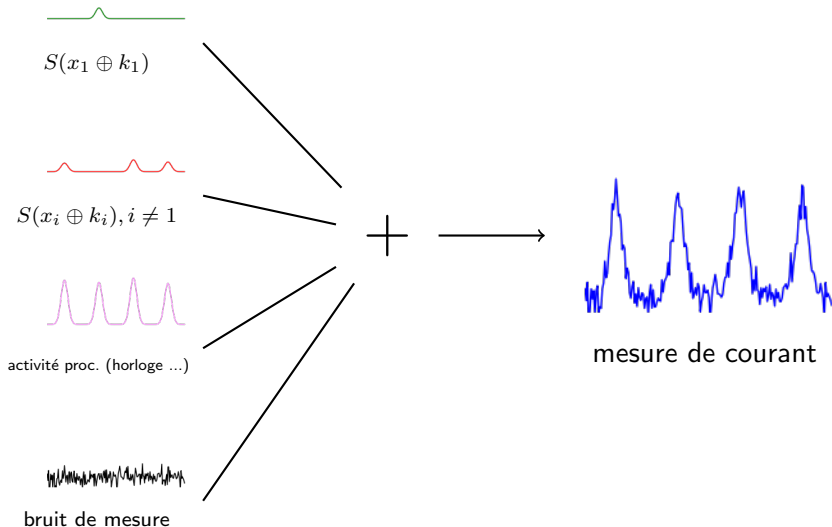
activité proc. (horloge ...)



bruit de mesure

# Differential Power Analysis

Décomposition d'une mesure



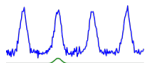


# Differential Power Analysis

Avec la bonne clef

$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$



$$\text{HW}\left(S(x^{(0)} \oplus k)\right) = 0$$

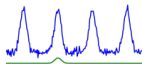
# Differential Power Analysis

Avec la bonne clef

$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$



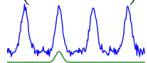
# Differential Power Analysis

Avec la bonne clef

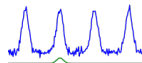
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$



$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$



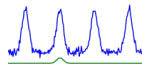
# Differential Power Analysis

Avec la bonne clef

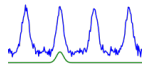
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$



$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$



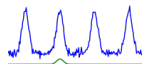
# Differential Power Analysis

Avec la bonne clef

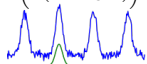
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

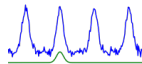
$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$



$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$



$$\text{HW}(S(x^{(2)} \oplus k)) = 6$$



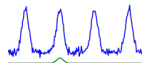
# Differential Power Analysis

Avec la bonne clef

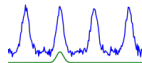
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

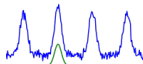
$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$



$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$



$$\text{HW}(S(x^{(2)} \oplus k)) = 6$$



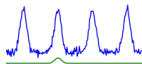
# Differential Power Analysis

Avec la bonne clef

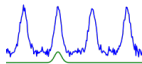
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

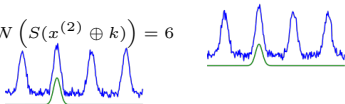
$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$



$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$



$$\text{HW}(S(x^{(2)} \oplus k)) = 6$$



$$\text{HW}(S(x^{(3)} \oplus k)) = 8$$

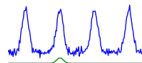
# Differential Power Analysis

Avec la bonne clef

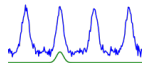
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

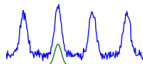
$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$



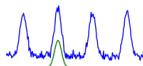
$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$



$$\text{HW}(S(x^{(2)} \oplus k)) = 6$$



$$\text{HW}(S(x^{(3)} \oplus k)) = 8$$

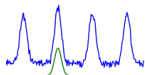




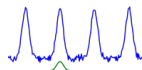
# Differential Power Analysis

Avec la bonne clef

$\text{HW}(\cdot) > 4$



$\text{HW}(\cdot) < 4$

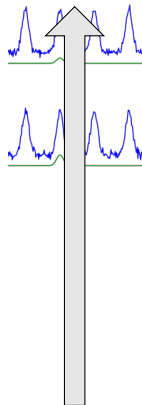
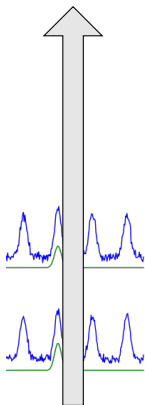


$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$

$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$

$$\text{HW}(S(x^{(2)} \oplus k)) = 6$$

$$\text{HW}(S(x^{(3)} \oplus k)) = 8$$

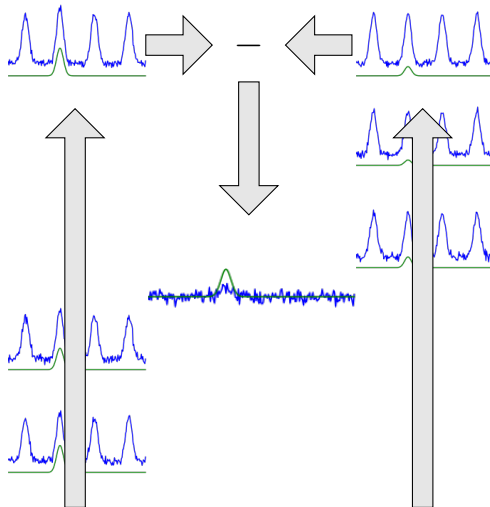


# Differential Power Analysis

Avec la bonne clef

$\text{HW}(\cdot) > 4$

$\text{HW}(\cdot) < 4$



$$\text{HW}(S(x^{(0)} \oplus k)) = 0$$

$$\text{HW}(S(x^{(1)} \oplus k)) = 2$$

$$\text{HW}(S(x^{(2)} \oplus k)) = 6$$

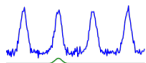
$$\text{HW}(S(x^{(3)} \oplus k)) = 8$$

# Differential Power Analysis

Avec la mauvaise clef

$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$



$$\text{HW}\left(S(x^{(0)} \oplus k')\right) = 1$$

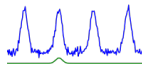
# Differential Power Analysis

Avec la mauvaise clef

$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



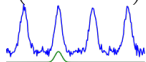
# Differential Power Analysis

Avec la mauvaise clef

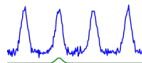
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$



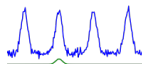
# Differential Power Analysis

Avec la mauvaise clef

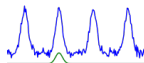
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$



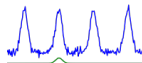
# Differential Power Analysis

Avec la mauvaise clef

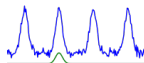
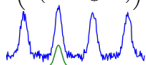
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$



$$\text{HW}(S(x^{(2)} \oplus k')) = 7$$

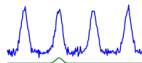
# Differential Power Analysis

Avec la mauvaise clef

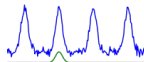
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

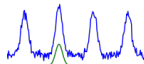
$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$



$$\text{HW}(S(x^{(2)} \oplus k')) = 7$$





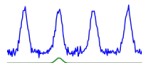
# Differential Power Analysis

Avec la mauvaise clef

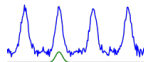
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

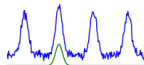
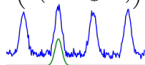
$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$



$$\text{HW}(S(x^{(2)} \oplus k')) = 7$$



$$\text{HW}(S(x^{(3)} \oplus k')) = 2$$

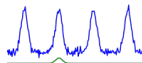
# Differential Power Analysis

Avec la mauvaise clef

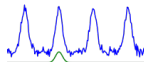
$$\text{HW}(\cdot) > 4$$

$$\text{HW}(\cdot) < 4$$

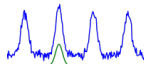
$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



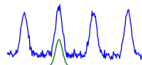
$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$



$$\text{HW}(S(x^{(2)} \oplus k')) = 7$$



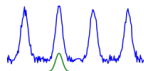
$$\text{HW}(S(x^{(3)} \oplus k')) = 2$$



# Differential Power Analysis

Avec la mauvaise clef

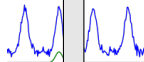
$\text{HW}(\cdot) > 4$



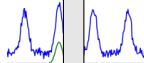
$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$



$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$

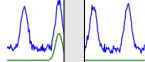
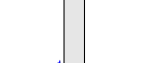
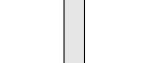
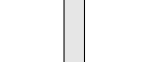
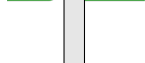
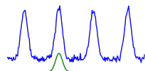


$$\text{HW}(S(x^{(2)} \oplus k')) = 7$$



$$\text{HW}(S(x^{(3)} \oplus k')) = 2$$

$\text{HW}(\cdot) < 4$

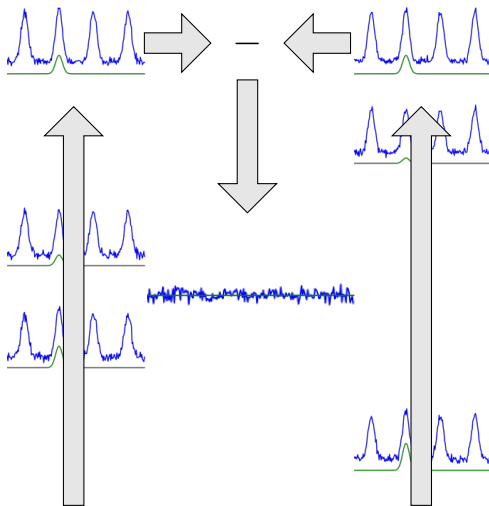


# Differential Power Analysis

Avec la mauvaise clef

$\text{HW}(\cdot) > 4$

$\text{HW}(\cdot) < 4$



$$\text{HW}(S(x^{(0)} \oplus k')) = 1$$

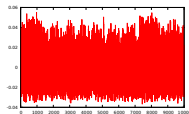
$$\text{HW}(S(x^{(1)} \oplus k')) = 5$$

$$\text{HW}(S(x^{(2)} \oplus k')) = 7$$

$$\text{HW}(S(x^{(3)} \oplus k')) = 2$$

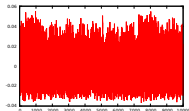
# Differential Power Analysis

Exemple sur une vrai mesure



# Differential Power Analysis

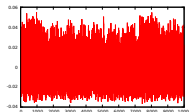
Exemple sur une vrai mesure



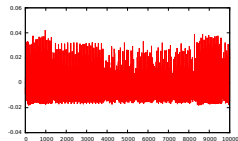
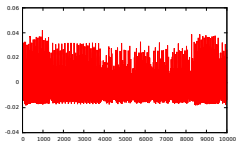
↙  $k = 0x00$  ↘

# Differential Power Analysis

Exemple sur une vrai mesure

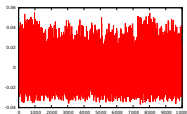


↙  $k = 0x00$  ↘

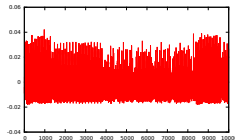
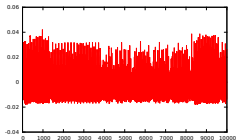


# Differential Power Analysis

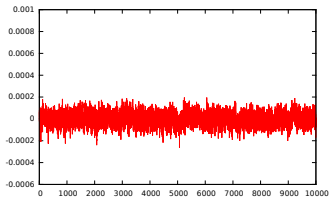
Exemple sur une vrai mesure



↙  $k = 0x00$  ↘



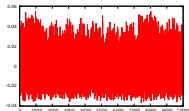
↙ — ↘





# Differential Power Analysis

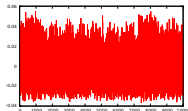
Exemple sur une vrai mesure



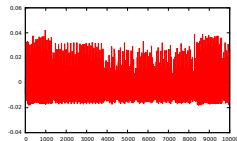
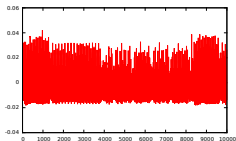
↙  $k = 0x52$  ↘

# Differential Power Analysis

Exemple sur une vrai mesure

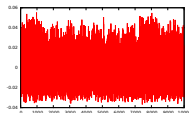


↙  $k = 0x52$  ↘

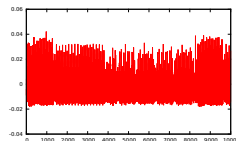
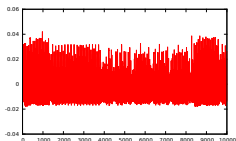


# Differential Power Analysis

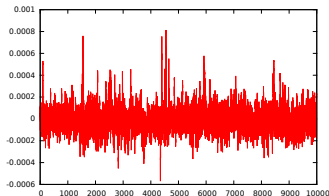
Exemple sur une vrai mesure



↙  $k = 0x52$  ↘



↙ — ↘



DÉMO

## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures

### Hypothèse

La consommation est liée linéairement à un modèle de fuite.

### Exemple 1

Poids de Hamming :

$$r \leftarrow x; \quad \Rightarrow \ell = \text{HW}(x).$$

### Exemple 2

Distance de Hamming :

$$r \leftarrow x; r \leftarrow y \quad \Rightarrow \ell = \text{HW}(x \oplus y).$$

### Idée

On n'utilise que le bit de poids fort du poids de Hamming alors que l'on pourrait tout prendre.

*input*    *conso.*

0x40	0,85mV
0x75	1,15mV
0x14	1,05mV
0xA4	0,95mV
0x3F	0,80mV

# Correlation Power Analysis

## Principe

### Idée

On n'utilise que le bit de poids fort du poids de Hamming alors que l'on pourrait tout prendre.

<i>input</i>	<i>conso.</i>	$k = 0x00$	$k = 0x42$	$k = 0xA7$	$k = 0xFF$
0x40	0,85mV	$\begin{bmatrix} 1 \end{bmatrix}$	$\begin{bmatrix} 1 \end{bmatrix}$	$\begin{bmatrix} 6 \end{bmatrix}$	$\begin{bmatrix} 7 \end{bmatrix}$
0x75	1,15mV	$\begin{bmatrix} 5 \end{bmatrix}$	$\begin{bmatrix} 5 \end{bmatrix}$	$\begin{bmatrix} 4 \end{bmatrix}$	$\begin{bmatrix} 3 \end{bmatrix}$
0x14	1,05mV	$\begin{bmatrix} 2 \end{bmatrix}$	$\dots$	$\begin{bmatrix} 5 \end{bmatrix}$	$\begin{bmatrix} 6 \end{bmatrix}$
0xA4	0,95mV	$\begin{bmatrix} 3 \end{bmatrix}$	$\dots$	$\begin{bmatrix} 2 \end{bmatrix}$	$\begin{bmatrix} 5 \end{bmatrix}$
0x3F	0,80mV	$\begin{bmatrix} 6 \end{bmatrix}$	$\dots$	$\begin{bmatrix} 3 \end{bmatrix}$	$\begin{bmatrix} 2 \end{bmatrix}$



# Correlation Power Analysis

## Principe

### Idée

On n'utilise que le bit de poids fort du poids de Hamming alors que l'on pourrait tout prendre.

<i>input</i>	<i>conso.</i>	$k = 0x00$	$k = 0x42$	$k = 0xA7$	$k = 0xFF$
0x40	0,85mV	$\begin{bmatrix} 1 \\ 5 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 5 \end{bmatrix}$	$\begin{bmatrix} 6 \\ 4 \end{bmatrix}$	$\begin{bmatrix} 7 \\ 3 \end{bmatrix}$
0x75	1,15mV	$\begin{bmatrix} 2 \\ 3 \end{bmatrix}$	$\begin{bmatrix} 4 \\ 5 \end{bmatrix}$	$\begin{bmatrix} 5 \\ 2 \end{bmatrix}$	$\begin{bmatrix} 6 \\ 5 \end{bmatrix}$
0x14	1,05mV	$\begin{bmatrix} 6 \\ 6 \end{bmatrix}$	$\begin{bmatrix} 6 \\ 6 \end{bmatrix}$	$\begin{bmatrix} 3 \\ 3 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 2 \end{bmatrix}$
0xA4	0,95mV				
0x3F	0,80mV				
		0.0253	<b>0.172</b>	0.0552	- 0.0253

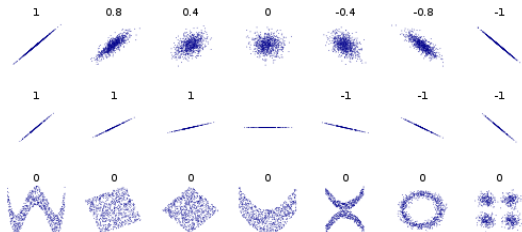
# Correlation Power Analysis

Coefficient de corrélation de Pearson

Produit scalaire de vecteurs normalisés

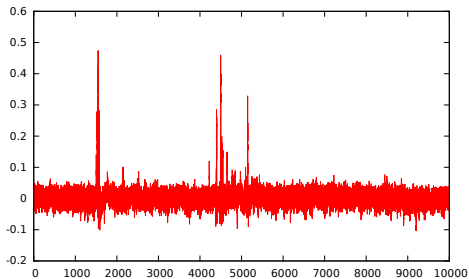
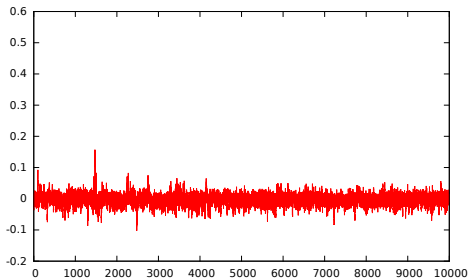
- ▶  $\mathbf{x}$  : prévisions,
- ▶  $\mathbf{y}$  : observations.

$$\rho(\mathbf{x}, \mathbf{y}) \triangleq \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}}$$



# Correlation Power Analysis

Exemple de résultat



## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer**

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures

Pour le moment, on a vu

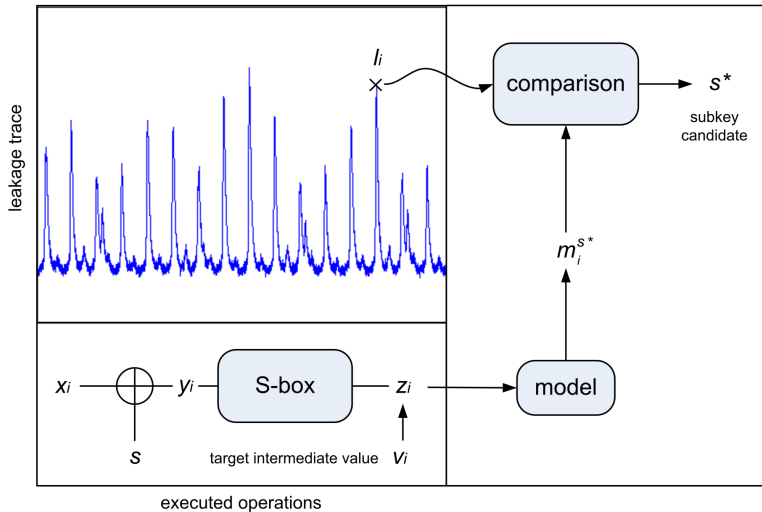
“Pour chaque clef j’effectue un calcul et je suis capable de détecter la bonne.”

... Ce n’est pas mieux qu’une recherche exhaustive et pour des clefs de 128 bits c’est difficile.

L’astuce : on peut cibler chaque octet indépendamment (pour l’AES)

# Autes attaques D&C

Canevas général



## Idée

Toutes les bascules/fils ne sont pas identiques (variabilité du processus de fabrication, routage contraint ...).

On généralise donc le modèle poids de Hamming à une fuite :

$$\mathcal{L}(x) - cte \propto \sum_{i=0}^{n-1} \alpha_i x_i.$$

On peut :

- ▶ soit calculer les  $\alpha_i$  en phase d'apprentissage puis attaquer avec le modèle,
- ▶ soit chercher le modèle obtenu pour chaque candidat et choisir la clef avec le modèle menant à l'erreur la plus faible.

### Idée

Il existe des phénomènes physiques de couplages entre fils.

On peut généraliser encore plus :

$$\mathcal{L}(x) - cte \propto \sum_{e=(e_0, \dots, e_{n-1}) \in \{0,1\}^n} \alpha_e \prod_{i=0}^{n-1} x_i^{e_i}.$$

Autrement dit : au lieu de juste considérer les  $x_i$  on regarde tous les monômes de degré au plus  $d$  i.e. les couplages entre au plus  $d$  fils.

**Attention !** Si on considère tous les monômes alors toutes les clefs mèneront à un bon modèle.



### Idée

Si on a accès à une cible similaire on peut apprendre précisément le modèle.

- ▶ Hypothèse Gaussienne (information dans la moyenne et les covariances uniquement).
- ▶ Sélection de point ou réduction de dimensionnalité sinon impraticable.

On estime les probabilités

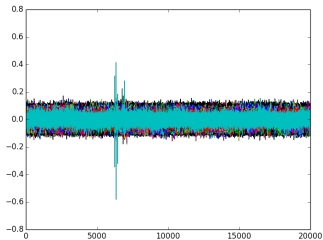
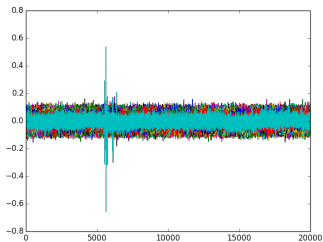
$$\Pr [L = l | X = x, K = k] .$$

On cherche ensuite

$$\operatorname{argmax}_k \prod_i \Pr [L = l_i | X = x_i, K = k] .$$

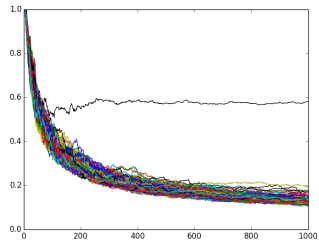
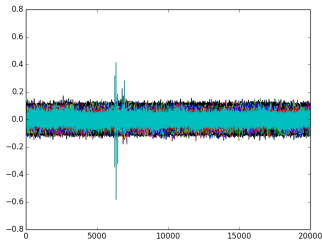
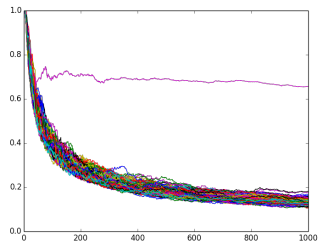
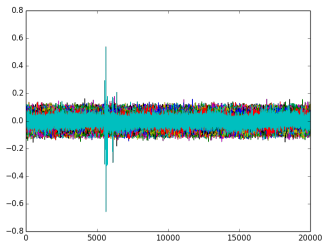
# Autres attaques D&C

Résultats sur un octet



# Autres attaques D&C

Résultats sur un octet

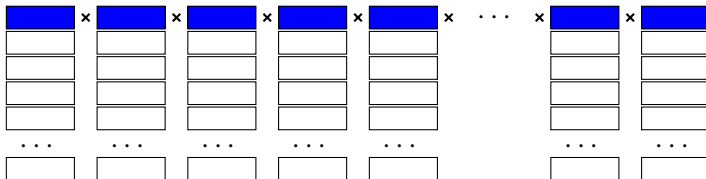


# Autres attaques D&C

Énumération : problématique

## Probabilité de succès

Probabilité que pour chaque octet, la bonne valeur soit en tête de liste.



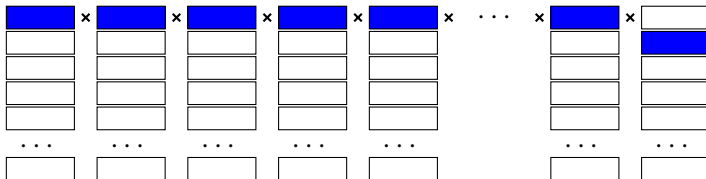
# Autres attaques D&C

Énumération : problématique

## Probabilité de succès

Probabilité que pour chaque octet, la bonne valeur soit en tête de liste.

Et si on a un peu moins de chance ?



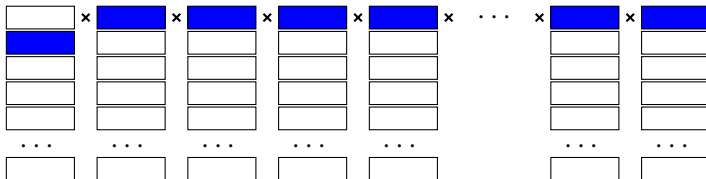
# Autres attaques D&C

Énumération : problématique

## Probabilité de succès

Probabilité que pour chaque octet, la bonne valeur soit en tête de liste.

Et si on a un peu moins de chance ?



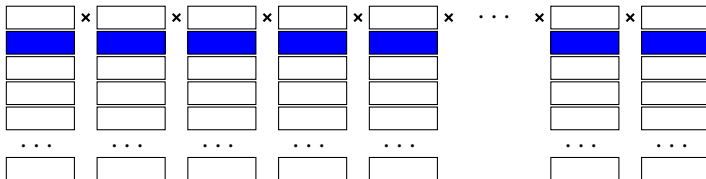
# Autres attaques D&C

Énumération : problématique

## Probabilité de succès

Probabilité que pour chaque octet, la bonne valeur soit en tête de liste.

Et si on a un peu moins de chance ?



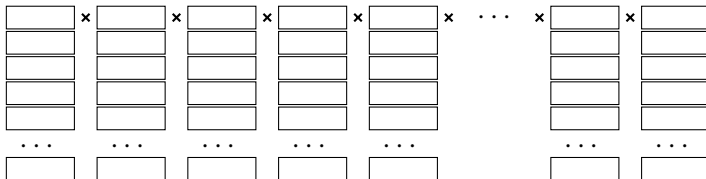
# Autres attaques D&C

Énumération : problématique

Probabilité de succès d'ordre  $o$

Probabilité que **le score de la bonne clef soit parmi les  $o$  meilleurs scores.**

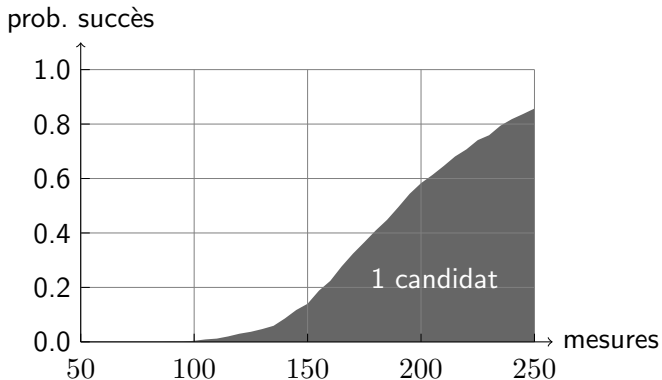
Et si on a un peu moins de chance ?





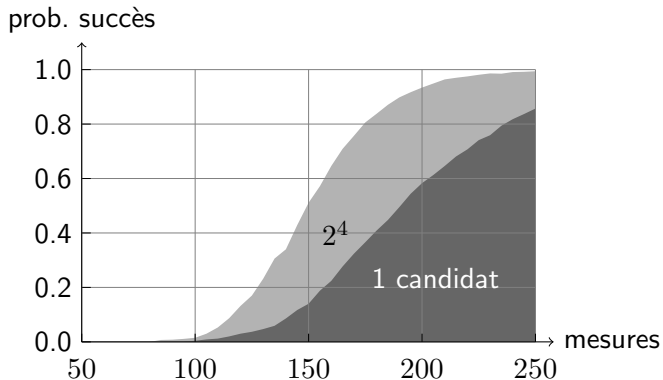
# Autres attaques D&C

Énumération : impact sur l'attaque



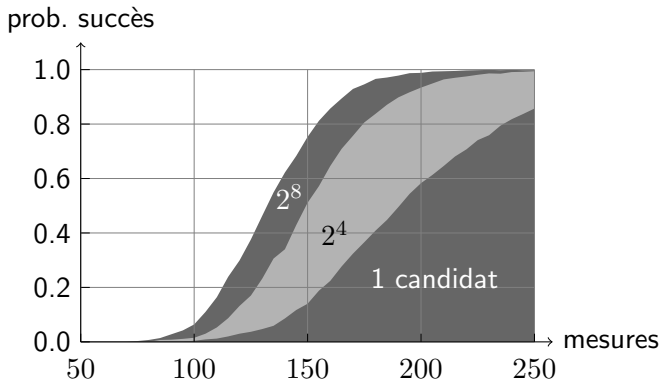
# Autres attaques D&C

Énumération : impact sur l'attaque



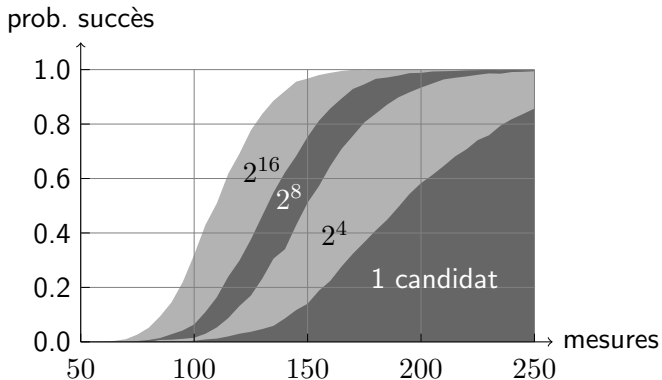
# Autres attaques D&C

Énumération : impact sur l'attaque



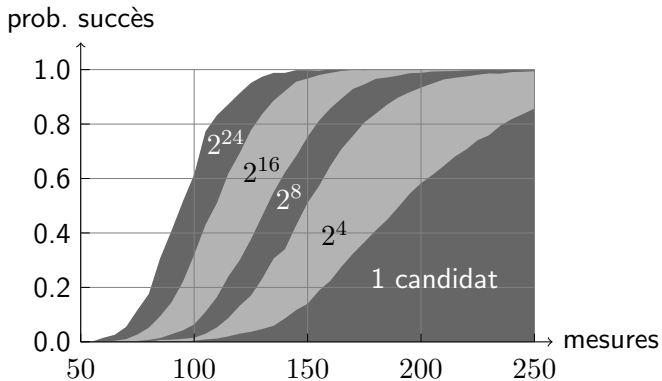
# Autres attaques D&C

Énumération : impact sur l'attaque



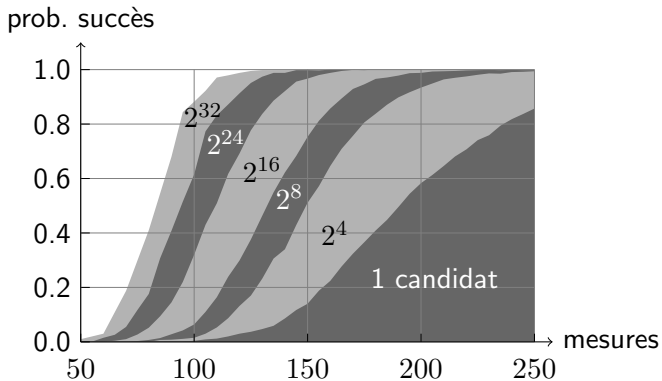
# Autres attaques D&C

Énumération : impact sur l'attaque



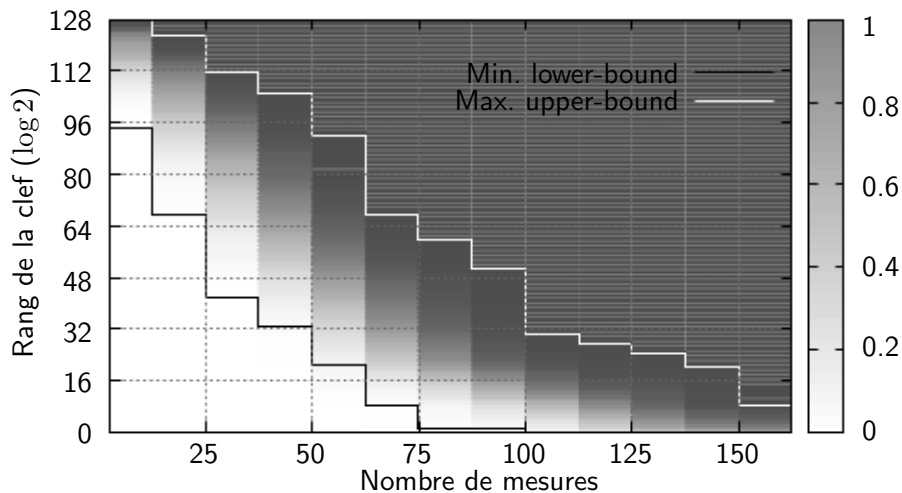
# Autres attaques D&C

Énumération : impact sur l'attaque



# Autres attaques D&C

Énumération et estimation de rang



## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures



### Augmentation du bruit :

- ▶ pipeline,
- ▶ jitter d'horloge,
- ▶ consommation parasite.

### Contre-mesures “algorithmiques”

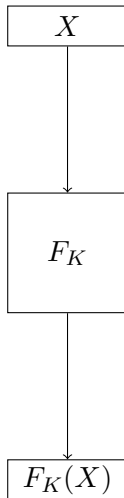
- ▶ exécution aléatoire,
- ▶ désynchronisation,
- ▶ partage de secret (masquage),
- ▶ utilisation du parallélisme.

La plupart des contre-mesures algorithmiques **nécessitent du bruit !**

### Attention

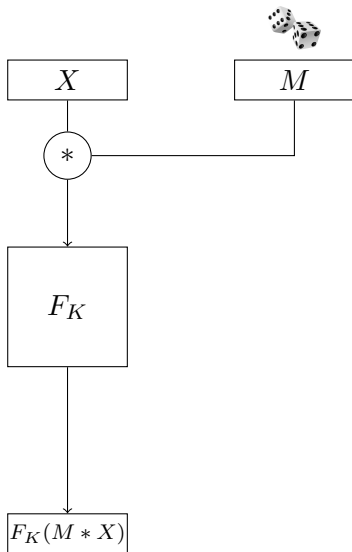
Des contremesures mal implémentées peuvent rendre l'algorithme plus vulnérable.

Calcul de  $F_K(X)$ .



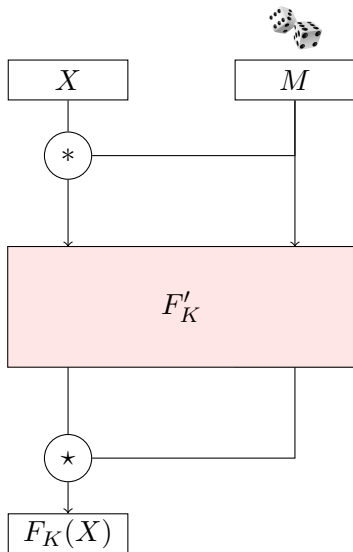
Calcul de  $F_K(X)$ .

1. Aléatorisation des calculs.

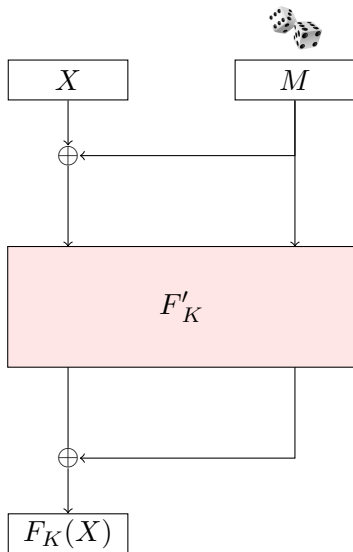


Calcul de  $F_K(X)$ .

1. Aléatorisation des calculs.
2. Ajout d'un circuit compensatoire.

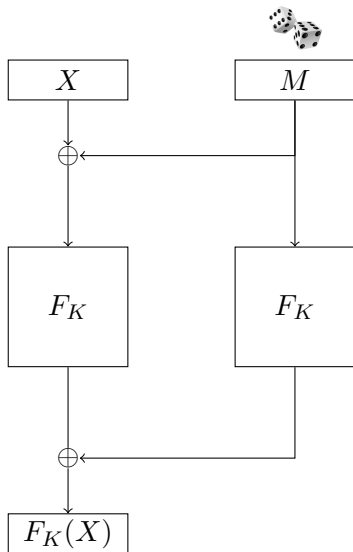


- Combinaison par XOR.



- Combinaison par XOR.
- Facile si  $F_K$  linéaire.

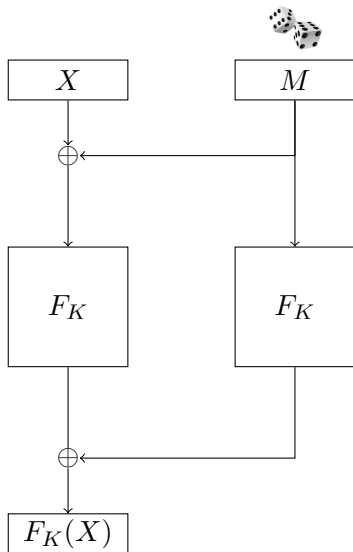
$$F_K(X \oplus M) = F_K(X) \oplus F_K(M)$$



- Combinaison par XOR.
- Facile si  $F_K$  linéaire.

$$F_K(X \oplus M) = F_K(X) \oplus F_K(M)$$

- Quid si  $F_K$  non linéaire (eg. boîte-S) ?

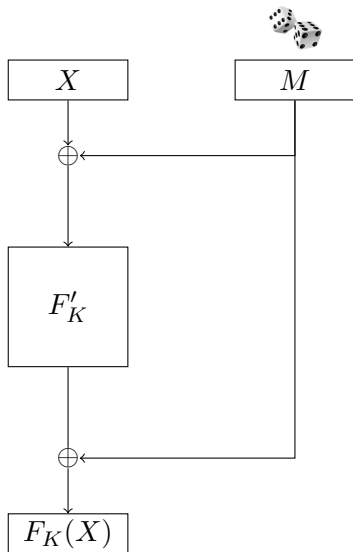


- ▶ Combinaison par XOR.
- ▶ Facile si  $F_K$  linéaire.

$$F_K(X \oplus M) = F_K(X) \oplus F_K(M)$$

- ▶ Quid si  $F_K$  non linéaire (eg. boîte-S)?
  - ▶ Calculer  $F'_K$  à chaque tirage de  $M$

$$F'_K(X \oplus M) = F_K(X) \oplus M$$





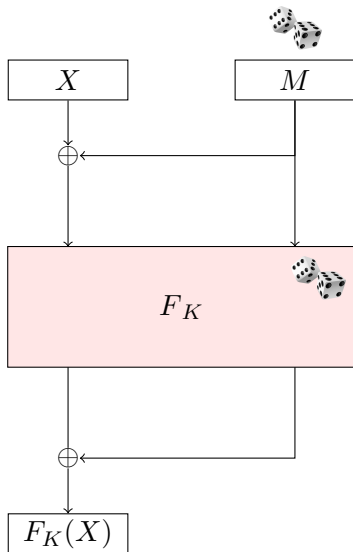
- ▶ Combinaison par XOR.
- ▶ Facile si  $F_K$  linéaire.

$$F_K(X \oplus M) = F_K(X) \oplus F_K(M)$$

- ▶ **Quid si  $F_K$  non linéaire (eg. boîte-S) ?**
  - ▶ Calculer  $F'_K$  à chaque tirage de  $M$

$$F'_K(X \oplus M) = F_K(X) \oplus M$$

- ▶ On s'autorise des “communications” entre les branches
  - ▶ nécessite de l'aléa en plus.



### Exemple

Masquage à l'ordre 1 : deux registres de 4 bits.

$S$	$M$	$S \oplus M$	$HW(\cdot)$
0000	0110	0110	4
	0010	0010	2
	1110	1110	6
	1001	1001	4

### Exemple

Masquage à l'ordre 1 : deux registres de 4 bits.

$S$	$M$	$S \oplus M$	$HW(\cdot)$
1111	0110	1001	4
	0010	1101	4
	1110	0001	4
	1001	0110	4

### Exemple

Masquage à l'ordre 1 : deux registres de 4 bits.

$S$	$M$	$S \oplus M$	$HW(\cdot)$
1111	0110	1001	4
	0010	1101	4
	1110	0001	4
	1001	0110	4

L'information se trouve dans la variance et plus la moyenne.

## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures

# Attaques à plusieurs mesures

## Différences avec le symétrique

- ▶ taille des données,
  - ▶ 128 → 256 à 2048 bits
- ▶ complexité des calculs,
- ▶ temps des calculs.
  - ▶ dizaines à milliers de cycles → milliers à millions de cycles
- ▶ relation mathématiques entre les données,

### Relations mathématiques : implications

Sécurité d'un AES-128 dont on connaît 1/4 des bit de clef :  $2^{96}$

Sécurité de RSA si on connaît 1/4 des bits de clef : peut être quasi nulle si le module n'est pas trop grand.

# Attaques à plusieurs mesures

## Opérations ciblées

Tout ce qui manipule des données sensibles :

- ▶ Exponentiation modulaire,
- ▶ Multiplication de point (sur courbe),
- ▶ Addition/soustraction,
- ▶ Multiplication,
- ▶ Inversion  $\text{mod } n$ ,
- ▶ ...

Attaques de type DPA (plusieurs traces)

Contrées par la randomisation (cf. suite).

# Attaques à plusieurs mesures

Collisions : exemple de la doubling attack

Algorithme d'exemple : Montgomery Ladder

$i$	$d_i$	$R_0$ pour $c^d$	$R_0$ pour $(c^2)^d$
6	1	$c^1$	$c^2$
5	0	$c^2$	$c^4$
4	0	$c^4$	$c^8$
3	1	$c^9$	$c^{18}$
2	1	$c^{19}$	$c^{38}$
1	0	$c^{38}$	$c^{76}$
0	1	$c^{77}$	$c^{154}$



## Introduction aux attaques par canaux auxiliaires

- Généralités sur les attaques non-invasives

- Simple Power Analysis (SPA)

## Cryptographie symétrique

- Differential Power Analysis (DPA)

- Correlation Power Analysis (CPA)

- Autres attaques Divide & Conquer

- Contremesures

## Cryptographie asymétrique

- Attaques à plusieurs mesures

- Contremesures

La DPA ne fonctionne que si on a un calcul qui manipule secret **et donnée connue**.

Calculs manipulant un secret  $s$  masqués avec un aléa  $a$  :

►  $x + s \rightarrow ((s + a) + x) - a$

►  $x \times s \rightarrow ((s \times a) \times x) \times a^{-1}$

►  $s^{-1} \rightarrow (s \times a)^{-1} \times a$

## Principe

Au lieu de calculer  $c^d \bmod N$ ,

- ▶ on tire un aléa  $\lambda$ ,
  - ▶ on calcule  $c^{d+\lambda \cdot \varphi(N)} \bmod N$ .
- 
- ▶ Par construction on obtient le même résultat.
  - ▶ L'exposant change à chaque fois  $\Rightarrow$  attaquant limité à 1 trace.

## Précaution

Prendre  $\lambda$  suffisamment grand sinon on obtient facilement plusieurs traces avec le même  $\lambda$ .

## Principe

Au lieu de calculer  $c^d \bmod N$ ,

- ▶ on tire un nombre aléatoire  $a < N$ ,
- ▶ on calcule  $(a \cdot c)^d / a^d \bmod N$ .

Le but est d'éviter les attaques

- ▶ où  $c$  est choisi,
- ▶ qui exploitent les valeurs intermédiaires.

## Principe

Au lieu de calculer  $[k] \cdot P$  avec  $P = (X, Y, Z)$ ,

- ▶ on tire un aléa  $\lambda$ ,
  - ▶ on calcule  $[k] \cdot P'$  avec  $P' = (\lambda X, \lambda Y, \lambda Z)$ .
- 
- ▶ Par construction on obtient le même résultat.
  - ▶ Évite les attaques exploitant les valeurs intermédiaires.
  - ▶ Coût négligeable (contrairement à la précédente).

Ne fonctionne que pour les courbes et certains systèmes de coordonnées.

- ▶ Les contremesures empêchent l'utilisation de plusieurs courbes.
- ▶ Les courbes contiennent énormément d'information.
- ▶ On découpe la courbe en plusieurs petits morceaux pour
  - ▶ faire des attaques de type DPA,
  - ▶ faire des attaques de type collisions.

### Exemple d'attaque horizontale type DPA

$$\begin{array}{r} s_2 \ s_1 \ s_0 \\ \times \quad x_4 \ x_3 \ x_2 \ x_1 \ x_0 \end{array}$$

Alors, DPA sur  $s_i$  avec 5 traces correspondant à  $x_0, x_1, x_2, x_3$  et  $x_4$ .

## Messages

- ▶ Comblers les trous avec des opérations fantômes ne protège pas contre les attaques locales.
- ▶ Pour se protéger il faut du bruit :
  - ▶ source physique,
  - ▶ source algorithmique,
- ▶ et de l'aléa.

## Bonnes pratiques

- ▶ Bien réfléchir au modèle d'attaquant à considérer.
- ▶ Limiter les manipulations inutiles de données secrètes (ou liées aux données secrètes).