Sécurisation du transport de données

Cryptographie symétrique

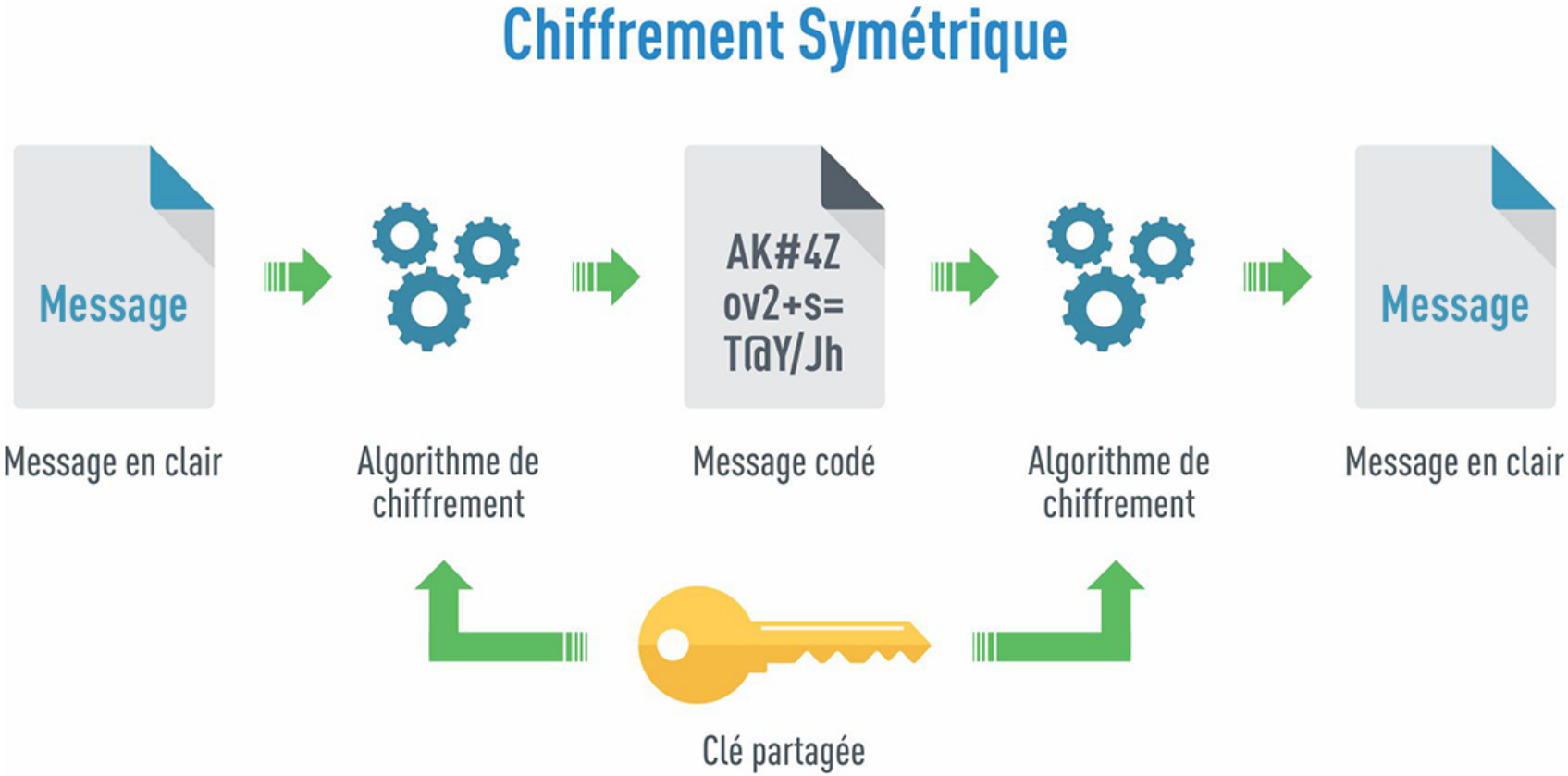
Baptiste Pasquier

Lycée privé Sainte-Geneviève

2018-2019

1. Cryptographie symétrique
   - Cryptographie symétrique
   - Chiffrement SPN
2. Cryptanalyse différentielle
   - Définitions
   - Tableau de distribution des différences
3. Conception d'un chiffrement SPN
   - Couche de substitution/confusion

Cryptographie symétrique



Source: `blog.emsisoft.com`

Définition 1 : Réseau de substitution-permutation

Un **réseau de substitution-permutation** est une architecture de chiffrement par bloc constituée d'une couche d'addition de clé, d'une couche de substitution et d'une couche de permutation

Définition 1 : Réseau de substitution-permutation

Un **réseau de substitution-permutation** est une architecture de chiffrement par bloc constituée d'une couche d'addition de clé, d'une couche de substitution et d'une couche de permutation

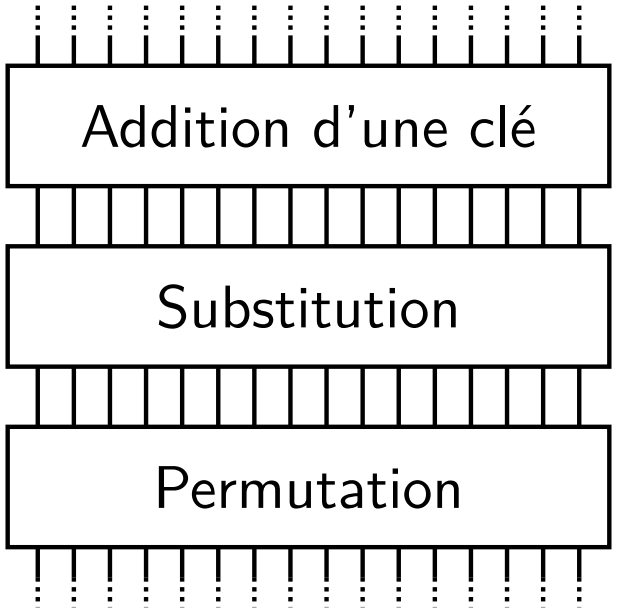


FIGURE – Tour d'un SPN sur 16 bits

Définition 2 : Fonction XOR

On définit la fonction OU exclusif (XOR, $\oplus$) par sa table de vérité :

x	0	0	1	1
y	0	1	0	1
$x \oplus y$	0	1	1	0

Définition 2 : Fonction XOR

On définit la fonction OU exclusif (XOR, $\oplus$) par sa table de vérité :

x	0	0	1	1
y	0	1	0	1
$x \oplus y$	0	1	1	0

On note $\mathbb{F}_2$ le corps $\mathbb{Z}/2\mathbb{Z}$.

Définition 3 : Extension à $\mathbb{F}_2^n$

Soit $n \in \mathbb{N}^*$. On étend la définition de la fonction $\oplus$ pour définir la fonction $\oplus : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ par :

$$\oplus : \begin{cases} \mathbb{F}_2^n \times \mathbb{F}_2^n & \longrightarrow \mathbb{F}_2^n \\ (x_1, \ldots, x_n), (y_1, \ldots, y_n) & \longmapsto x_1 \oplus y_1, \ldots, x_n \oplus y_n \end{cases}$$

Définition 4 : Fonction booléenne

Une fonction booléenne de n variables est une fonction de $\mathbb{F}_2^n$ dans $\mathbb{F}_2$.

Définition 4 : Fonction booléenne

Une fonction booléenne de n variables est une fonction de $\mathbb{F}_2^n$ dans $\mathbb{F}_2$.

x_1	0	1	0	1
x_2	0	0	1	1
$f(x_1, x_2)$	0	1	0	0

TABLE – Table de vérité d'une fonction booléenne de 2 variables

Définition 5 : Sbox

Une table de substitution (Sbox) est la table de vérité d'une fonction de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^n$. Elle est donc composée de n fonctions booléennes de m variables.

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$S_1(x_1, x_2, x_3, x_4)$	0	0	1	1	0	1	1	0	1	0	0	0	1	1	0	1
$S_2(x_1, x_2, x_3, x_4)$	1	0	0	0	1	1	1	0	1	1	1	0	0	0	0	1
$S_3(x_1, x_2, x_3, x_4)$	1	1	1	0	0	1	0	0	0	0	1	1	1	0	0	1
$S_4(x_1, x_2, x_3, x_4)$	1	0	1	0	0	1	1	1	0	1	0	1	0	1	0	0

TABLE – Sbox de $\mathbb{F}_2^4$ dans $\mathbb{F}_2^4$

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$S_1(x_1, x_2, x_3, x_4)$	0	0	1	1	0	1	1	0	1	0	0	0	1	1	0	1
$S_2(x_1, x_2, x_3, x_4)$	1	0	0	0	1	1	1	0	1	1	1	0	0	0	0	1
$S_3(x_1, x_2, x_3, x_4)$	1	1	1	0	0	1	0	0	0	0	1	1	1	0	0	1
$S_4(x_1, x_2, x_3, x_4)$	1	0	1	0	0	1	1	1	0	1	0	1	0	1	0	0

TABLE – Sbox de $\mathbb{F}_2^4$ dans $\mathbb{F}_2^4$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	e	4	d	1	2	f	b	8	3	a	6	c	5	9	0	7

TABLE – Même Sbox en écriture hexadécimale

Définition 6 : Pbox

Une table de permutation (Pbox) est le tableau de valeurs d'une bijection de $\{0, \ldots, n-1\}$.

Définition 6 : Pbox

Une table de permutation (Pbox) est le tableau de valeurs d'une bijection de $\{0, \ldots, n-1\}$.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$P(x)$	0	4	8	c	1	5	9	d	2	6	a	e	3	7	b	f

TABLE – Pbox

Définition 6 : Pbox

Une table de permutation (Pbox) est le tableau de valeurs d'une bijection de $\{0, \ldots, n-1\}$.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$P(x)$	0	4	8	c	1	5	9	d	2	6	a	e	3	7	b	f

TABLE – Pbox

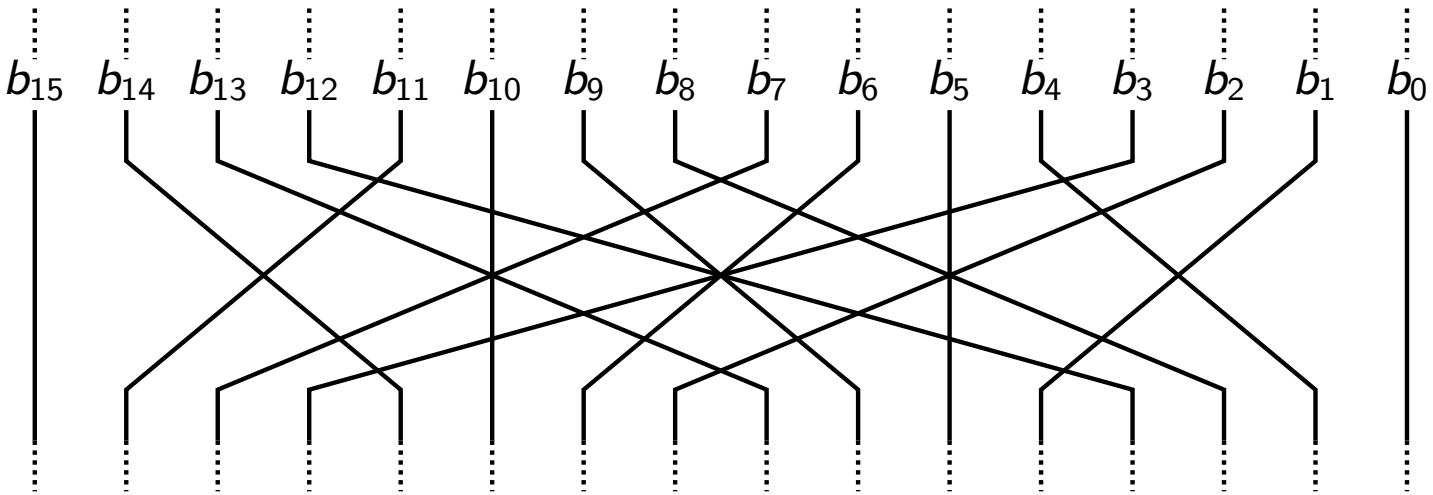
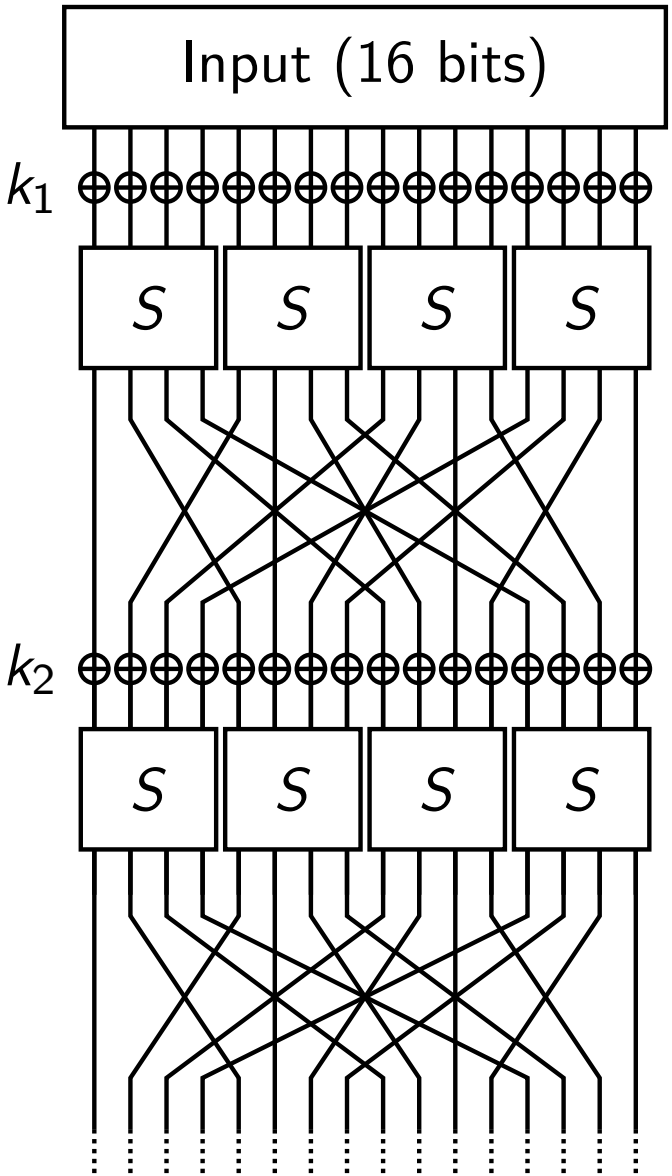
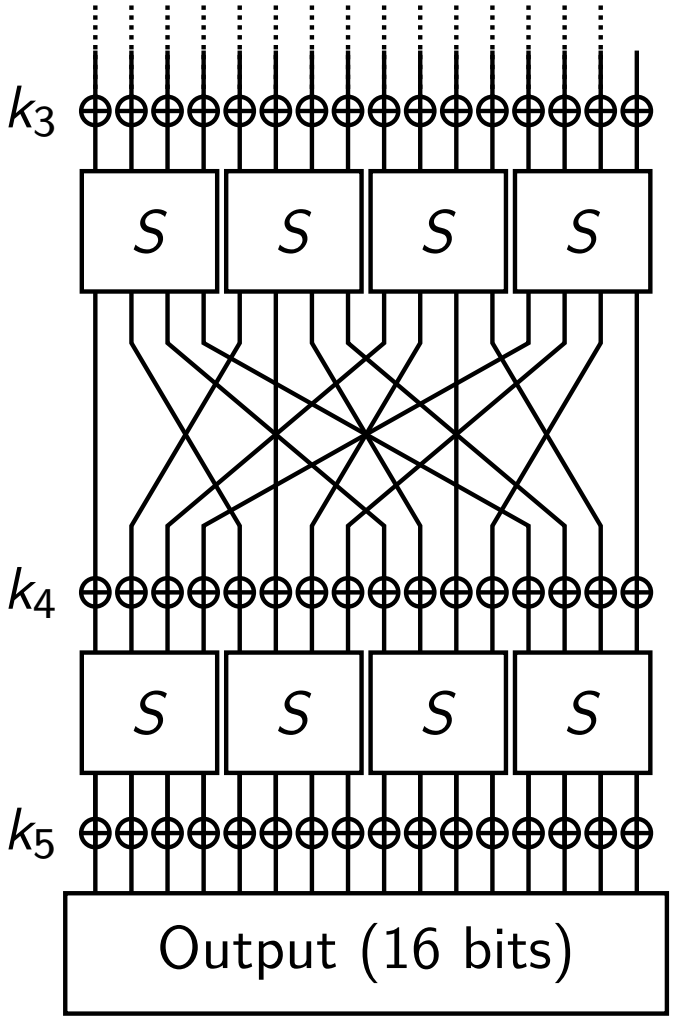


FIGURE – Schéma de la Pbox


Input (16 bits)
k_1
S S S S
k_2
S S S S


k_3
S S S S
k_4
S S S S
k_5
Output (16 bits)

Problème

Comment retrouver les clés k_i en supposant pouvoir appliquer l'algorithme de chiffrement à n'importe quelle chaine ?

Soit un algorithme de chiffrement.

Définition 7 : Différentielle

Une **différentielle** est un couple $(\Delta X, \Delta Y) \in (\mathbb{F}_2^n)^2$ de différence en entrée et de différence en sortie de l'algorithme de chiffrement.

Définition 8 : Chemin différentiel

Un **chemin différentiel** est un (r)-uplet de $(F_2^n)^r$ correspondant à des différences à chaque étape de l'algorithme de chiffrement.

Soit $X, X' \in (\mathbb{F}_2^n)^2$. On note $\Delta X = X \oplus X'$.

Proposition 1 :

Pour toute clé K, on a :

$$(X \oplus K) \oplus (X' \oplus K) = X \oplus X' = \Delta X$$

Proposition 2 :

Pour toute Pbox P, on a :

$$P(X) \oplus P(X') = P(X \oplus X') = P(\Delta X)$$

Exemple :

$$\left.\begin{array}{l} X = 0011 \\ X' = 0101 \end{array}\right\} \Delta X = 0110$$

Exemple :

$$\left.\begin{array}{l} X = 0011 \\ X' = 0101 \end{array}\right\} \Delta X = 0110$$

$$k = 0100$$

Exemple :

$$\left.\begin{array}{l} X = 0011 \\ X' = 0101 \end{array}\right\} \Delta X = 0110$$

$$k = 0100$$

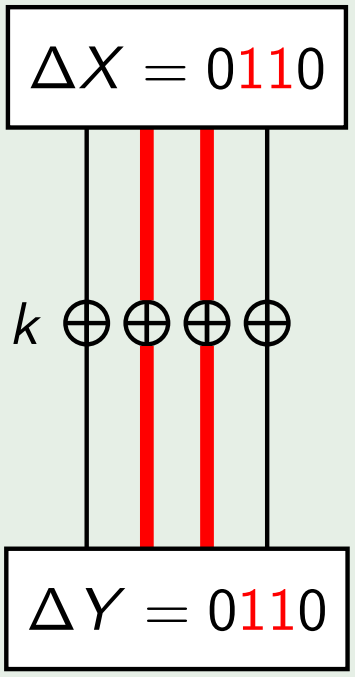
$$\left.\begin{array}{l} Y = 0111 \\ Y' = 0001 \end{array}\right\} \Delta Y = 0110$$

Exemple :

$$\left.\begin{array}{l} X = 0011 \\ X' = 0101 \end{array}\right\} \Delta X = 0110$$

$$k = 0100$$

$$\left.\begin{array}{l} Y = 0111 \\ Y' = 0001 \end{array}\right\} \Delta Y = 0110$$



Exemple :

$$\left.\begin{array}{l} X = 0011 \\ X' = 0101 \end{array}\right\} \Delta X = 0110$$

x	0	1	2	3
$P(x)$	2	0	1	3

TABLE – Pbox

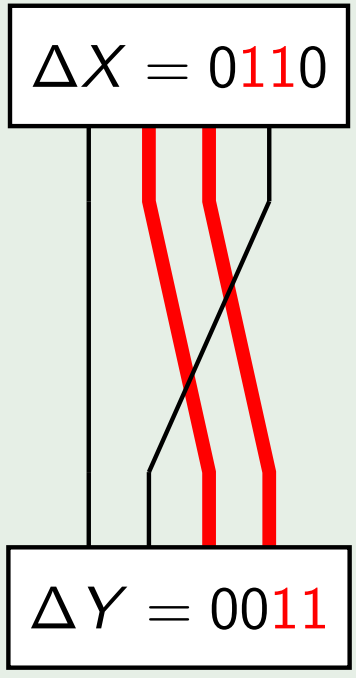
$$\left.\begin{array}{l} Y = 0101 \\ Y' = 0110 \end{array}\right\} \Delta Y = 0011$$

Exemple :

$$\left.\begin{array}{l} X = 0011 \\ X' = 0101 \end{array}\right\} \Delta X = 0110$$

x	0	1	2	3
$P(x)$	2	0	1	3

TABLE – Pbox



$$\left.\begin{array}{l} Y = 0101 \\ Y' = 0110 \end{array}\right\} \Delta Y = 0011$$

Tableau de distribution des différences d'une Sbox

Soit S une Sbox.

Notations :

Soit $(\Delta X, \Delta Y) \in (\mathbb{F}_2^n)^2$. On définit :

$$\delta(\Delta X, \Delta Y) = \text{card}\{X \in \mathbb{F}_2^n \mid S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}$$

Tableau de distribution des différences d'une Sbox

Soit S une Sbox.

Notations :

Soit $(\Delta X, \Delta Y) \in (\mathbb{F}_2^n)^2$. On définit :

$$\delta(\Delta X, \Delta Y) = \text{card}\{X \in \mathbb{F}_2^n \mid S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}$$

Définition 9 : Difference distribution table (DDT)

Le **tableau de distribution des différences** de la Sbox S donne les valeurs de $\delta(\Delta X, \Delta Y)$ pour tout $(\Delta X, \Delta Y) \in (\mathbb{F}_2^n)^2$.

Exemple

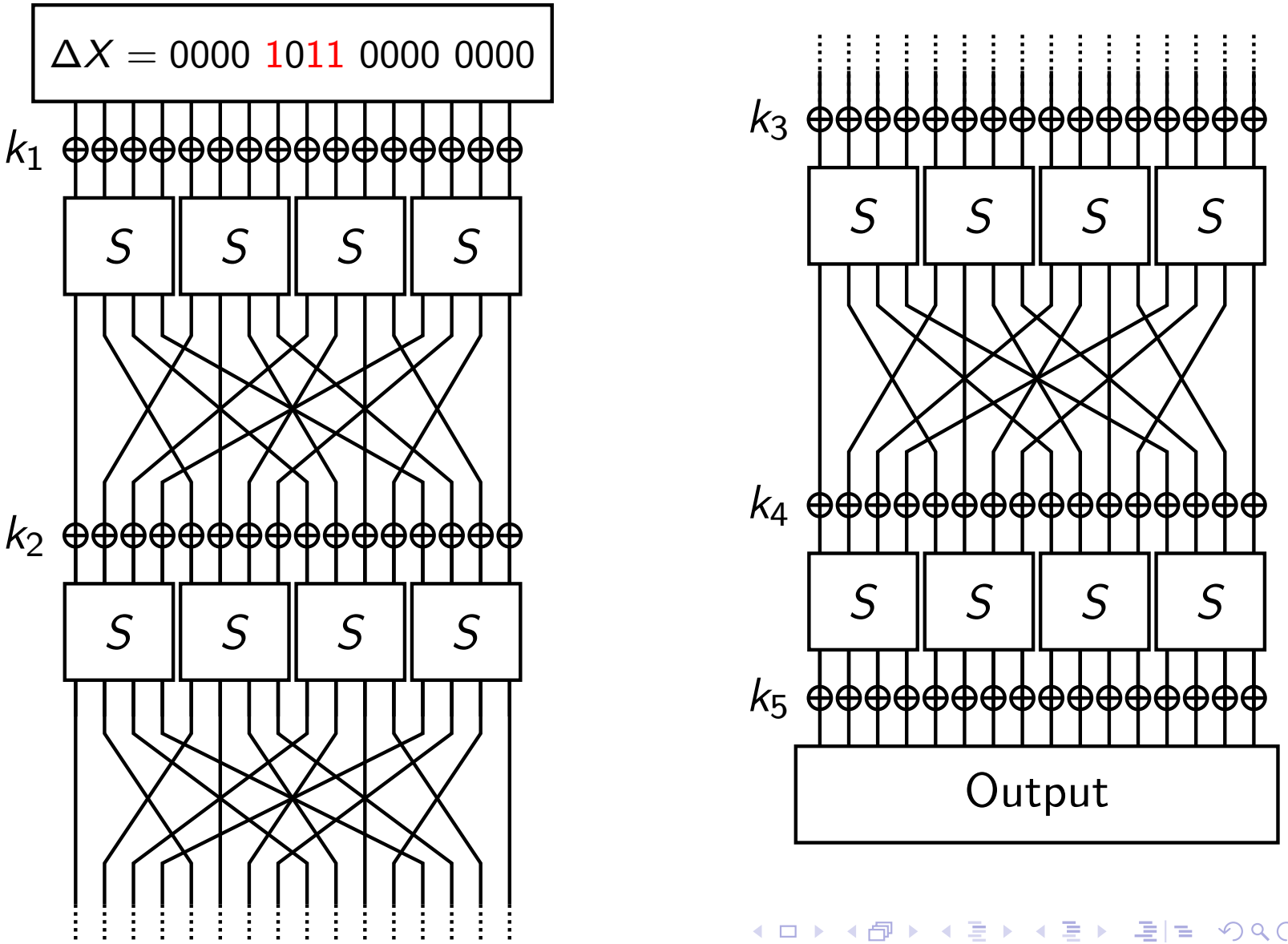
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	e	4	d	1	2	f	b	8	3	a	6	c	5	9	0	7

TABLE – Sbox

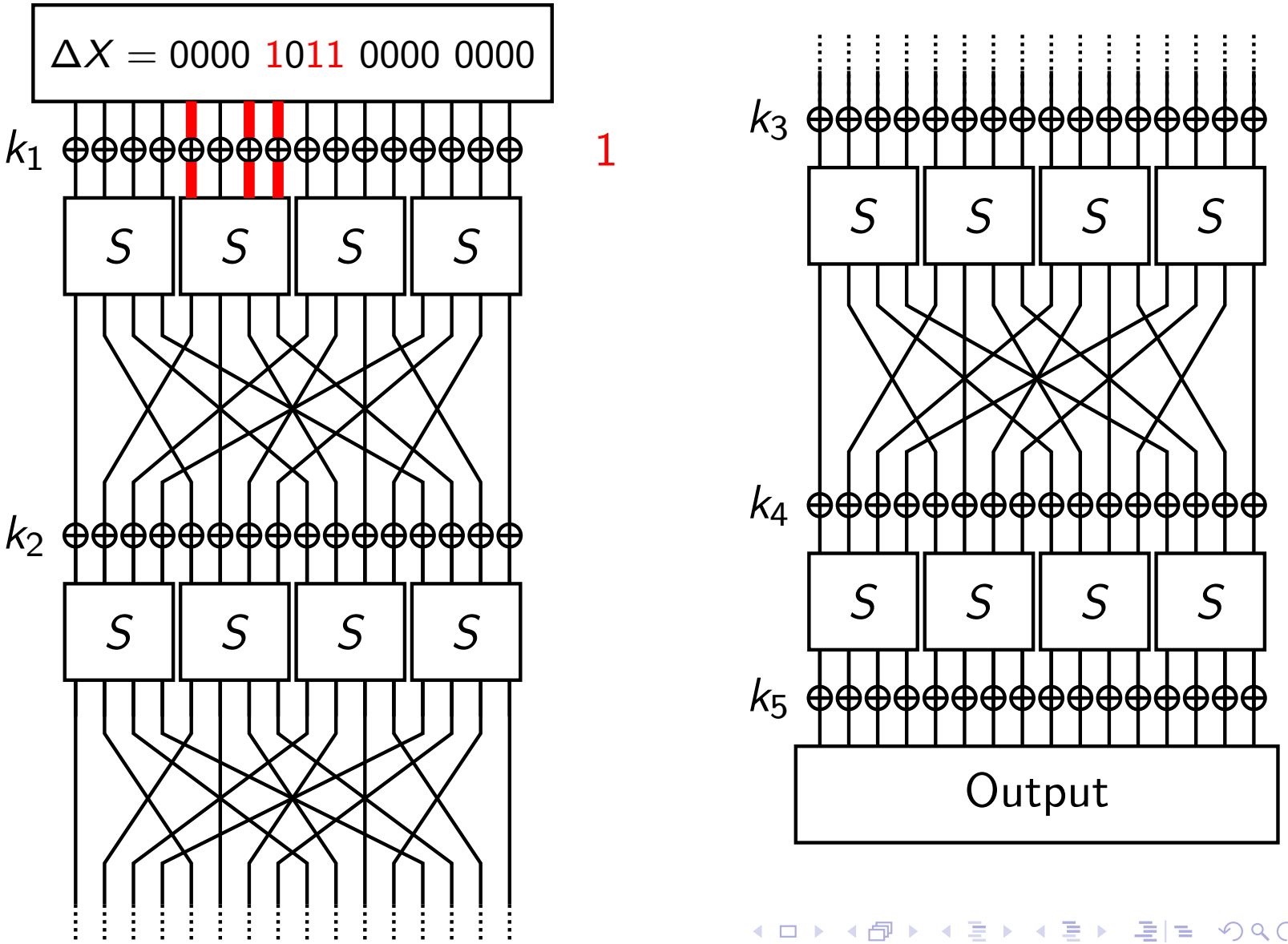
Input difference \ Output difference	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	-	2	-	-	-	2	-	2	4	-	4	2	-	-
2	-	-	-	2	-	6	2	2	-	2	-	-	-	-	2	-
3	-	-	2	-	2	-	-	-	-	4	2	-	2	-	-	4
4	-	-	-	2	-	-	6	-	-	2	-	4	2	-	-	-
5	-	4	-	-	-	2	2	-	-	-	4	-	2	-	-	2
6	-	-	-	4	-	4	-	-	-	-	-	-	2	2	2	2
7	-	-	2	2	2	-	2	-	-	2	2	-	-	-	-	4
8	-	-	-	-	-	-	2	2	-	-	-	4	-	4	2	2
9	-	2	-	-	2	-	-	4	2	-	2	2	2	-	-	-
10	-	2	2	-	-	-	-	-	6	-	-	2	-	-	4	0
11	-	-	8	-	-	2	-	2	-	-	-	-	-	2	-	2
12	-	2	-	-	2	2	2	-	-	-	-	2	-	6	-	-
13	-	4	-	-	-	-	-	4	2	-	2	-	2	-	2	-
14	-	-	2	4	2	-	-	-	6	-	-	-	-	-	2	-
15	-	2	-	-	6	-	-	-	-	4	-	2	-	-	2	-

TABLE – DDT de la Sbox

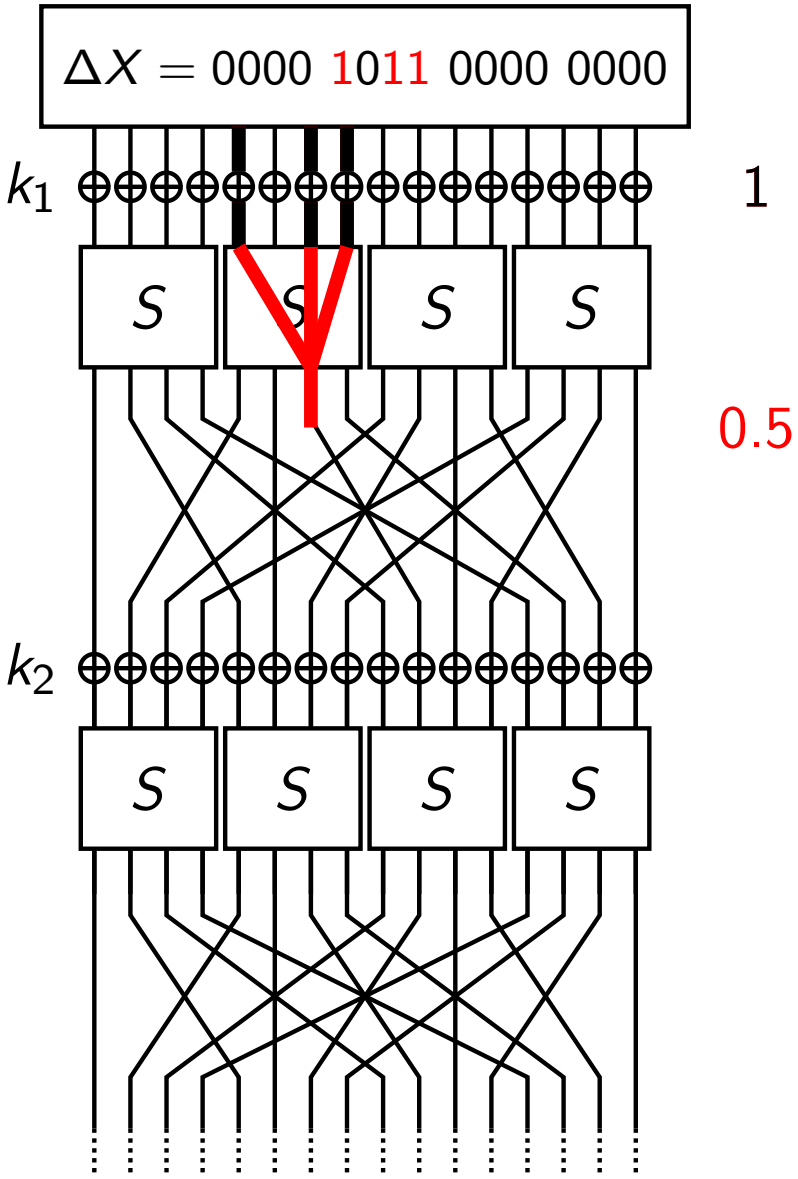
Exemple

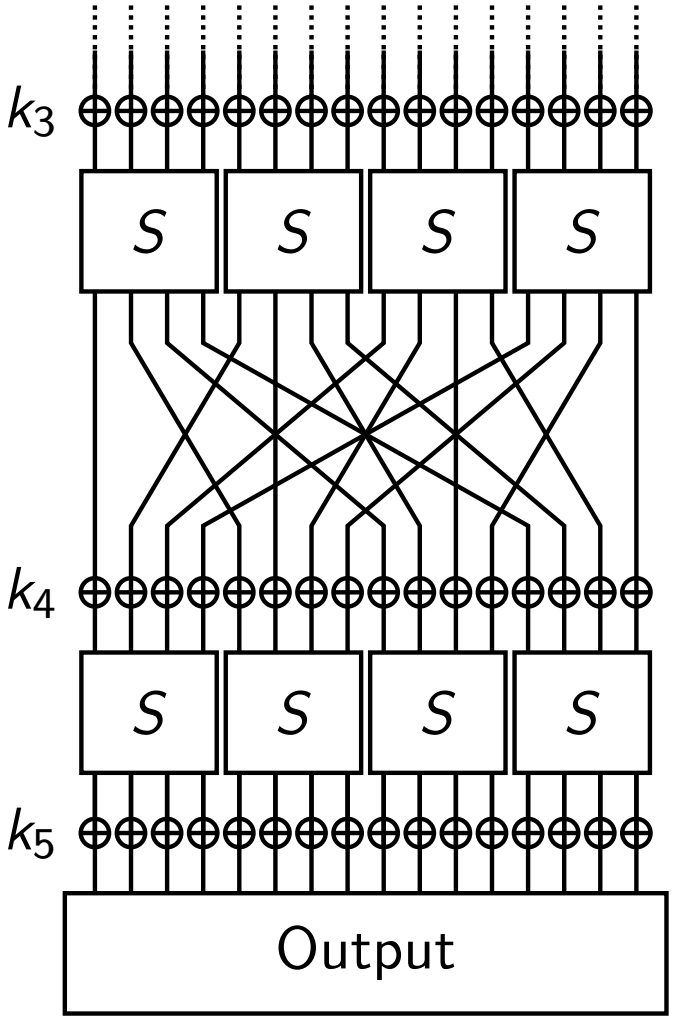

ΔX = 0000 1011 0000 0000
k1
S S S S
k2
S S S S
k3
S S S S
k4
S S S S
k5
Output

Exemple

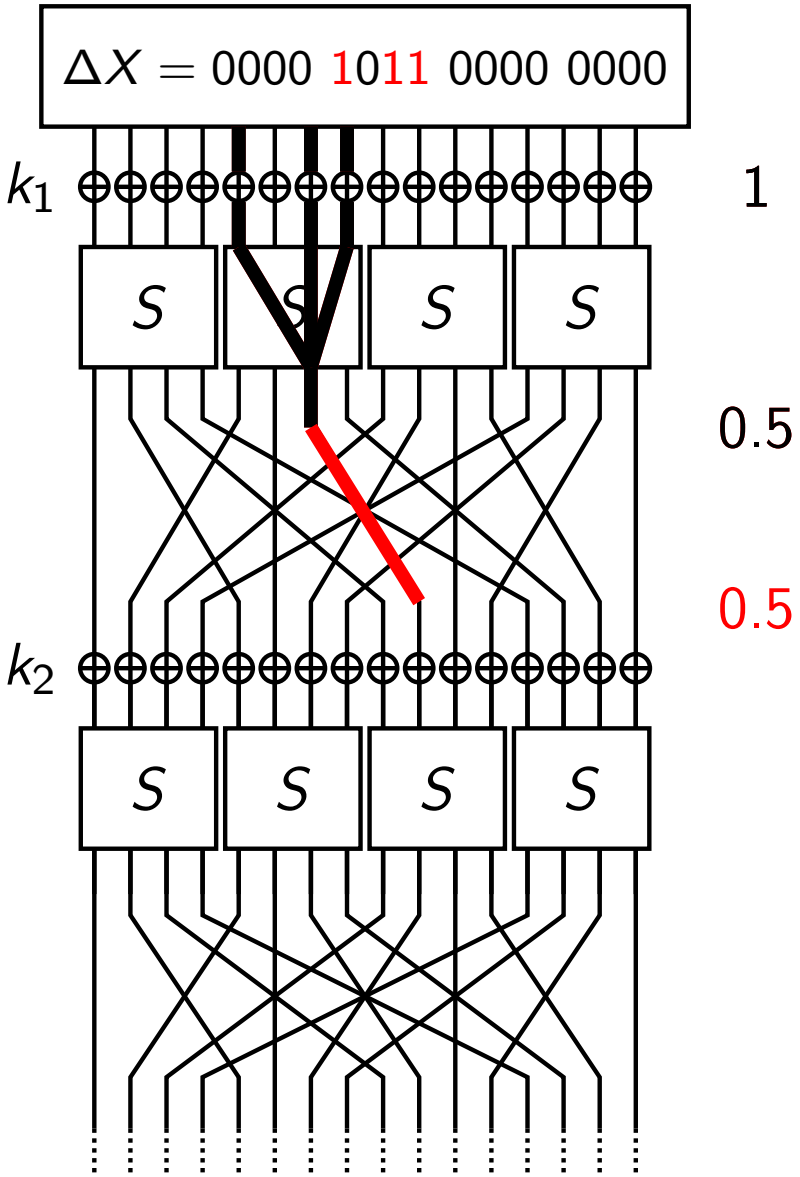


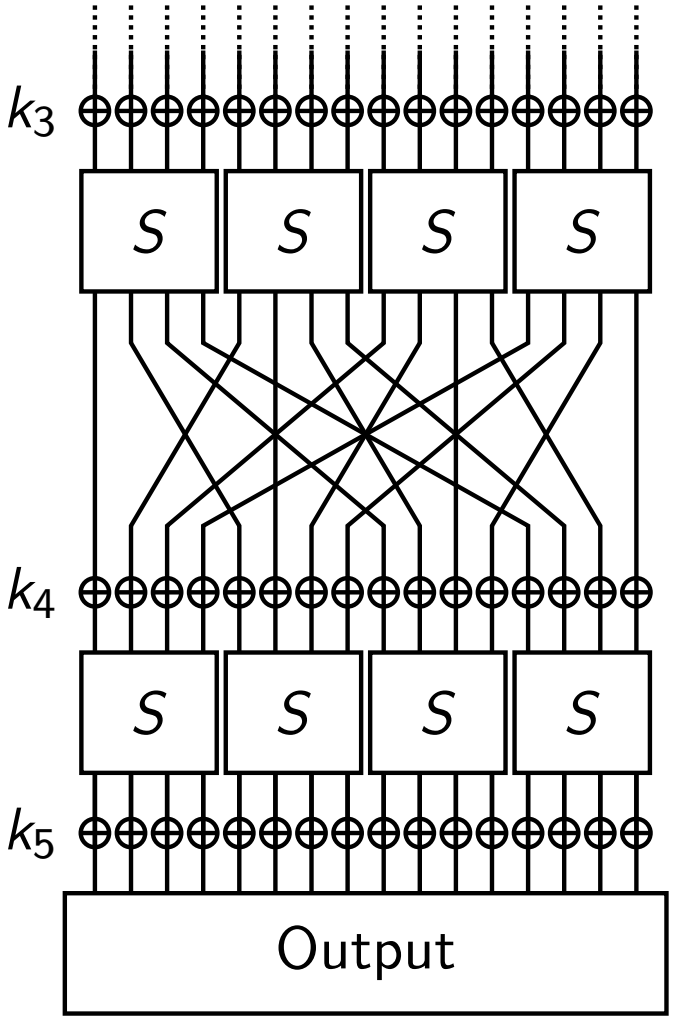
Exemple


ΔX = 0000 1011 0000 0000
k1
S
S
S
S
1
0.5
k2
S
S
S
S

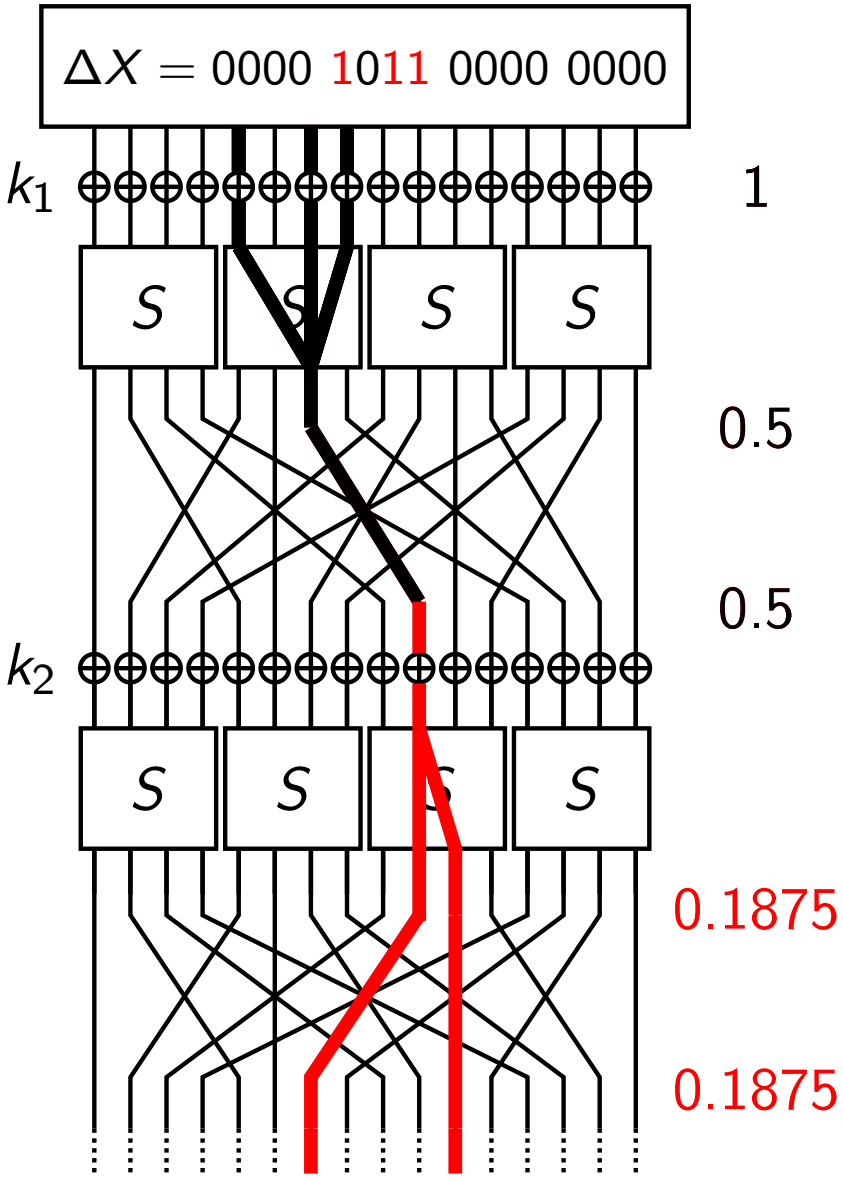

k3
S
S
S
S
k4
S
S
S
S
k5
Output

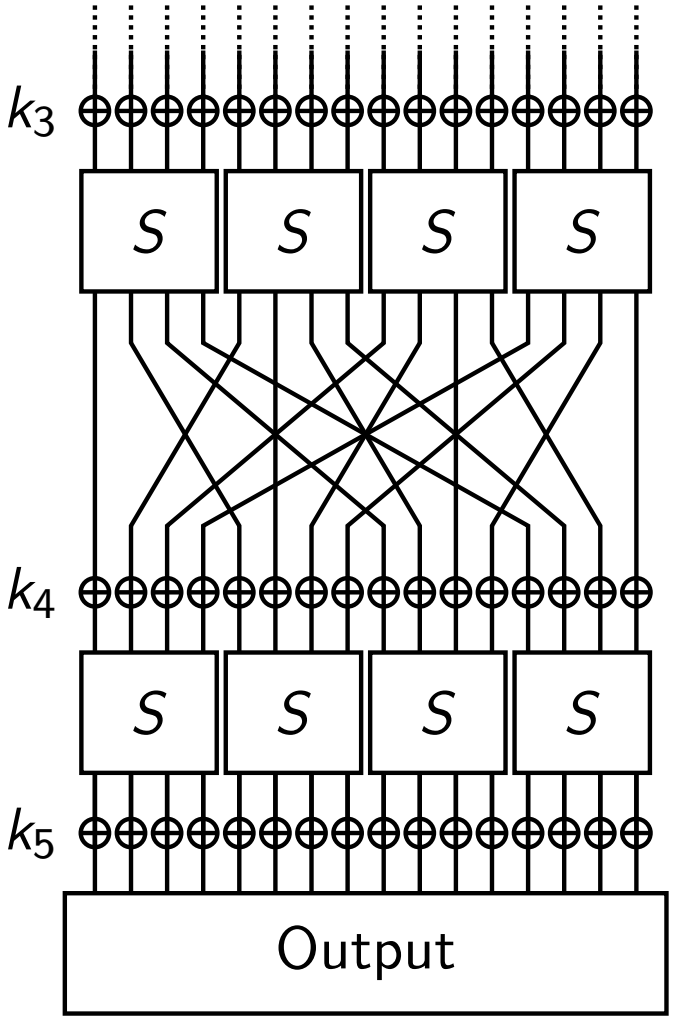
Exemple


ΔX = 0000 1011 0000 0000
k1
S
S
S
S
1
0.5
0.5
k2
S
S
S
S

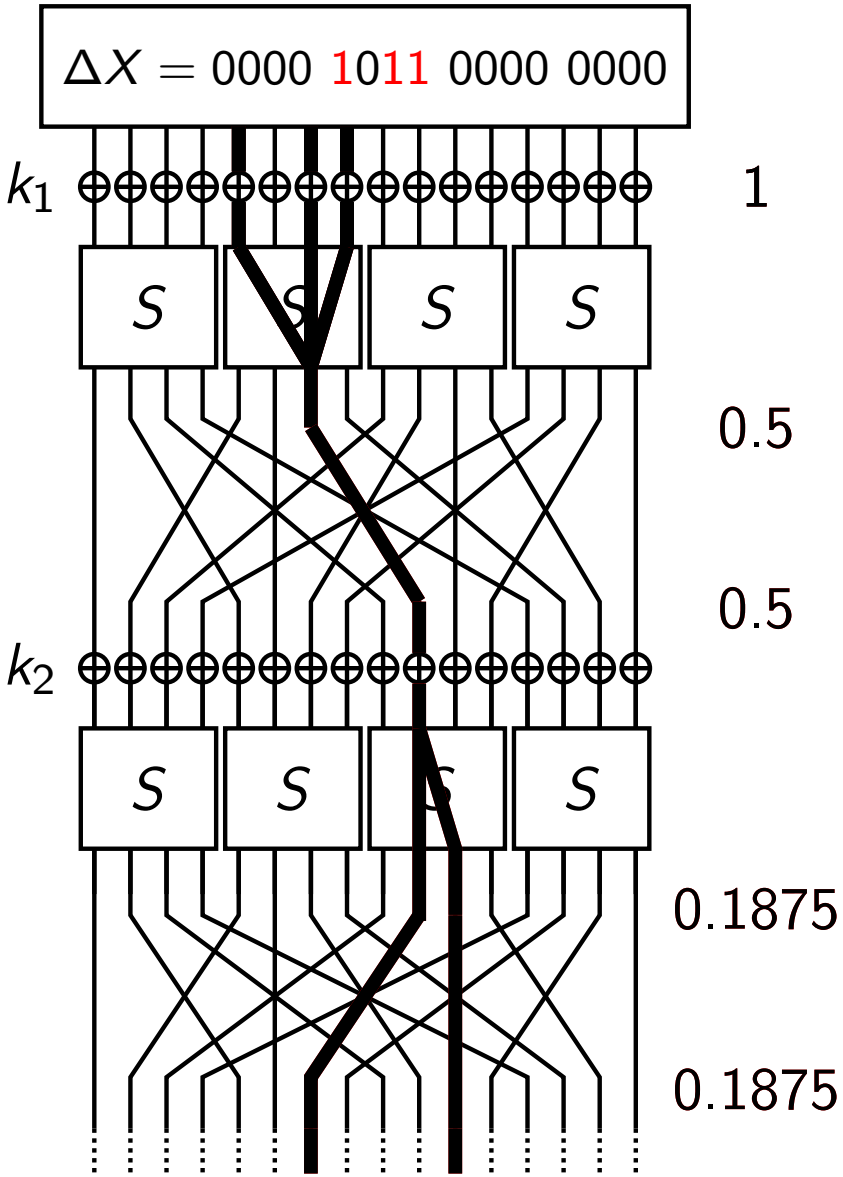

k3
S
S
S
S
k4
S
S
S
S
k5
Output

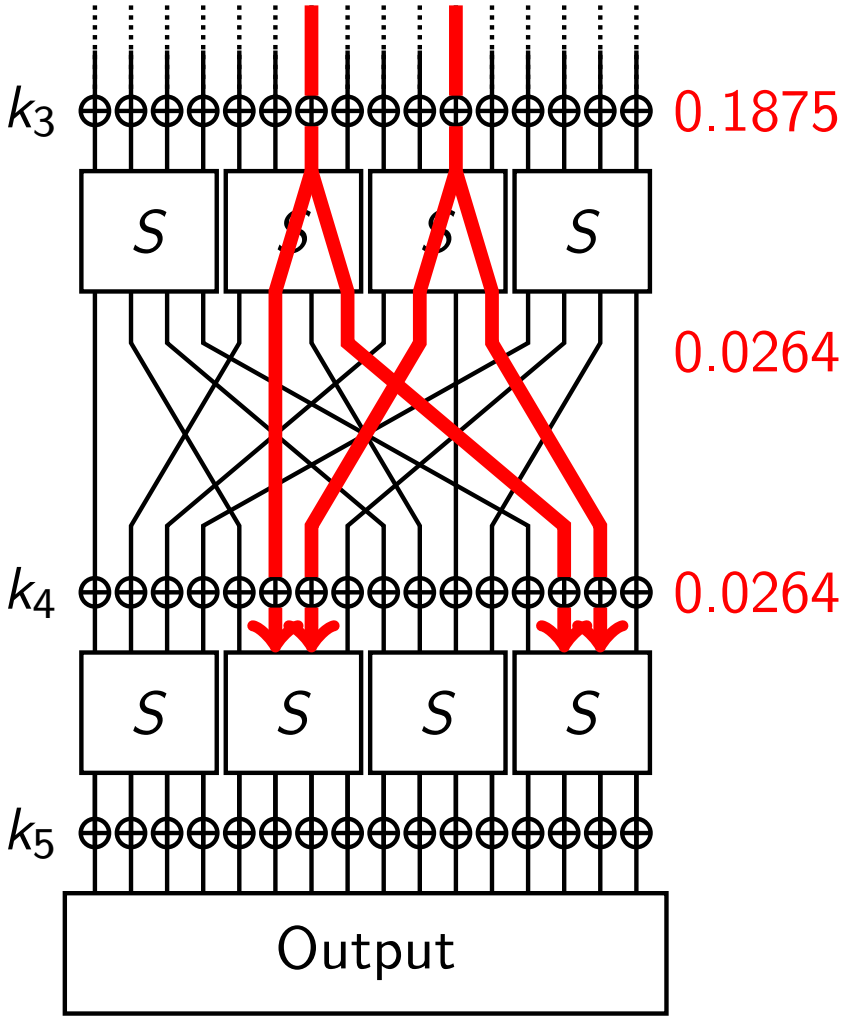
Exemple


ΔX = 0000 1011 0000 0000
k1
S
S
S
S
1
0.5
0.5
k2
S
S
S
S
0.1875
0.1875


k3
S
S
S
S
k4
S
S
S
S
k5
Output

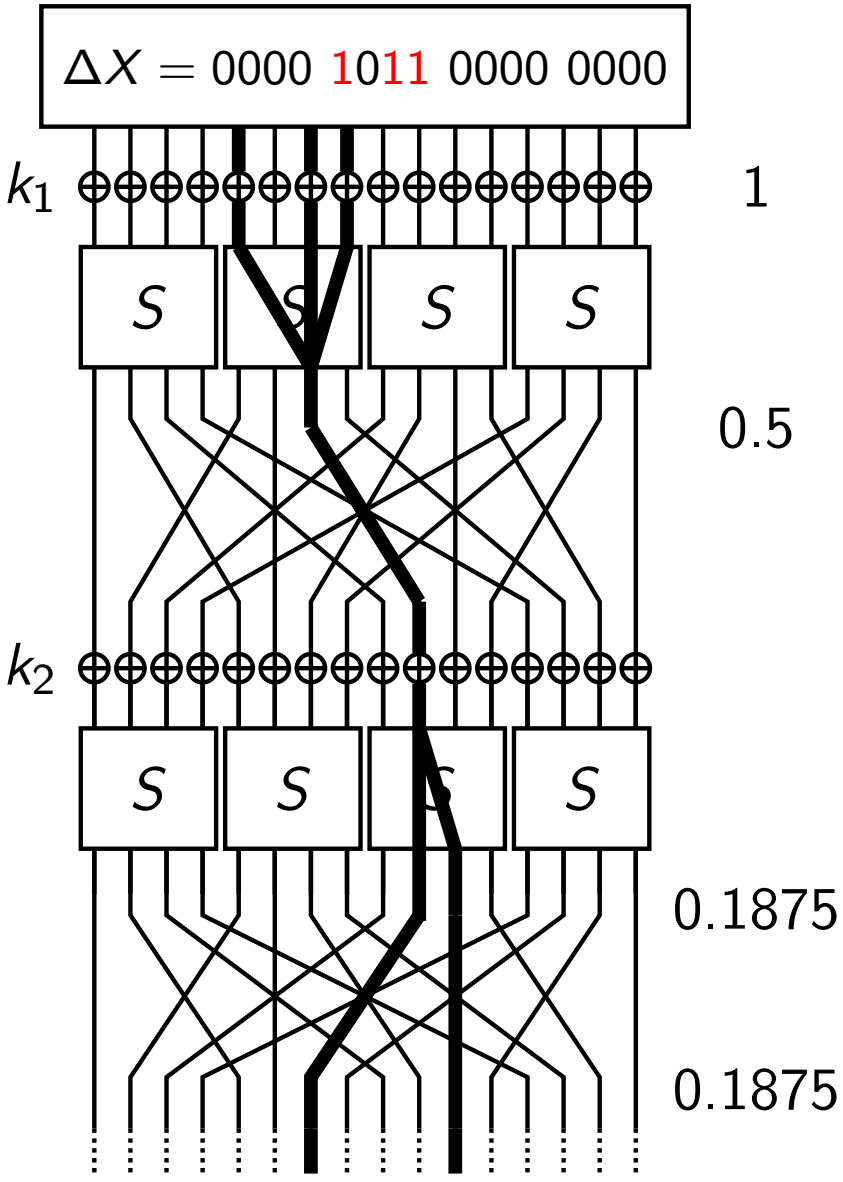
Exemple

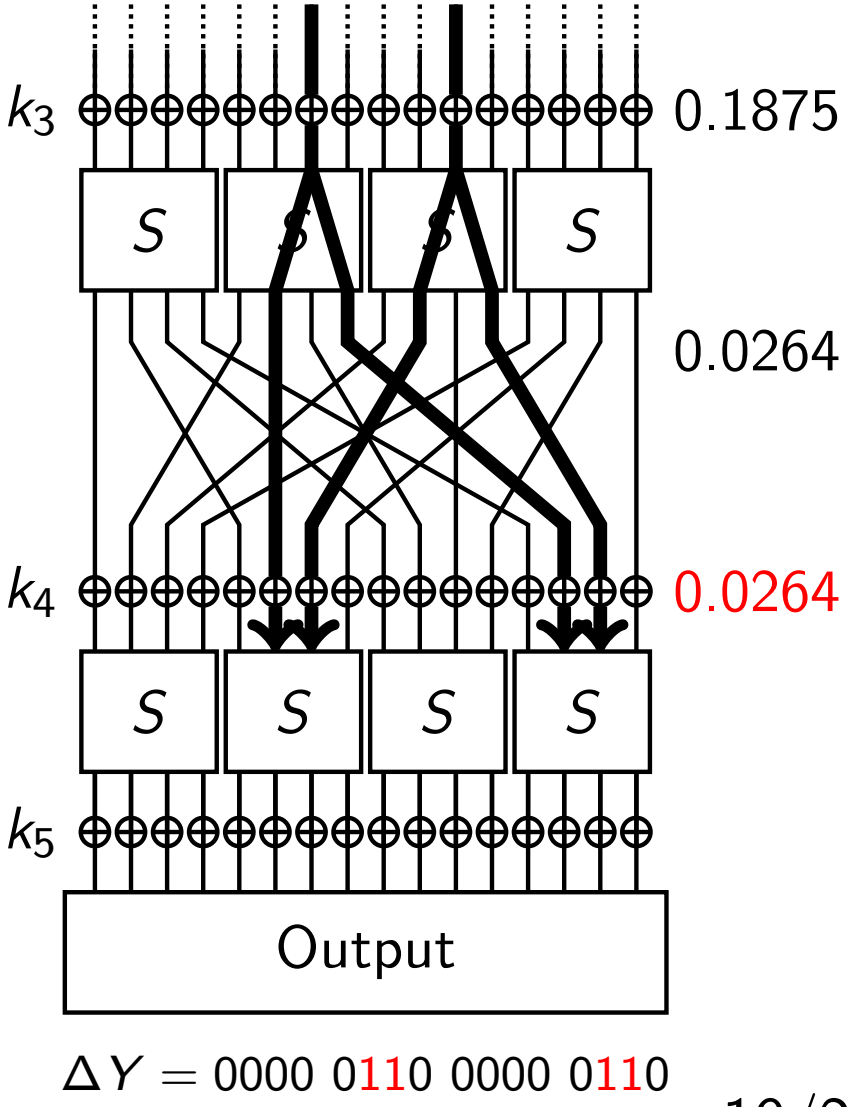




$\Delta Y = 0000\ 0110\ 0000\ 0110$

Comment déterminer k_5 ?





Définition 10 : Uniformité différentielle

On définit l'**uniformité différentielle** $\mu(S)$ d'une Sbox S par le **maximum** de son tableau de distribution des différences.

$$\mu(S) = \max_{\Delta X, \Delta Y \in (F_2^n)^2 \, , \, \Delta X \neq 0} \delta(\Delta X, \Delta Y)$$

Définition 10 : Uniformité différentielle

On définit l'**uniformité différentielle** $\mu(S)$ d'une Sbox S par le **maximum** de son tableau de distribution des différences.

$$\mu(S) = \max_{\Delta X, \Delta Y \in (F_2^n)^2 \, , \, \Delta X \neq 0} \delta(\Delta X, \Delta Y)$$

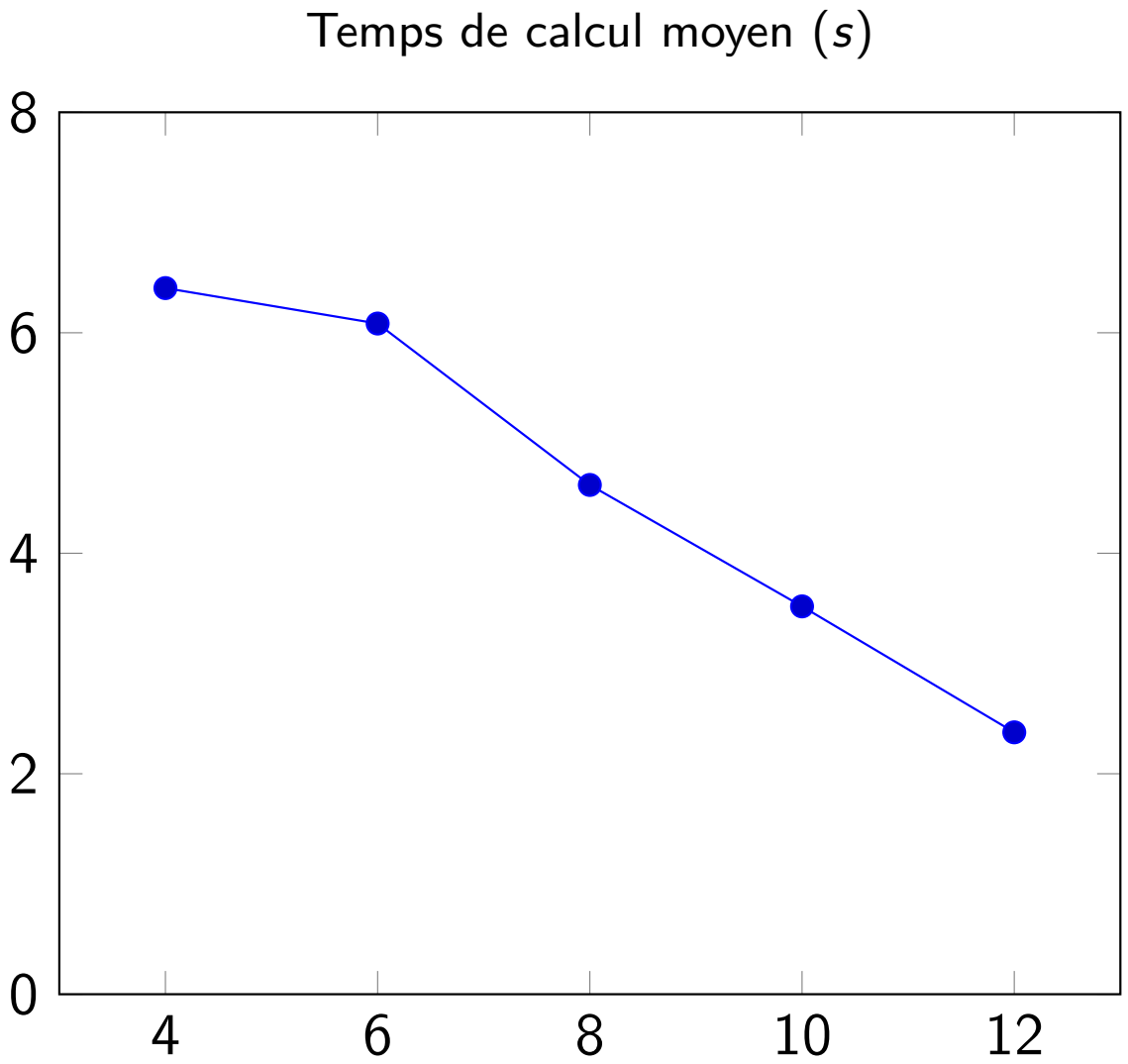
Input difference \ Output difference	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	-	2	-	-	-	2	-	2	4	-	4	2	-	-
2	-	-	-	2	-	6	2	2	-	2	-	-	-	-	2	-
3	-	-	2	-	2	-	-	-	-	4	2	-	2	-	-	4
4	-	-	-	2	-	-	6	-	-	2	-	4	2	-	-	-
5	-	4	-	-	-	2	2	-	-	-	4	-	2	-	-	2
6	-	-	-	4	-	4	-	-	-	-	-	-	2	2	2	2
7	-	-	2	2	2	-	2	-	-	2	2	-	-	-	-	4
8	-	-	-	-	-	-	2	2	-	-	-	4	-	4	2	2
9	-	2	-	-	2	-	-	4	2	-	2	2	2	-	-	-
10	-	2	2	-	-	-	-	-	6	-	-	2	-	-	4	0
11	-	-	8	-	-	2	-	2	-	-	-	-	-	2	-	2
12	-	2	-	-	2	2	2	-	-	-	-	2	-	6	-	-
13	-	4	-	-	-	-	-	4	2	-	2	-	2	-	2	-
14	-	-	2	4	2	-	-	-	6	-	-	-	-	-	2	-
15	-	2	-	-	6	-	-	-	-	4	-	2	-	-	2	-

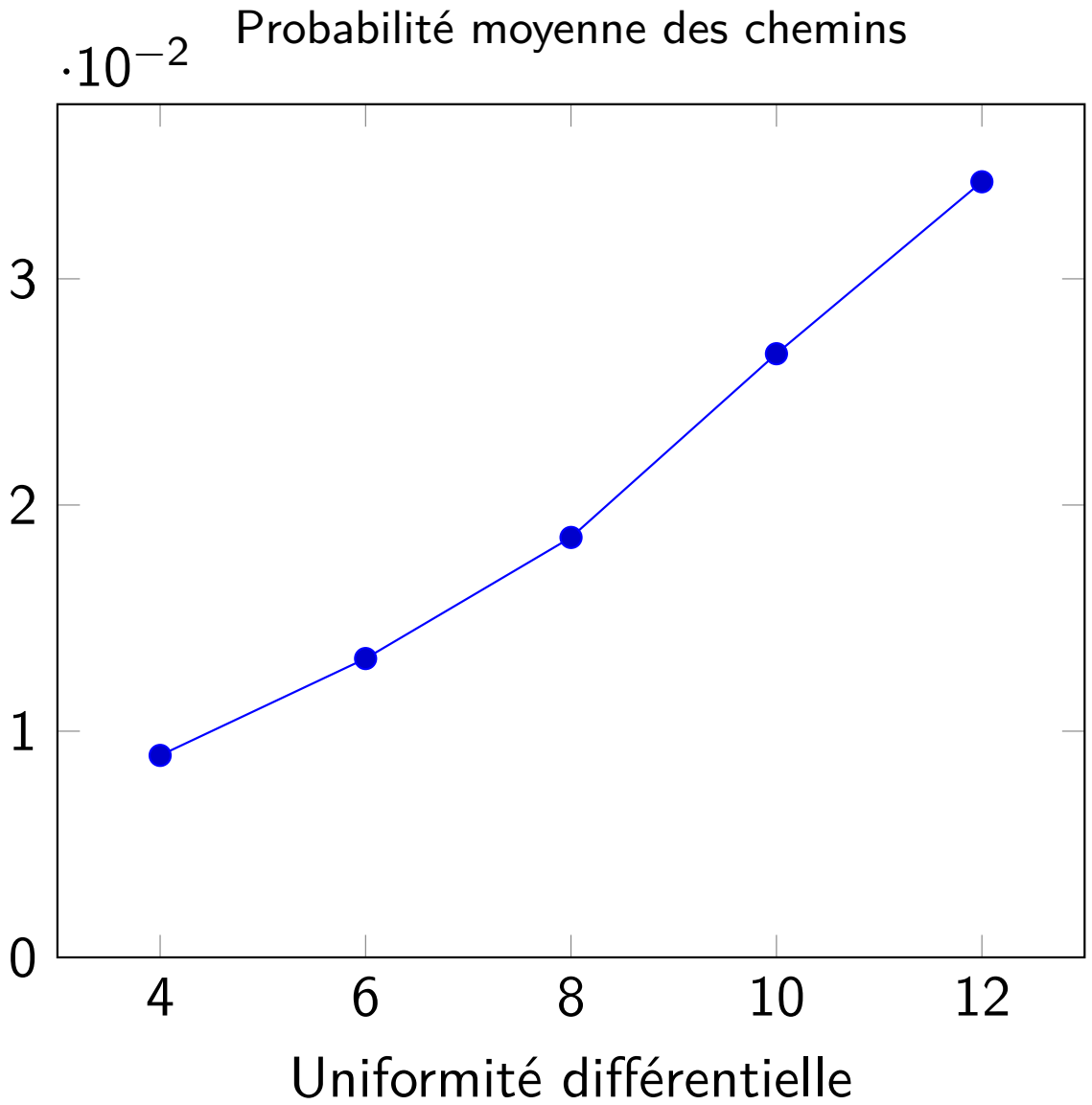
TABLE – DDT de la Sbox

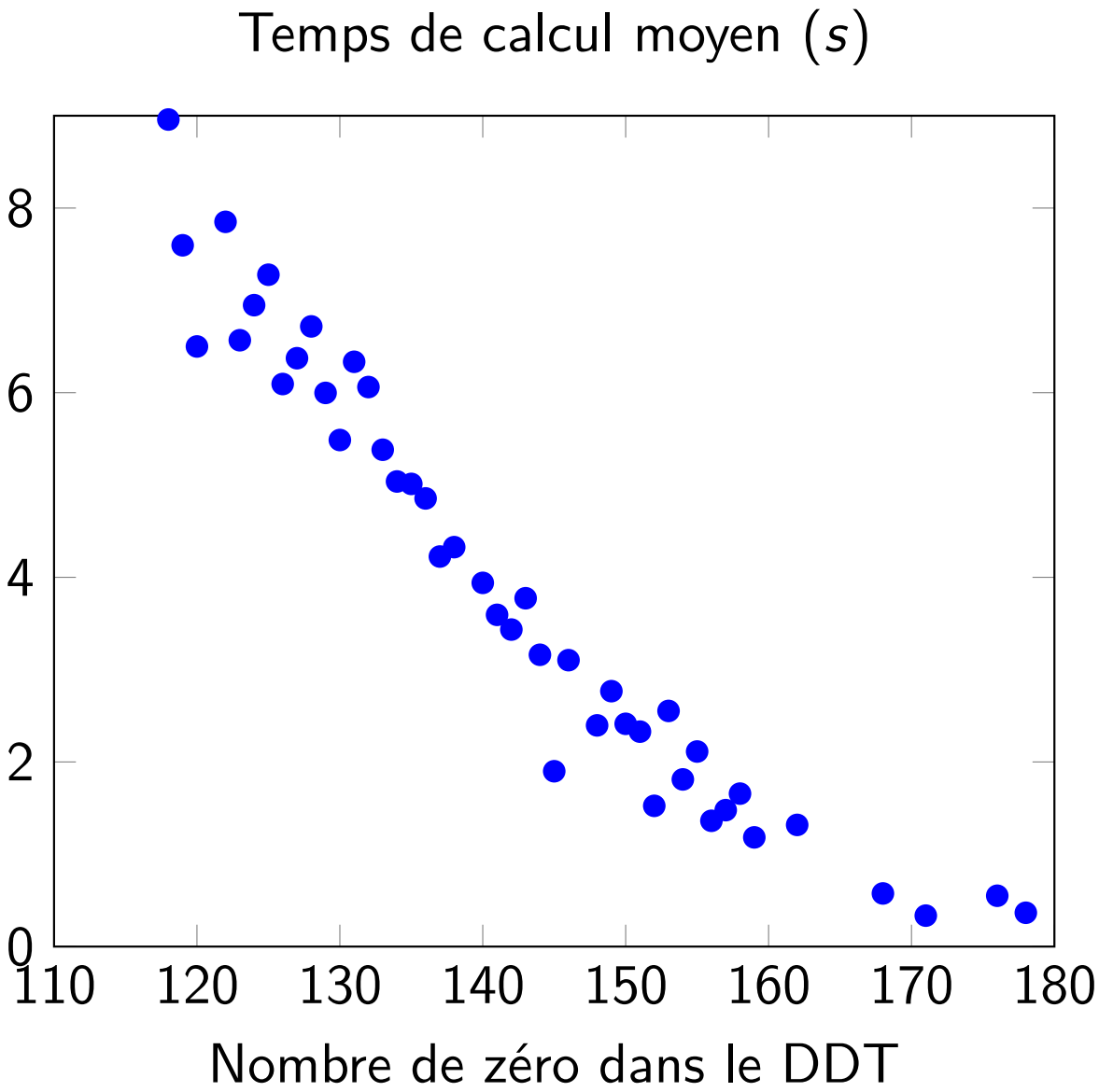
Hypothèse :

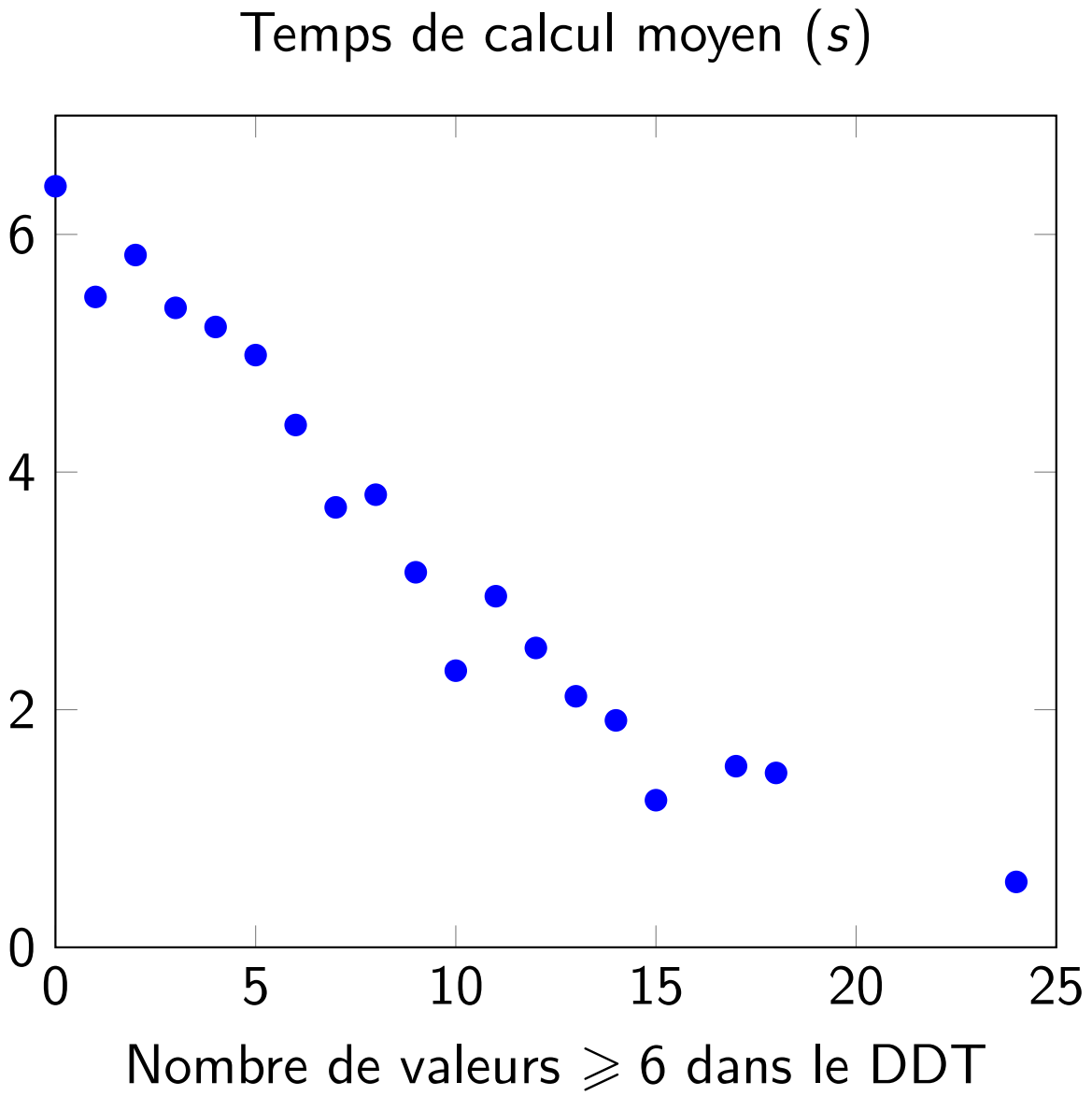
Un bon algorithme de chiffrement nécessite une Sbox avec la plus **faible uniformité différentielle**.

Vérification




Probabilité moyenne des chemins
$\cdot 10^{-2}$
3
2
1
0
4
6
8
10
12
Uniformité différentielle


Temps de calcul moyen (s)
8
6
4
2
0
110
120
130
140
150
160
170
180
Nombre de zéro dans le DDT


Temps de calcul moyen (s)
6
4
2
0
0
5
10
15
20
25
Nombre de valeurs ⩾ 6 dans le DDT

Conclusion

- Importance de l'uniformité différentielle

Conclusion

- Importance de l'uniformité différentielle
- Permutations APN

Conclusion

- Importance de l'uniformité différentielle
- Permutations APN
- Couche de diffusion/permutation

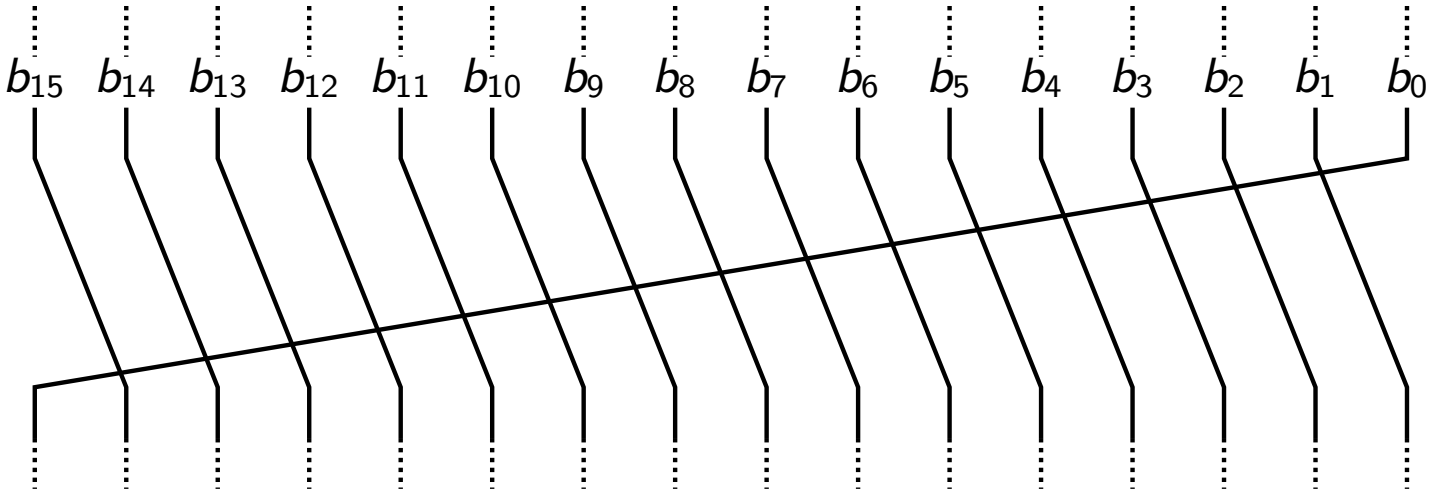


FIGURE – Pbox A

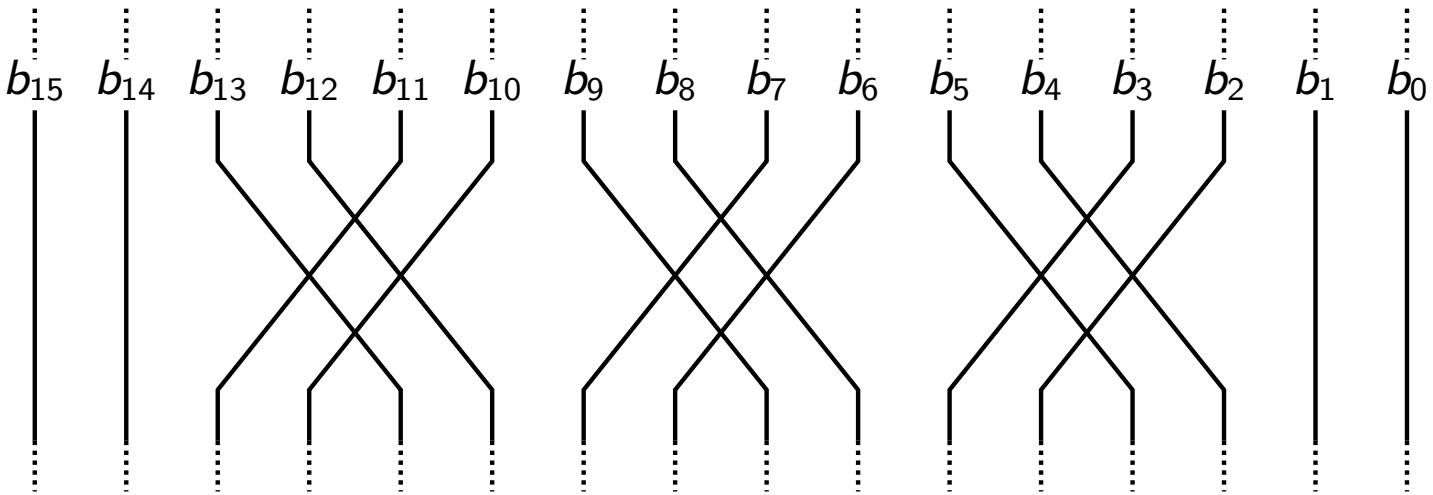


FIGURE – Pbox B

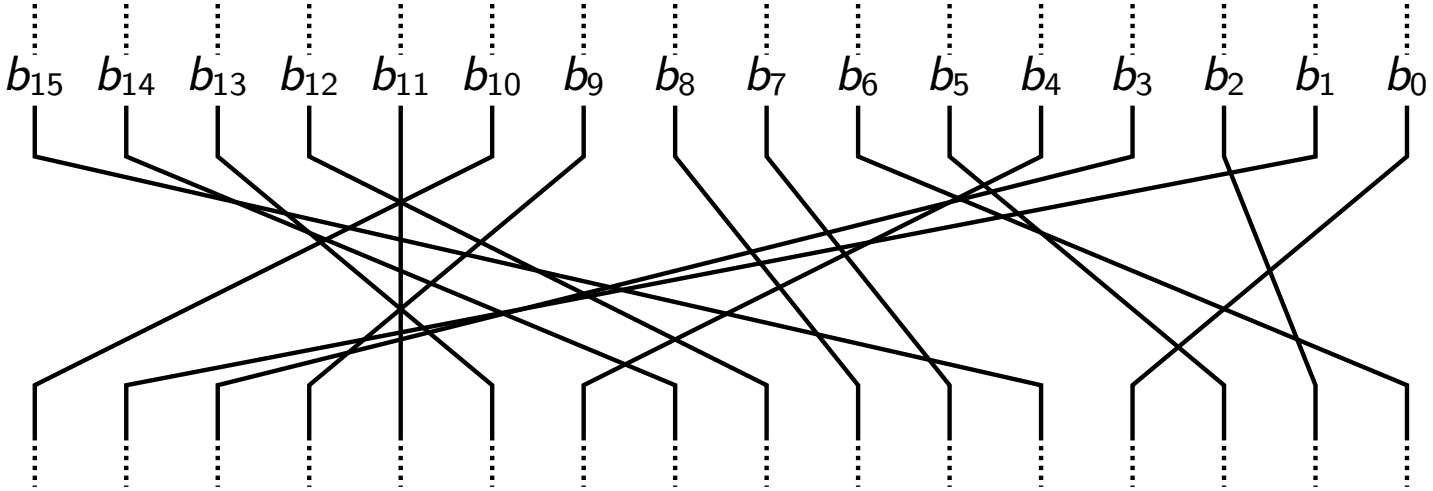


FIGURE – Pbox C

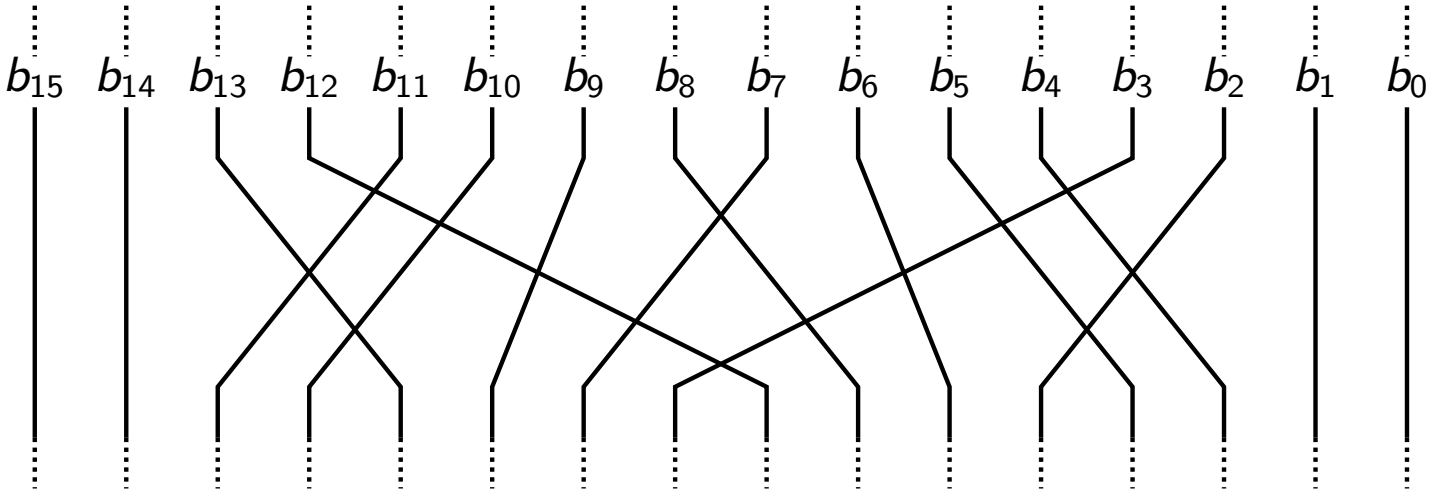
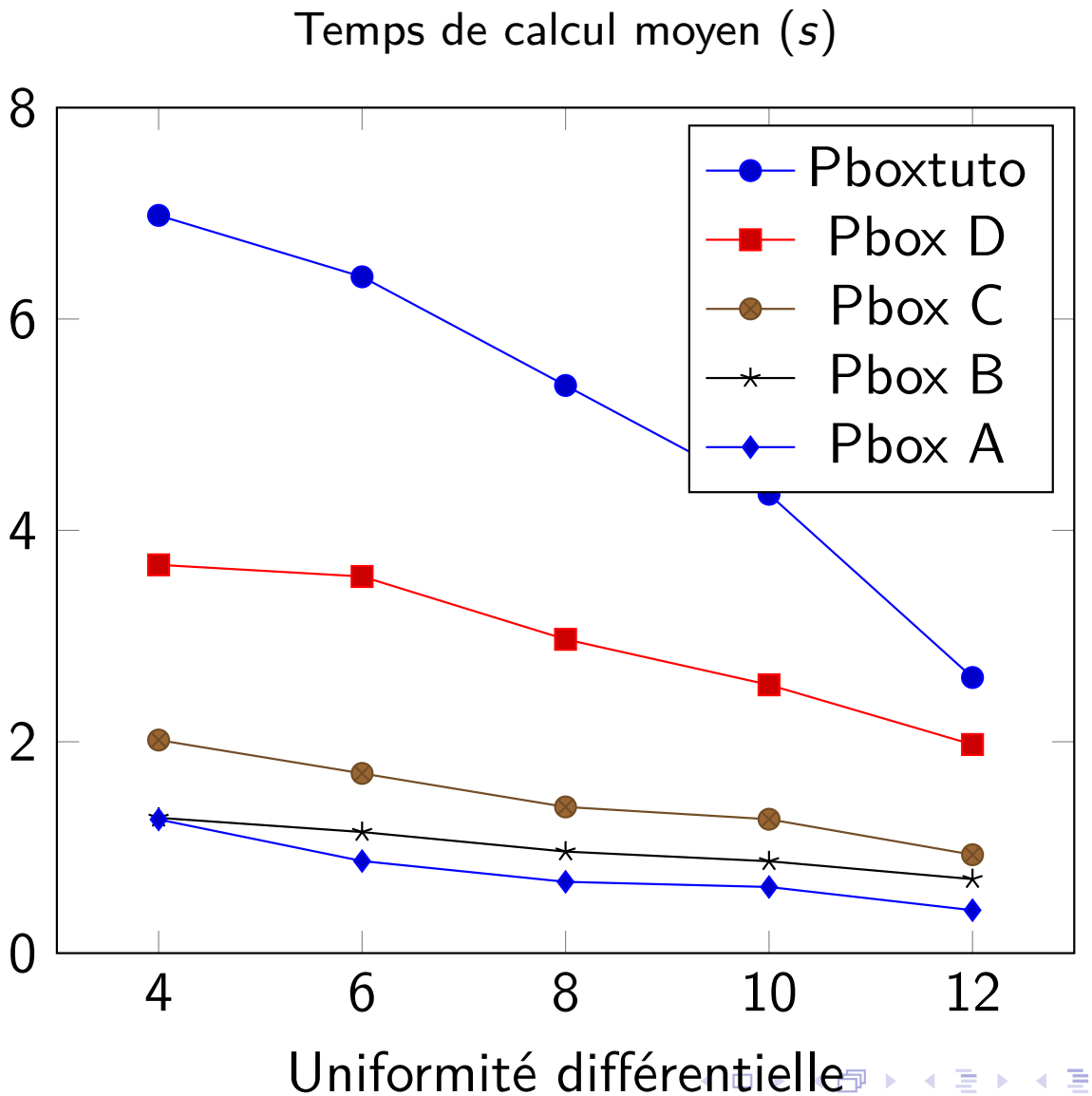


FIGURE – Pbox D

Vérification



Bibliographie


Céline Blondeau. *La cryptanalyse différentielle et ses généralisations*. Université Pierre et Marie Curie - Paris VI, 2011.


Anne Canteaut. *Lecture Notes on Cryptographic Boolean Functions*. Inria, 2016.


Howars M. Heys. « A tutorial on linear and differential cryptanalysis ». In : *Cryptologia* 26.3 (2002), p. 189-221.


Lars R. Knudsen et Matthew J. B. Robshaw. *The Block Cipher Companion*. *Chapitre 6*. Springer Publishing Company, 2011.