Réduire le nombre de traces en CPA

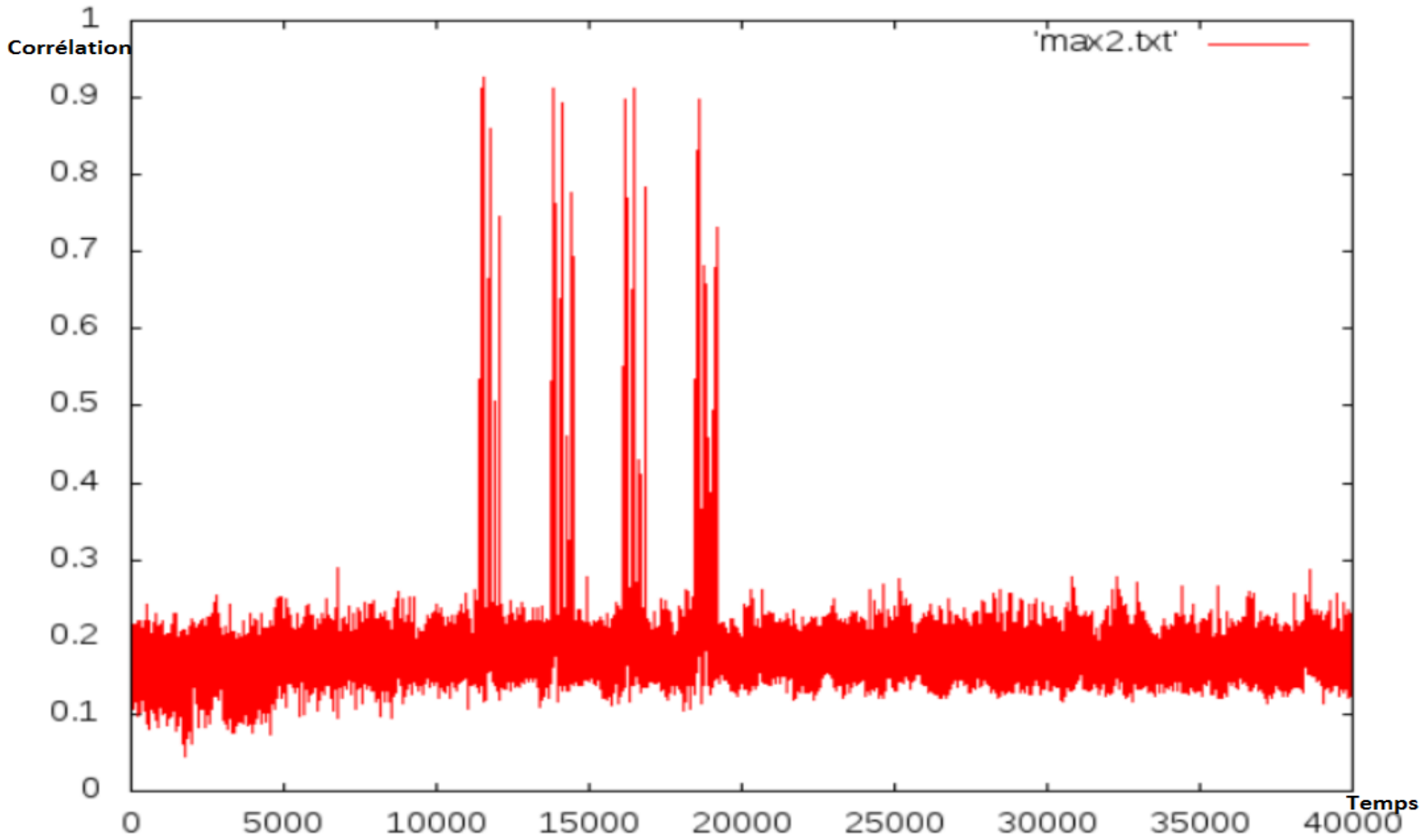
Crypto'Puces 2017

M. Ouladj, P. Guillot, F. Mokrane

LAGA CNRS (UMR 7539) Univ.paris8

1 juin 2017

Introduction/Motivation



Résultat d'une attaque CPA avec toutes les traces possibles (2^n clairs)

Sommaire

- Modélisation de l'attaque ;

Sommaire

- Modélisation de l'attaque ;
- Attaque de l'entrée de la S-Box (1^{er} tour AES) ;

Sommaire

- Modélisation de l'attaque ;
- Attaque de l'entrée de la S-Box (1^{er} tour AES) ;
- Attaque de la sortie de la S-Box (1^{er} tour AES) ;

Sommaire

- Modélisation de l'attaque ;
- Attaque de l'entrée de la S-Box (1^{er} tour AES) ;
- Attaque de la sortie de la S-Box (1^{er} tour AES) ;
- Conclusions et perspectives ;

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$

$$\begin{array}{rccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & Hw(k \oplus x) \end{array}$$

$Hw(k \oplus x)$	x=0	x=1	x=2	x=3	x=4	x=5	x=6	x=7
k=0	0	1	1	2	1	2	2	3
k=1	1	0	2	1	2	1	3	2
k=2	1	2	0	1	2	3	1	2
k=3	2	1	1	0	3	2	2	1
k=4	1	2	2	3	0	1	1	2
k=5	2	1	3	2	1	0	2	1
k=6	2	3	1	2	1	2	0	1
k=7	3	2	2	1	2	1	1	0

La fonction modèle de fuite

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$, $SX = \{0,1,2\} \subset X$

$$\begin{array}{rcccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & Hw(k \oplus x) \end{array}$$

$Hw(k \oplus x)$	x=0	x=1	x=2	x=3	x=4	x=5	x=6	x=7
k=0	0	1	1	2	1	2	2	3
k=1	1	0	2	1	2	1	3	2
k=2	1	2	0	1	2	3	1	2
k=3	2	1	1	0	3	2	2	1
k=4	1	2	2	3	0	1	1	2
k=5	2	1	3	2	1	0	2	1
k=6	2	3	1	2	1	2	0	1
k=7	3	2	2	1	2	1	1	0

La fonction modèle de fuite sur un sous ensemble

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$, $SX = \{0,1,2\} \subset X$

$$\begin{array}{rcccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & Hw(k \oplus x) \end{array}$$

$Hw(k \oplus x)$	x=0	x=1	x=2	x=3	x=4	x=5	x=6	x=7
k=0	0	1	1	2	1	2	2	3
k=1	1	0	2	1	2	1	3	2
k=2	1	2	0	1	2	3	1	2
k=3	2	1	1	0	3	2	2	1
k=4	1	2	2	3	0	1	1	2
k=5	2	1	3	2	1	0	2	1
k=6	2	3	1	2	1	2	0	1
k=7	3	2	2	1	2	1	1	0

La fonction modèle de fuite sur un sous ensemble

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$, $SX = \{0,1,2\} \subset X$

$$\begin{array}{rcccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & Hw(k \oplus x) \end{array}$$

$Hw(k \oplus x)$	x=0	x=1	x=2	x=3	x=4	x=5	x=6	x=7
k=0	0	1	1	2	1	2	2	3
k=1	1	0	2	1	2	1	3	2
k=2	1	2	0	1	2	3	1	2
k=3	2	1	1	0	3	2	2	1
k=4	1	2	2	3	0	1	1	2
k=5	2	1	3	2	1	0	2	1
k=6	2	3	1	2	1	2	0	1
k=7	3	2	2	1	2	1	1	0

La fonction modèle de fuite sur un sous ensemble

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$, $SX = \{0,1,2\} \subset X$

$$\begin{array}{rcccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & Hw(k \oplus x) \end{array}$$

$Hw(k \oplus x)$	x=0	x=1	x=2	x=3	x=4	x=5	x=6	x=7
k=0	0	1	1	2	1	2	2	3
k=1	1	0	2	1	2	1	3	2
k=2	1	2	0	1	2	3	1	2
k=3	2	1	1	0	3	2	2	1
k=4	1	2	2	3	0	1	1	2
k=5	2	1	3	2	1	0	2	1
k=6	2	3	1	2	1	2	0	1
k=7	3	2	2	1	2	1	1	0

La fonction modèle de fuite sur un sous ensemble

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$

$$\begin{array}{rccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & L(k \oplus x) \end{array}$$

$L(k \oplus x)$	$x = 0$	$x = 1$	$\cdots$	$x = 2^n - 1$
0	$L(0,0)$	$L(0,1)$	$\cdots$	$L(0, 2^n - 1)$
1	$L(1,0)$	$L(1,1)$	$\cdots$	$L(1, 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k	$L(k,0)$	$L(k,1)$	$\cdots$	$L(k, 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k'	$L(k',0)$	$L(k',1)$	$\cdots$	$L(k', 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$2^n - 1$	$L(2^n - 1, 0)$	$L(2^n - 1, 1)$	$\cdots$	$L(2^n - 1, 2^n - 1)$

La fonction modèle de fuite

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$

$$\begin{array}{rccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & L(k \oplus x) \end{array}$$

$L(k \oplus x)$	$x = 0$	$x = 1$	$\cdots$	$x = 2^n - 1$
0	$L(0,0)$	$L(0,1)$	$\cdots$	$L(0, 2^n - 1)$
1	$L(1,0)$	$L(1,1)$	$\cdots$	$L(1, 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k	$L(k,0)$	$L(k,1)$	$\cdots$	$L(k, 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k'	$L(k',0)$	$L(k',1)$	$\cdots$	$L(k', 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$2^n - 1$	$L(2^n - 1, 0)$	$L(2^n - 1, 1)$	$\cdots$	$L(2^n - 1, 2^n - 1)$

La fonction modèle de fuite

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$

$$\begin{array}{rccc} L & : & K \times X & \rightarrow & \mathbb{R} \\ & & (k,x) & \mapsto & L(k \oplus x) \end{array}$$

$L(k \oplus x)$	$x = 0$	$x = 1$	$\cdots$	$x = 2^n - 1$
0	$L(0,0)$	$L(0,1)$	$\cdots$	$L(0, 2^n - 1)$
1	$L(1,0)$	$L(1,1)$	$\cdots$	$L(1, 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k	$L(k,0)$	$L(k,1)$	$\cdots$	$L(k, 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k'	$L(k',0)$	$L(k',1)$	$\cdots$	$L(k', 2^n - 1)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$2^n - 1$	$L(2^n - 1, 0)$	$L(2^n - 1, 1)$	$\cdots$	$L(2^n - 1, 2^n - 1)$

La fonction modèle de fuite

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$, $SX = \{x_1, ..., x_m\} \subset X$

$$\begin{array}{rccc} L & : & K \times SX & \rightarrow & \mathbb{R} \\ & & (k, x_i) & \mapsto & L(k \oplus x_i) \end{array}$$

$L(k \oplus x)$	x_0	x_1	$\cdots$	x_m
0	$L(0, x_0)$	$L(0, x_1)$	$\cdots$	$L(0, x_m)$
1	$L(1, x_0)$	$L(1, x_1)$	$\cdots$	$L(1, x_m)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k	$L(k, x_0)$	$L(k, x_1)$	$\cdots$	$L(k, x_m)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k'	$L(k', x_0)$	$L(k', x_1)$	$\cdots$	$L(k', x_m)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$2^n - 1$	$L(2^n - 1, x_0)$	$L(2^n - 1, x_1)$	$\cdots$	$L(2^n - 1, x_m)$

La fonction modèle de fuite sur un sous-ensemble de traces

Principe d'attaque : la fonction modèle de fuite

$K = X = \{0,1\}^3$, $SX = \{x_1, ..., x_m\} \subset X$

$$\begin{array}{rccc} L & : & K \times SX & \rightarrow & \mathbb{R} \\ & & (k, x_i) & \mapsto & L(k \oplus x_i) \end{array}$$

$L(k \oplus x)$	x_0	x_1	$\cdots$	x_m
0	$L(0, x_0)$	$L(0, x_1)$	$\cdots$	$L(0, x_m)$
1	$L(1, x_0)$	$L(1, x_1)$	$\cdots$	$L(1, x_m)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k	$L(k, x_0)$	$L(k, x_1)$	$\cdots$	$L(k, x_m)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
k'	$L(k', x_0)$	$L(k', x_1)$	$\cdots$	$L(k', x_m)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$2^n - 1$	$L(2^n - 1, x_0)$	$L(2^n - 1, x_1)$	$\cdots$	$L(2^n - 1, x_m)$

La fonction modèle de fuite sur un sous-ensemble de traces

on note Le vecteur $V_k = (v_{k,1}, ..., v_{k,m}) = L_k - E(L_k)$

Principe d'attaque : condition de réussite de la CPA

- La corrélation entre la fuite réelle M et la fuite estimée par le modèle pour la clé k est :

$$\rho_{M,V_k} = \frac{cov(M,V_k)}{\sigma_M.\sigma_{V_k}} = \frac{\langle M,V_k \rangle}{\|M\|\|V_k\|}$$

Principe d'attaque : condition de réussite de la CPA

- La corrélation entre la fuite réelle M et la fuite estimée par le modèle pour la clé k est :

$$\rho_{M,V_k} = \frac{cov(M,V_k)}{\sigma_M.\sigma_{V_k}} = \frac{\langle M,V_k \rangle}{\|M\|\|V_k\|}$$

- La CPA réussit si et seulement si :

$$\rho_{M,V_k} \succ \rho_{M,V_{k'}}; \forall k' \neq k \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Principe d'attaque : condition de réussite de la CPA

- La corrélation entre la fuite réelle M et la fuite estimée par le modèle pour la clé k est :

$$\rho_{M,V_k} = \frac{cov(M,V_k)}{\sigma_M.\sigma_{V_k}} = \frac{\langle M,V_k \rangle}{\|M\|\|V_k\|}$$

- La CPA réussit si et seulement si :

$$\rho_{M,V_k} \succ \rho_{M,V_{k'}}; \forall k' \neq k \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

- Comme la fuite mesurée M correspond à la bonne clé k, alors :
  $M = V_k + N$;
  $V_k = (v_{k,1}, ..., v_{k,m})$ la fuite qui correspond à la bonne clé k
  $N = (N_1, ..., N_m)$ erreurs du modèle et de mesures

Principe d'attaque : condition de réussite de la CPA

- $(1) \Longleftrightarrow \rho_{M,V_k} \succ \rho_{M,V_{k'}}; \forall k' \neq k$
  comme $M = V_k + N$ alors,

1. SNR :Rapport Signal sur Bruit

Principe d'attaque : condition de réussite de la CPA

- $(1) \Longleftrightarrow \rho_{M,V_k} \succ \rho_{M,V_{k'}}; \forall k' \neq k$
  comme $M = V_k + N$ alors,
  $(1) \Longleftrightarrow 1 - \frac{\langle V_k, V_{k'} \rangle}{\|V_k\| \|V_{k'}\|} \succ \left\langle \frac{N}{\|V_k\|}, \frac{V_k}{\|V_k\|} - \frac{V_{k'}}{\|V_{k'}\|} \right\rangle$

1. SNR :Rapport Signal sur Bruit

Principe d'attaque : condition de réussite de la CPA

- $(1) \Longleftrightarrow \rho_{M,V_k} \succ \rho_{M,V_{k'}}; \forall k' \neq k$
  comme $M = V_k + N$ alors,
  $(1) \Longleftrightarrow 1 - \frac{\langle V_k, V_{k'} \rangle}{\|V_k\| \|V_{k'}\|} \succ \left\langle \frac{N}{\|V_k\|}, \frac{V_k}{\|V_k\|} - \frac{V_{k'}}{\|V_{k'}\|} \right\rangle$

- $\frac{2}{SNR}$ [1] $= 2\frac{\|N\|}{\|V_k\|} \succ \left| \left\langle \frac{N}{\|V_k\|}, \frac{V_k}{\|V_k\|} - \frac{V_{k'}}{\|V_{k'}\|} \right\rangle \right|; \forall k' \neq k$

(l'inégalité de Cauchy-Schwarz)

1. SNR :Rapport Signal sur Bruit

Principe d'attaque : condition de réussite de la CPA

- $(1) \Longleftrightarrow \rho_{M,V_k} \succ \rho_{M,V_{k'}}; \forall k' \neq k$
  comme $M = V_k + N$ alors,
  $(1) \Longleftrightarrow 1 - \frac{\langle V_k, V_{k'} \rangle}{\|V_k\| \|V_{k'}\|} \succ \left\langle \frac{N}{\|V_k\|}, \frac{V_k}{\|V_k\|} - \frac{V_{k'}}{\|V_{k'}\|} \right\rangle$

- $\frac{2}{SNR}$ [1] $= 2\frac{\|N\|}{\|V_k\|} \succ \left| \left\langle \frac{N}{\|V_k\|}, \frac{V_k}{\|V_k\|} - \frac{V_{k'}}{\|V_{k'}\|} \right\rangle \right|; \forall k' \neq k$

  (l'inégalité de Cauchy-Schwarz)

- D'où, pour réussir l'attaque CPA il suffit que

$$\forall (k, k'); k' \neq k, 1 - \frac{\langle V_k, V_{k'} \rangle}{\|V_k\| \|V_{k'}\|} \succ \frac{2}{SNR}$$

1. SNR :Rapport Signal sur Bruit

Principe d'attaque : recherche des mesures adéquates

Require: $Model[2^n][2^n] \vee SNR$

Principe d'attaque : recherche des mesures adéquates

Require: $Model[2^n][2^n] \vee SNR$
Ensure: $List\_Mesures\_Choisies$

Principe d'attaque : recherche des mesures adéquates

Require: $Model[2^n][2^n] \vee SNR$
Ensure: $List\_Mesures\_Choisies$

1: $List\_Mesures\_Choisies = choisir\_une\_mesure(List\_Mesures\_Possibles)$
2: $mesure, Correlation\_courante = 1$

Principe d'attaque : recherche des mesures adéquates

Require: $Model[2^n][2^n] \vee SNR$
Ensure: $List\_Mesures\_Choisies$

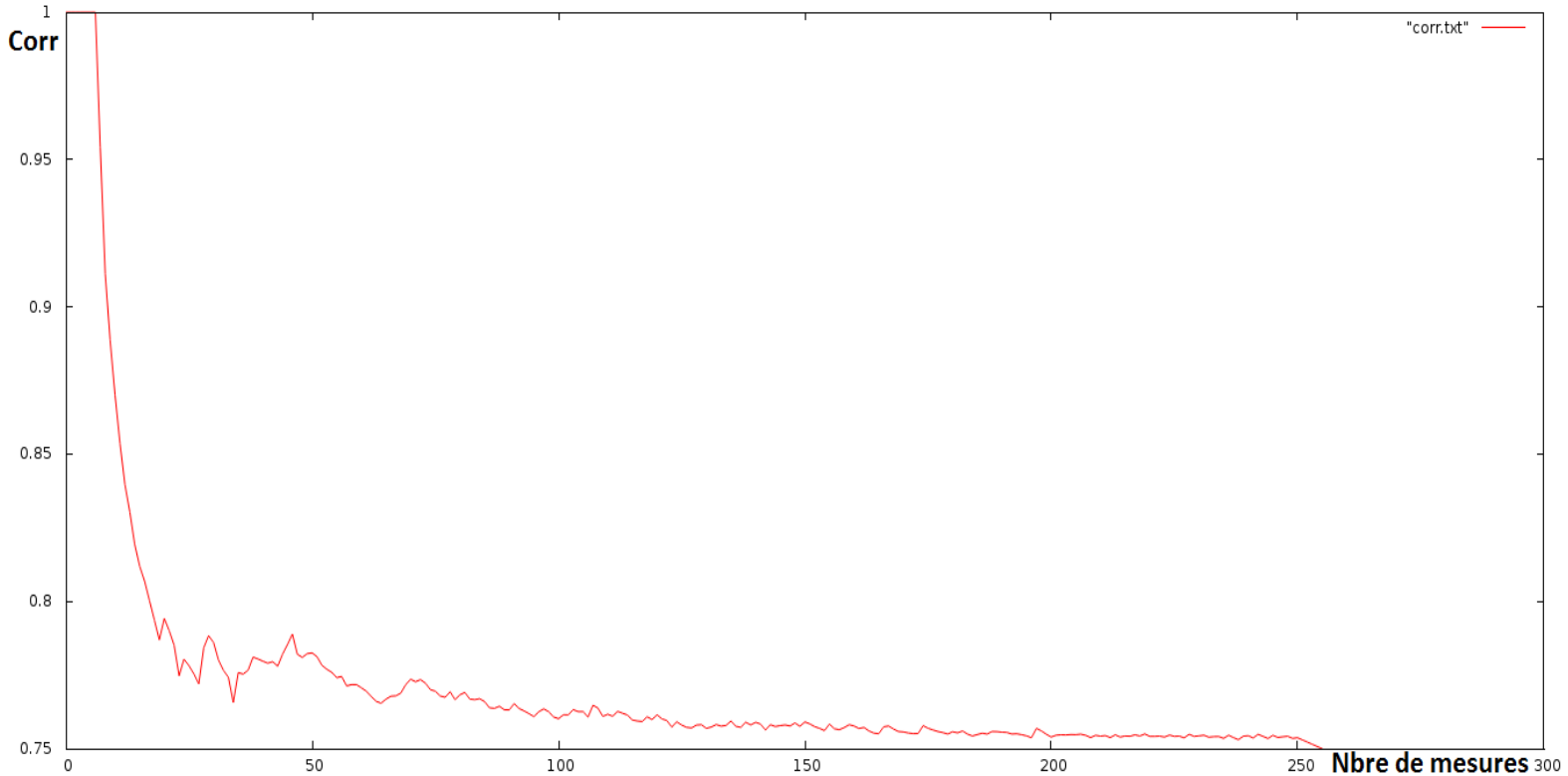
1: $List\_Mesures\_Choisies = choisir\_une\_mesure(List\_Mesures\_Possibles)$
2: $mesure, Correlation\_courante = 1$

3: **while** $\neg($ 1-Correlation_courante $\succ \frac{2}{SNR})$ **do**
4: $\quad mesure = chercher\_Min\_correlation(List\_Mesures\_Possibles)$
5: $\quad deplacer(mesure, List\_Mesures\_Possibles, List\_Mesures\_choisies)$
6: $\quad Correlation\_courante = correlation\_maximale(List\_Mesures\_choisies)$
7: **end while**

Attaque de l'entrée de la S-Box (1^{er} *tour de l'AES*)

Min_corrélation(256 mesure)=0.75.

Avec 24 mesures (10%) on est déjà à 97% (0.77)

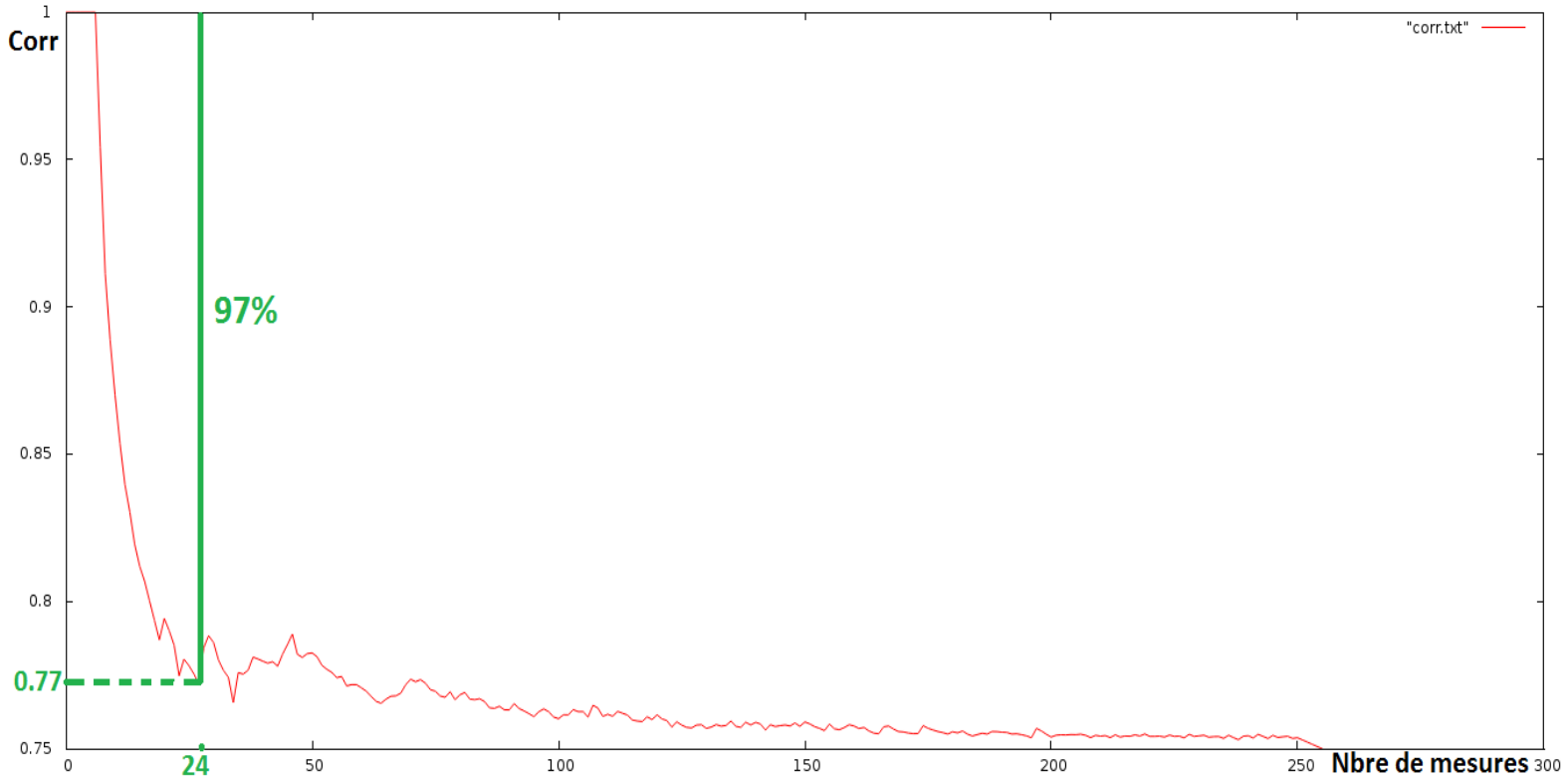


Corrélation maximale en fonction de nombre de mesures (cas de XOR)

Attaque de l'entrée de la S-Box (1^{er} *tour de l'AES*)

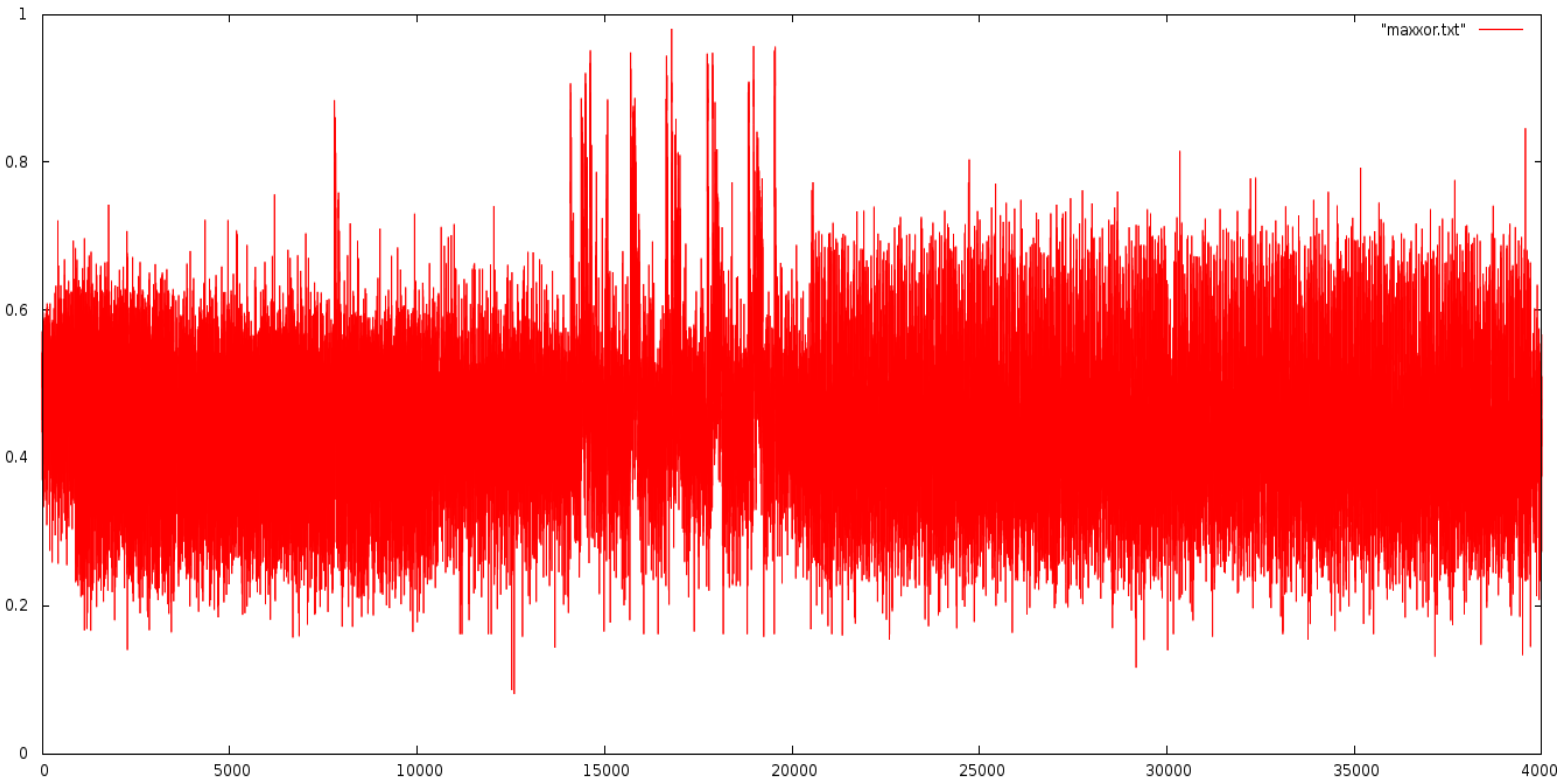
Min_corrélation(256 mesure)=0.75.

Avec 24 mesures (10%) on est déjà à 97% (0.77)



Corrélation maximale en fonction de nombre de mesures (cas de XOR)

Attaque de l'entrée de la S-Box (1^{er} *tour de l'AES*)

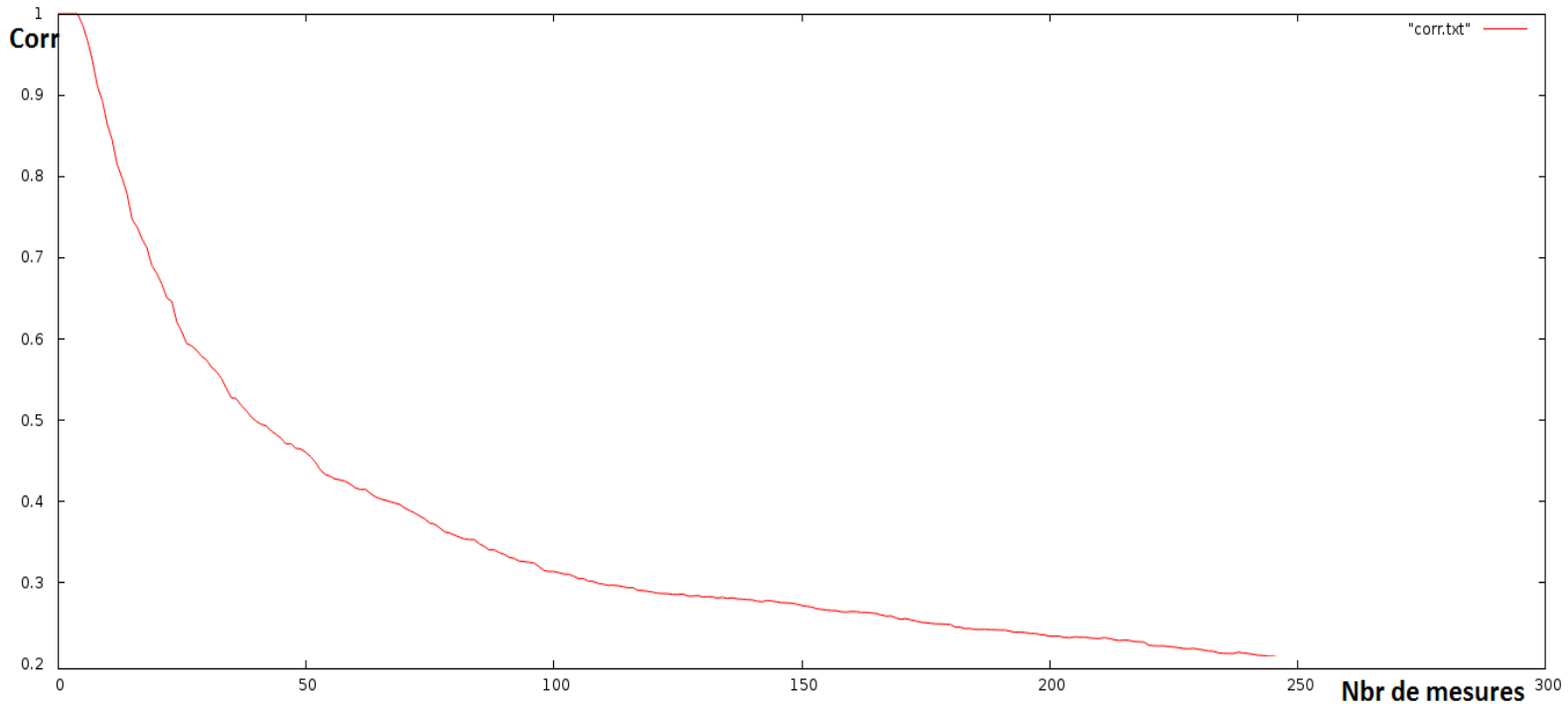


Résultat de l'attaque (cas de XOR)

Attaque de la sortie de la S-Box (1^{er} *tour de l'AES*)

Min_corrélation(256 mesure)=0.2.

Avec 26 mesures (10%) on est déjà à 50% (0.60<0.75 du cas de XOR)

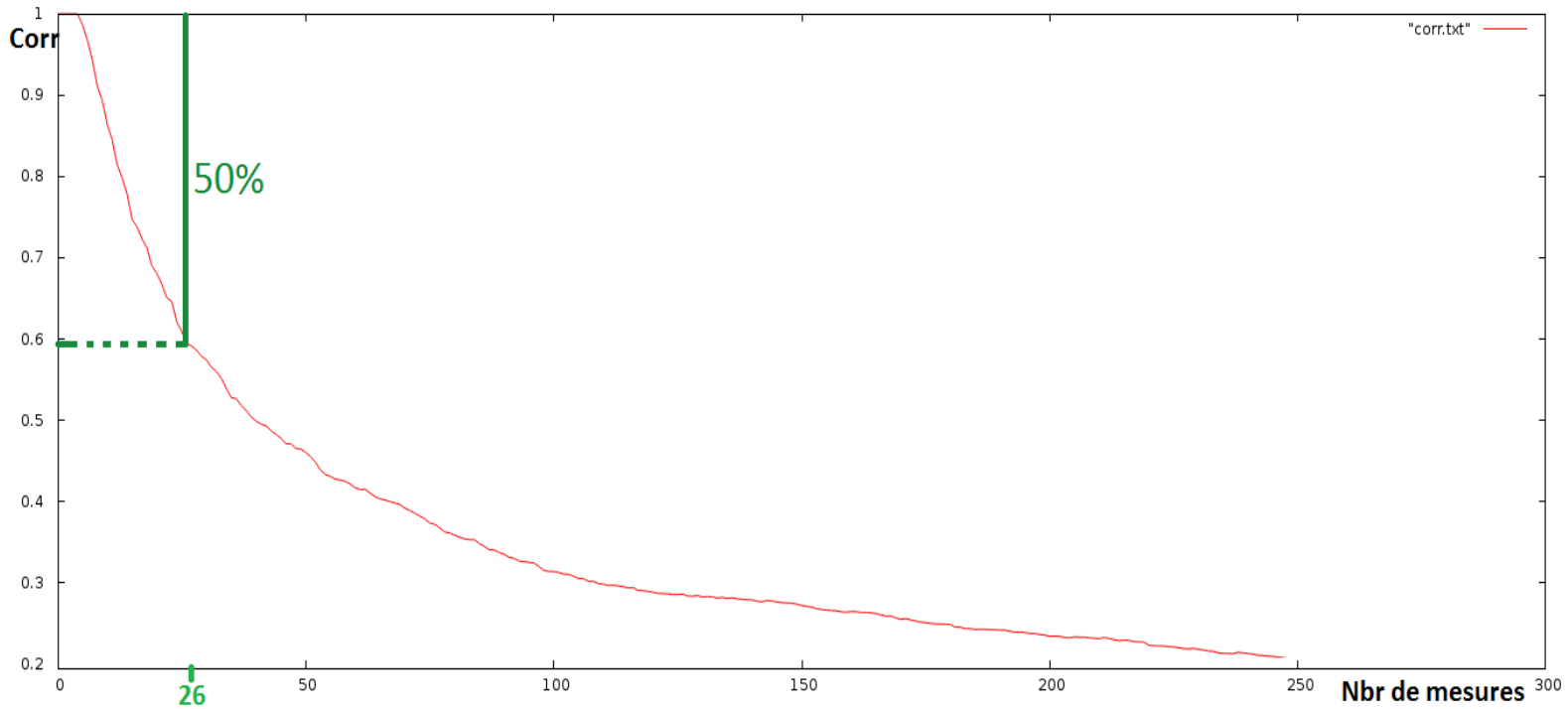


Corrélation maximale en fonction de nombre de mesures (cas de S-Box)

Attaque de la sortie de la S-Box (1^{er} *tour de l'AES*)

Min_corrélation(256 mesure)=0.2.

Avec **26 mesures** (10%) on est déjà à **50%** (0.60<0.75 du cas de XOR)

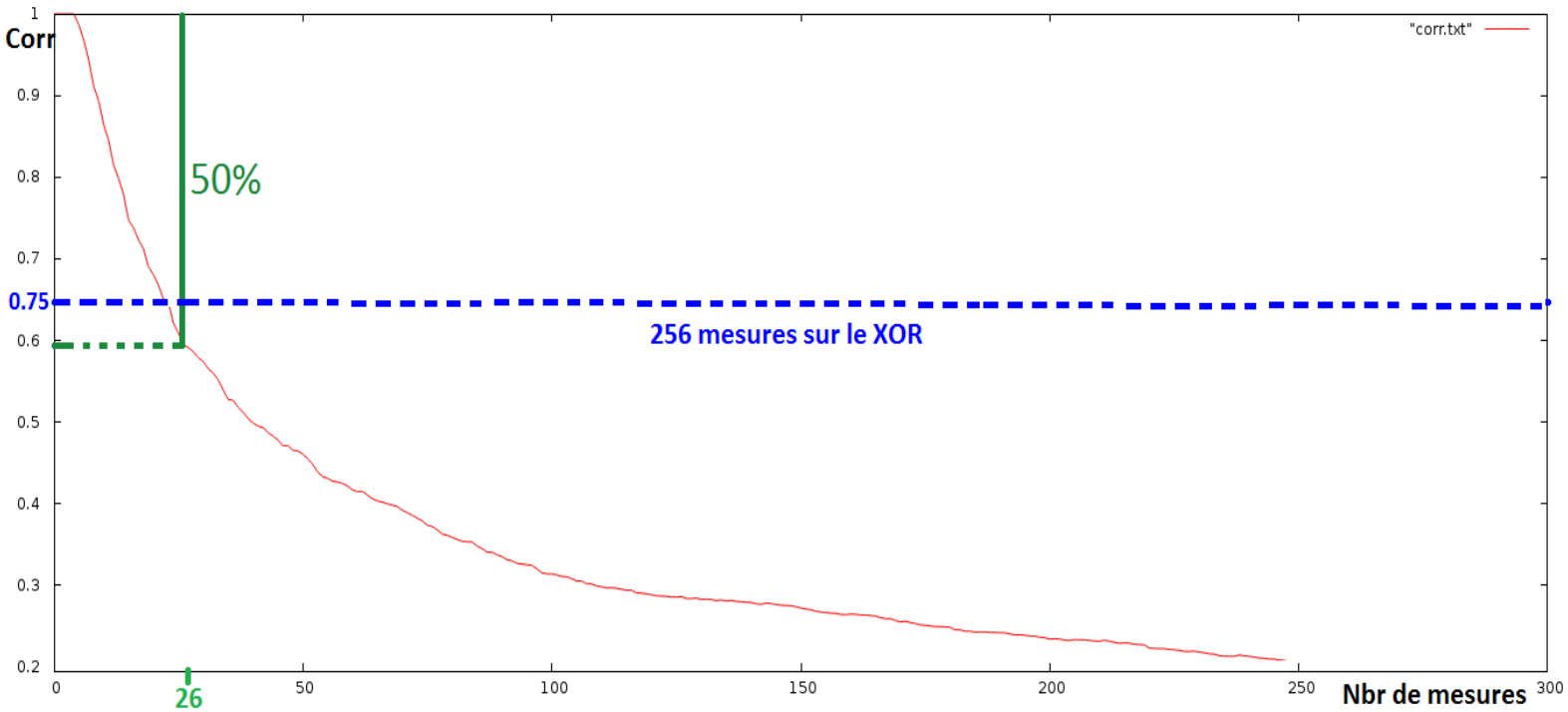


Corrélation maximale en fonction de nombre de mesures (cas de S-Box)

Attaque de la sortie de la S-Box (1^{er} *tour de l'AES*)

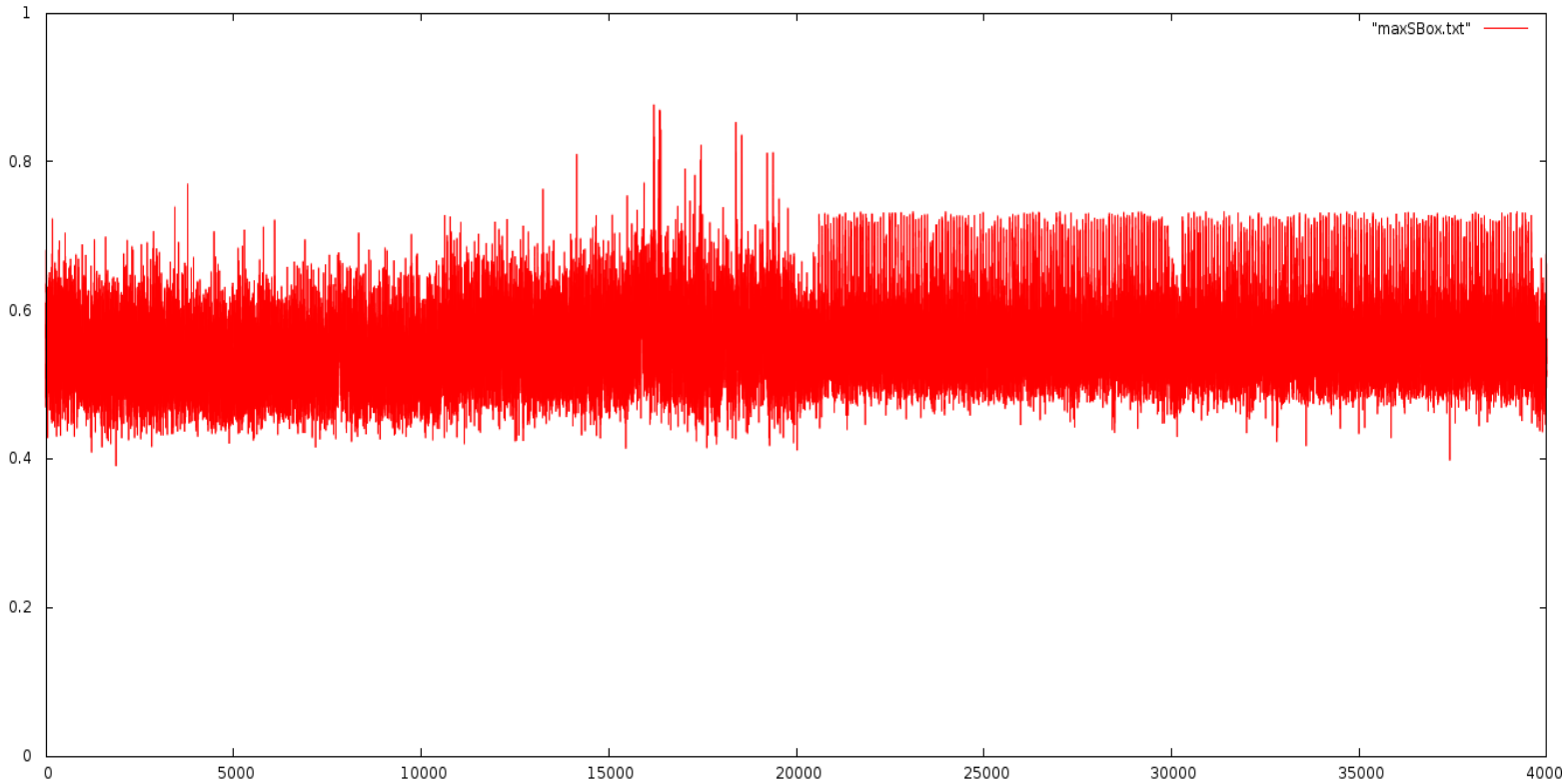
Min_corrélation(256 mesure)=0.2.

Avec 26 mesures (10%) on est déjà à 50% (0.60<0.75 du cas de XOR)



Corrélation maximale en fonction de nombre de mesures (cas de S-Box)

Attaque de la sortie de la S-Box (1^{er} *tour de l'AES*)



Résultat de l'attaque (cas de la S-Box)

Conclusions

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.
2. Complexité :

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.
2. Complexité :
    1. Pré-calcul pour trouver les traces optimales : $m * 2^{2n}$.

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.
2. Complexité :
   1. Pré-calcul pour trouver les traces optimales : $m * 2^{2n}$.
   2. Recherche des sous clés :$2^m * 2^n$.

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.
2. Complexité :
   1. Pré-calcul pour trouver les traces optimales : $m * 2^{2n}$.
   2. Recherche des sous clés :$2^m * 2^n$.

Perspectives

1. Attaque de plusieurs points pour minimiser encore le nombre de traces.

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.
2. Complexité :
   1. Pré-calcul pour trouver les traces optimales : $m * 2^{2n}$.
   2. Recherche des sous clés :$2^m * 2^n$.

Perspectives

1. Attaque de plusieurs points pour minimiser encore le nombre de traces.
2. Masquage et choix de mesures.

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.
2. Complexité :
   1. Pré-calcul pour trouver les traces optimales : $m * 2^{2n}$.
   2. Recherche des sous clés :$2^m * 2^n$.

Perspectives

1. Attaque de plusieurs points pour minimiser encore le nombre de traces.
2. Masquage et choix de mesures.
3. Amélioration du pré-calcul des traces optimales.

Conclusions & perspectives

Conclusions

1. Réduction du nombre de traces.
2. Complexité :
   1. Pré-calcul pour trouver les traces optimales : $m * 2^{2n}$.
   2. Recherche des sous clés :$2^m * 2^n$.

Perspectives

1. Attaque de plusieurs points pour minimiser encore le nombre de traces.
2. Masquage et choix de mesures.
3. Amélioration du pré-calcul des traces optimales.
4. Approche spectrale pour réduire la complexité du calcul à $m * 2^n$.

Réduire le nombre de traces en CPA

Merci pour votre attention