# AES in a (white)box.

Eric Sageloli & Guillaume Wafo-Tapa

11 mai 2018

# Introduction : contexte Whitebox

- Contexte classique blackbox
- DRM : modèle blackbox inadapté
- nouveau contexte : whitebox

# Introduction : comment cacher la clé ?

Première idée :

$$\text{Message M} = \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

$$\downarrow$$

$$\boxed{\quad T \quad}$$

$$\downarrow$$

$$\text{Chiffré C} = \begin{bmatrix} y_0 & y_4 & y_8 & y_{12} \\ y_1 & y_5 & y_9 & y_{13} \\ y_2 & y_6 & y_{10} & y_{14} \\ y_3 & y_7 & y_{11} & y_{15} \end{bmatrix}$$

# Introduction : comment cacher la clé ?

Première idée :

$$\text{Message } M = \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

$$\downarrow$$

$$\boxed{T}$$

$$\downarrow$$

$$\text{Chiffré } C = \begin{bmatrix} y_0 & y_4 & y_8 & y_{12} \\ y_1 & y_5 & y_9 & y_{13} \\ y_2 & y_6 & y_{10} & y_{14} \\ y_3 & y_7 & y_{11} & y_{15} \end{bmatrix}$$

- clef complètement obfusquée ;

# Introduction : comment cacher la clé ?

Première idée :

$$\text{Message M} = \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

$$\downarrow$$

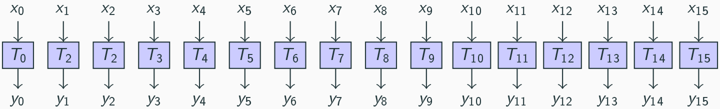
$$\boxed{\quad \mathrm{T} \quad}$$

$$\downarrow$$

$$\text{Chiffré C} = \begin{bmatrix} y_0 & y_4 & y_8 & y_{12} \\ y_1 & y_5 & y_9 & y_{13} \\ y_2 & y_6 & y_{10} & y_{14} \\ y_3 & y_7 & y_{11} & y_{15} \end{bmatrix}$$

- clef complètement obfusquée ;
- taille de la table :
  - $2^{128}$ entrées
  - 16 octets par sortie
  - $16 * 2^{128} = 2^{132}$ octets

# Introduction : comment cacher la clé ?




Pour chaque table :

- $2^8$ entrées
- 1 octet en sortie
- taille : $2^8$ octets

taille totale : $16 * 2^8 = 2^{12}$ octet = 4 KiB

# Introduction : comment cacher la clé ?

$$\begin{array}{cccccccccccccccc}
x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} & x_{12} & x_{13} & x_{14} & x_{15} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\boxed{T_0} & \boxed{T_2} & \boxed{T_2} & \boxed{T_3} & \boxed{T_4} & \boxed{T_5} & \boxed{T_6} & \boxed{T_7} & \boxed{T_8} & \boxed{T_9} & \boxed{T_{10}} & \boxed{T_{11}} & \boxed{T_{12}} & \boxed{T_{13}} & \boxed{T_{14}} & \boxed{T_{15}} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
y_0 & y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 & y_8 & y_9 & y_{10} & y_{11} & y_{12} & y_{13} & y_{14} & y_{15}
\end{array}$$

Pour chaque table :

- $2^8$ entrées
- 1 octet en sortie
- taille : $2^8$ octets

taille totale : $16 * 2^8 = 2^{12}$ octet $=$ 4 KiB

- La clef n'est plus complètement obfusquée.
- On aura besoin de 2032 tables, stockés sur $500KB$

# Plan

# Découpage de l'algorithme AES

# Algorithme AES standard

```
state = plaintext;

AddRoundKey (state, key[0]);
for (round = 0; round < 9; round++)
{
  SubBytes (state);
  ShiftRows (state);
  MixColumns (state);
  AddRoundKey (state, key[round + 1]);
}
SubBytes (state);
ShiftRows (state);
AddRoundKey (state, key[10]);

ciphertext = state;
```

# Découpage des fonctions de l'AES : AddRoundKey

au round r, ajoute key[r] au state :

$$\mathrm{AddRoundKey}(state) = state \oplus key[r]$$

$$= \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix} \oplus \begin{bmatrix} key[r]_0 & key[r]_4 & key[r]_8 & key[r]_{12} \\ key[r]_1 & key[r]_5 & key[r]_9 & key[r]_{13} \\ key[r]_2 & key[r]_6 & key[r]_{10} & key[r]_{14} \\ key[r]_3 & key[r]_7 & key[r]_{11} & key[r]_{15} \end{bmatrix}$$

$$= \begin{bmatrix} x_0 \oplus key[r]_0 & x_4 \oplus key[r]_4 & x_8 \oplus key[r]_8 & x_{12} \oplus key[r]_{12} \\ x_1 \oplus key[r]_1 & x_5 \oplus key[r]_5 & x_9 \oplus key[r]_9 & x_{13} \oplus key[r]_{13} \\ x_2 \oplus key[r]_2 & x_6 \oplus key[r]_6 & x_{10} \oplus key[r]_{10} & x_{14} \oplus key[r]_{14} \\ x_3 \oplus key[r]_3 & x_7 \oplus key[r]_7 & x_{11} \oplus key[r]_{11} & x_{15} \oplus key[r]_{15} \end{bmatrix}$$

- AddRoundKey peut s'appliquer octet par octet.

# Découpage des fonctions de l'AES : SubBytes

$$\text{SubBytes}\left(\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}\right)$$

$$= \begin{bmatrix} SBox(x_0) & SBox(x_4) & SBox(x_8) & SBox(x_{12}) \\ SBox(x_1) & SBox(x_5) & SBox(x_9) & SBox(x_{13}) \\ SBox(x_2) & SBox(x_6) & SBox(x_{10}) & SBox(x_{14}) \\ SBox(x_3) & SBox(x_7) & SBox(x_{11}) & SBox(x_{15}) \end{bmatrix}$$

- SubBytes peut s'appliquer octet par octet.

# Découpage des fonctions de l'AES : MixColumns

$$\text{MixColumns}\left(\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}\right) = MC * \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

$$= \begin{bmatrix} MC * \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} & MC * \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} & MC * \begin{bmatrix} x_8 \\ x_9 \\ x_{10} \\ x_{11} \end{bmatrix} & MC * \begin{bmatrix} x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{bmatrix} \end{bmatrix}$$

- MixColumns peut s'appliquer colonne par colonne.

# Découpage des fonctions de l'AES : ShiftRows

$$\text{ShiftRows}\left(\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}\right) = \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_5 & x_9 & x_{13} & x_1 \\ x_{10} & x_{14} & x_6 & x_{10} \\ x_{15} & x_3 & x_7 & x_{11} \end{bmatrix}$$

- ShiftRows se prête mal au découpage.

# Réarrangement de l'algorithme AES

```
s = plaintext;

AddRoundKey (s, key[0]);
for (r = 0; r < 9; r++)
{
  SubBytes (s);
  ShiftRows (s);
  MixColumns (s);
  AddRoundKey (s, key[r + 1]);
}
SubBytes (s);
ShiftRows (s);
AddRoundKey (s, key[10]);

ciphertext = s;
```

# Réarrangement de l'algorithme AES

```
s = plaintext;

AddRoundKey (s, key[0]);
for (r = 0; r < 9; r++)
{
  SubBytes (s);
  ShiftRows (s);
  MixColumns (s);
  AddRoundKey (s, key[r + 1]);
}
SubBytes (s);
ShiftRows (s);
AddRoundKey (s, key[10]);

ciphertext = s;
```

```
s = plaintext;

for (r = 0; r < 9; r++)
{
  AddRoundKey (s, key[r]);
  ShiftRows (s);
  SubBytes (s);
  MixColumns (s);
}
AddRoundKey (s, key[9]);
ShiftRows (s);
SubBytes (s);
AddRoundKey (s, key[10]);

ciphertext = s;
```

# Réarrangement de l'algorithme AES

```
AddRoundKey (state, key[r]);
ShiftRows (state);
```

est équivalent à :

```
ShiftRows (state);
AddRoundKey (state, ShiftRows (key[r]));
```

# Algorithme AES réarrangé

```
state = plaintext;

for (round = 0; round < 9; round++)
{
  ShiftRows (state);
  AddRoundKey (state, ShiftRows (key[round]));
  SubBytes (state);
  MixColumns (state);
}
ShiftRows (state);
AddRoundKey (state, ShiftRows (key[9]));
SubBytes (state);
AddRoundKey (state, key[bloc 10]);

ciphertext = state;
```

# Algorithme AES réarrangé

```
state = plaintext;

for (round = 0; round < 9; round++)
{
  ShiftRows (state);
  AddRoundKey (state, ShiftRows (key[round]));
  SubBytes (state);
  MixColumns (state);
}
ShiftRows (state);
AddRoundKey (state, ShiftRows (key[9]));
SubBytes (state);
AddRoundKey (state, key[bloc 10]);

ciphertext = state;
```

- À partir de maintenant, key désigne ShiftRows (key) .

# Tables de correspondance

**début du tour**

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

clef étendue du tour :

$$\begin{bmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{bmatrix} = \begin{bmatrix} K_0 & K_1 & K_2 & K_3 \end{bmatrix}$$

$$\Big\downarrow \text{ShiftRows}$$

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_5 & x_9 & x_{13} & x_1 \\ x_{10} & x_{14} & x_2 & x_6 \\ x_{11} & x_{15} & x_3 & x_7 \end{bmatrix}$$

**division en 4 étapes**

$$C_0 = \begin{bmatrix} x_0 \\ x_5 \\ x_{10} \\ x_{11} \end{bmatrix} \quad C_1 = \begin{bmatrix} x_4 \\ x_9 \\ x_{14} \\ x_{15} \end{bmatrix} \quad C_2 = \begin{bmatrix} x_8 \\ x_{13} \\ x_2 \\ x_3 \end{bmatrix} \quad C_3 = \begin{bmatrix} x_{12} \\ x_1 \\ x_6 \\ x_7 \end{bmatrix}$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$C_0 \oplus K_0 \qquad C_1 \oplus K_1 \qquad C_2 \oplus K_2 \qquad C_3 \oplus K_3$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$\text{SubBytes}(C_0 \oplus K_0) \qquad \text{SubBytes}(C_1 \oplus K_1) \qquad \text{SubBytes}(C_2 \oplus K_2) \qquad \text{SubBytes}(C_3 \oplus K_3)$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$MC \cdot \text{SubBytes}(C_0 \oplus K_0) \qquad MC \cdot \text{SubBytes}(C_1 \oplus K_1) \qquad MC \cdot \text{SubBytes}(C_2 \oplus K_2) \qquad MC \cdot \text{SubBytes}(C_3 \oplus K_3)$$

$$\begin{bmatrix} y_0 & y_4 & y_8 & y_{12} \\ y_1 & y_5 & y_9 & y_{13} \\ y_2 & y_6 & y_{10} & y_{14} \\ y_3 & y_7 & y_{11} & y_{15} \end{bmatrix}$$

**fin du tour**

**début du tour**

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

clef étendue du tour :

$$\begin{bmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{bmatrix} = \begin{bmatrix} K_0 & K_1 & K_2 & K_3 \end{bmatrix}$$

$$\downarrow \text{ShiftRows}$$

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_5 & x_9 & x_{13} & x_1 \\ x_{10} & x_{14} & x_2 & x_6 \\ x_{11} & x_{15} & x_3 & x_7 \end{bmatrix}$$

**division en 4 étapes**

$$C_0 = \begin{bmatrix} x_0 \\ x_5 \\ x_{10} \\ x_{11} \end{bmatrix} \quad C_1 = \begin{bmatrix} x_4 \\ x_9 \\ x_{14} \\ x_{15} \end{bmatrix} \quad C_2 = \begin{bmatrix} x_8 \\ x_{13} \\ x_2 \\ x_3 \end{bmatrix} \quad C_3 = \begin{bmatrix} x_{12} \\ x_1 \\ x_6 \\ x_7 \end{bmatrix}$$

$$C_0 \oplus K_0 \quad C_1 \oplus K_1 \quad C_2 \oplus K_2 \quad C_3 \oplus K_3$$

$$\text{SubBytes}(C_0 \oplus K_0) \quad \text{SubBytes}(C_1 \oplus K_1) \quad \text{SubBytes}(C_2 \oplus K_2) \quad \text{SubBytes}(C_3 \oplus K_3)$$

$$MC \cdot \text{SubBytes}(C_0 \oplus K_0) \quad MC \cdot \text{SubBytes}(C_1 \oplus K_1) \quad MC \cdot \text{SubBytes}(C_2 \oplus K_2) \quad MC \cdot \text{SubBytes}(C_3 \oplus K_3)$$

$$\begin{bmatrix} y_0 & y_4 & y_8 & y_{12} \\ y_1 & y_5 & y_9 & y_{13} \\ y_2 & y_6 & y_{10} & y_{14} \\ y_3 & y_7 & y_{11} & y_{15} \end{bmatrix}$$

**fin du tour**

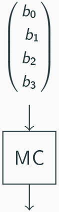
# Une étape

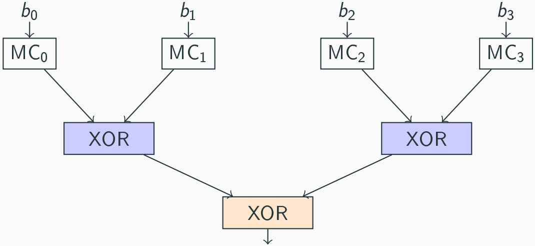
$$
\begin{tikzcd}
B = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \arrow[d] \\
B \oplus K \arrow[d] \\
\mathrm{SubBytes}(B \oplus K) \arrow[d] \\
MC \cdot \mathrm{Sub}(B \oplus K)
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & B \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] & \\
b_0 \arrow[d] & b_1 \arrow[d] & b_2 \arrow[d] & b_3 \arrow[d] \\
b_0 \oplus k_0 \arrow[d] & b_1 \oplus k_1 \arrow[d] & b_2 \oplus k_2 \arrow[d] & b_3 \oplus k_3 \arrow[d] \\
\mathrm{SBox}(b_0 \oplus k_0) \arrow[d] & \mathrm{SBox}(b_1 \oplus k_1) \arrow[d] & \mathrm{SBox}(b_2 \oplus k_2) \arrow[d] & \mathrm{SBox}(b_3 \oplus k_3) \arrow[d] \\
? & ? & ? & ?
\end{tikzcd}
$$

# Redécoupage de MixColumns

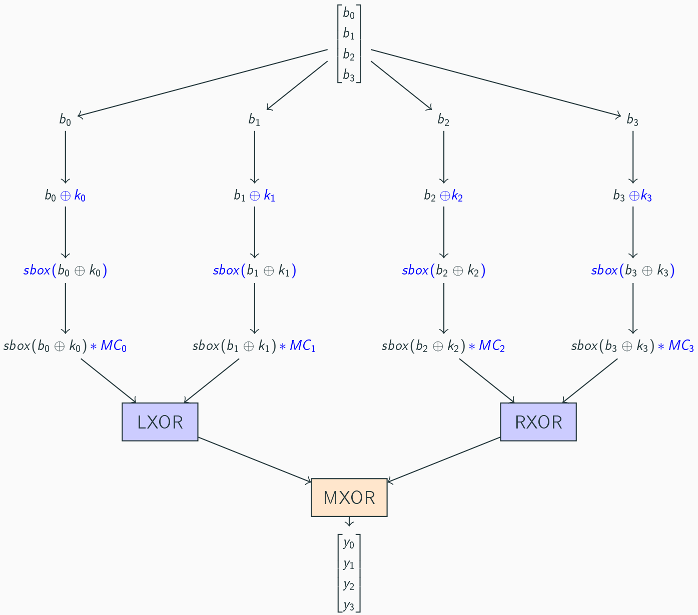
$$\mathrm{MC} = (MC_1 \;\; MC_2 \;\; MC_3 \;\; MC_4)$$

$$\mathrm{MC}\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = (b_0 \cdot \mathrm{MC}_0 \oplus b_1 \cdot \mathrm{MC}_1) \oplus (b_2 \cdot \mathrm{MC}_2 \oplus b_3 \cdot \mathrm{MC}_3)$$

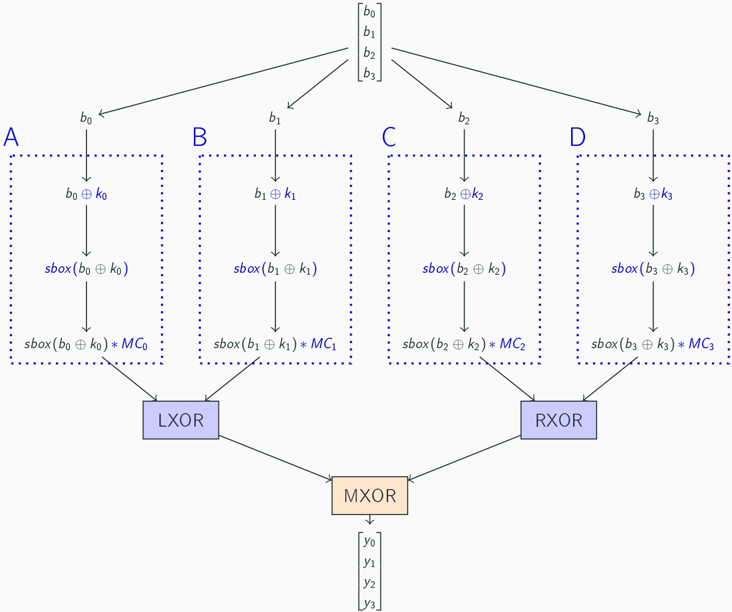


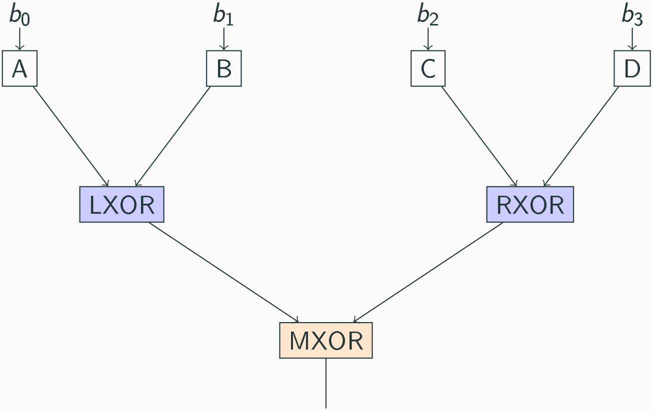
# Construction des tables de correspondance



# Construction des tables de correspondance

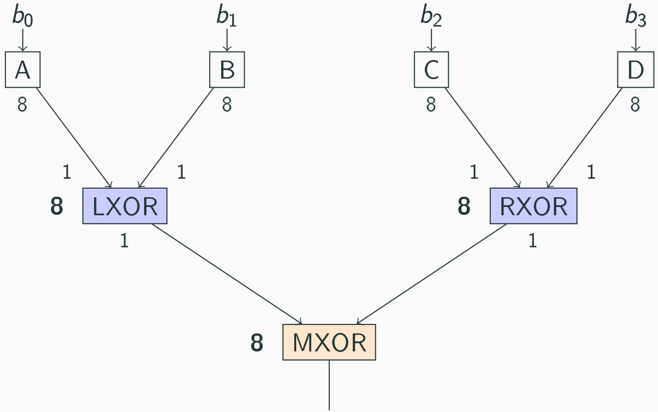


# Construction des tables de correspondance



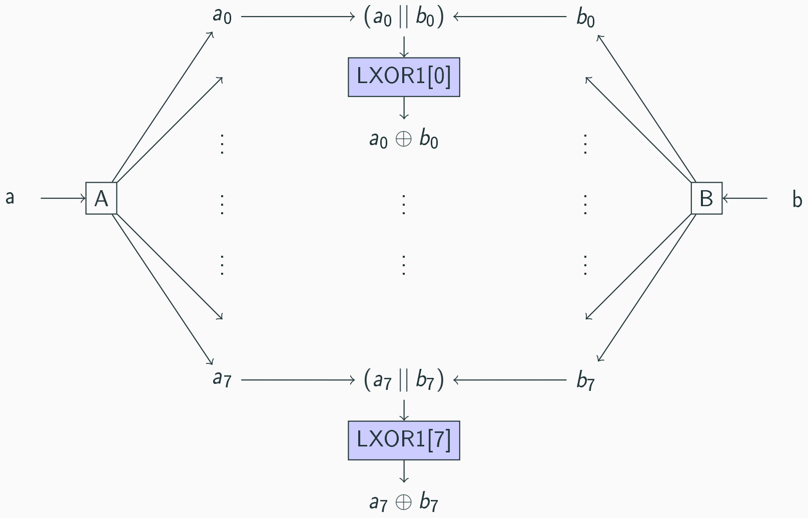

$$\left[A(\texttt{col}) \oplus B(\texttt{col})\right] \oplus \left[C(\texttt{col}) \oplus D(\texttt{col})\right]$$

# Construction des tables de correspondance

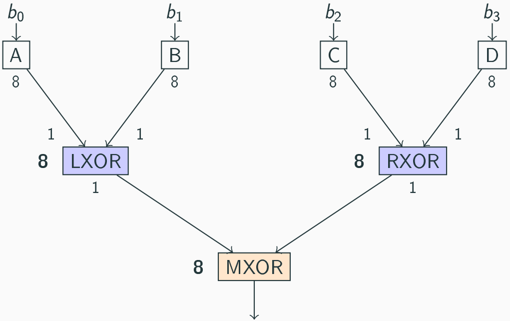



$$\left[A(\texttt{col}) \oplus B(\texttt{col})\right] \oplus \left[C(\texttt{col}) \oplus D(\texttt{col})\right]$$

# Construction des tables de correspondance



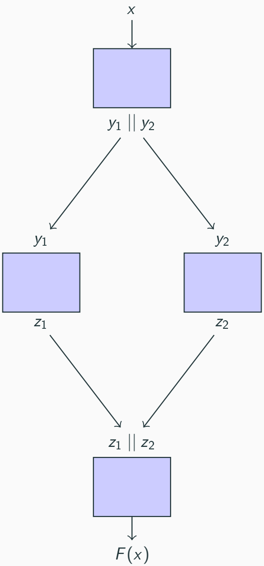
# Première attaque



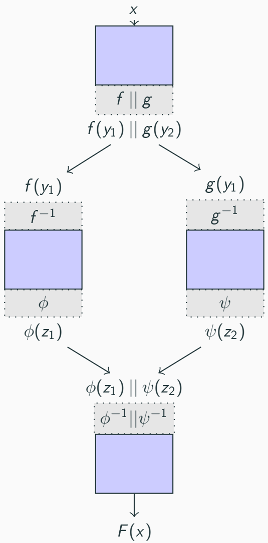

$$A[b_0] = \begin{pmatrix} 02 * SBox(b_0 \oplus k) \\ 01 * SBox(b_0 \oplus k) \\ 01 * SBox(b_0 \oplus k) \\ 03 * SBox(b_0 \oplus k) \end{pmatrix}$$

# Encodages

# Encodages



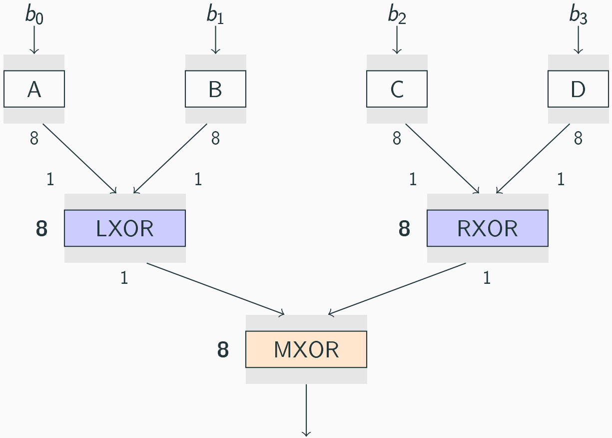
# Encodages



$x$
$f \,||\, g$
$f(y_1) \,||\, g(y_2)$
$f(y_1)$
$g(y_1)$
$f^{-1}$
$g^{-1}$
$\phi$
$\psi$
$\phi(z_1)$
$\psi(z_2)$
$\phi(z_1) \,||\, \psi(z_2)$
$\phi^{-1}||\psi^{-1}$
$F(x)$

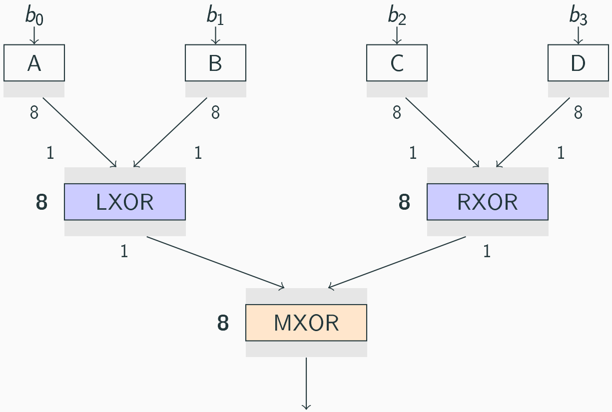
# Encodages

Étape d'un tour générique :



# Encodages

Étape du premier tour :



# Encodages : signature de fréquence

signature de fréquence

- s'applique à un tableau de dimensions $N \times N$

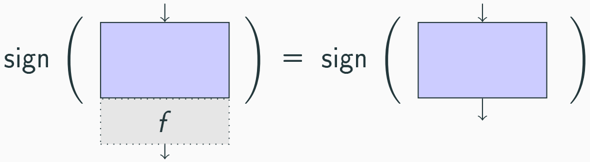
# Encodages : signature de fréquence

signature de fréquence

- s'applique à un tableau de dimensions $N \times N$
- $\mathrm{sign}(A)$ permet de retrouver k

signature de fréquence

- s'applique à un tableau de dimensions $N \times N$
- sign($A$) permet de retrouver k
- invariant :



# Encodages : signature de fréquence

$$\begin{bmatrix} 0x11 & 0x32 & 0x03 & 0x10 \\ 0x03 & 0x23 & 0x01 & 0x00 \\ 0x01 & 0x20 & 0x23 & 0x20 \\ 0x11 & 0x21 & 0x02 & 0x30 \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} (1,1) & (3,2) & (0,3) & (1,0) \\ (0,3) & (2,3) & (0,1) & (0,0) \\ (0,1) & (2,0) & (2,3) & (2,0) \\ (1,1) & (2,1) & (0,2) & (3,0) \end{bmatrix} \begin{matrix} \longrightarrow (211,1111) \\ \longrightarrow (31,211) \\ \\ \\ \end{matrix}$$

$$\begin{matrix} \downarrow & \downarrow \\ (22,31) & (31,1111) \end{matrix}$$

# Encodages : signature de fréquence

$$\phi(0) = e \quad \phi(1) = b \quad \phi(2) = 5 \quad \phi(3) = a \quad \cdots$$

$$\psi(0) = 2 \quad \psi(1) = b \quad \psi(2) = 3 \quad \psi(3) = c \quad \cdots$$

$$\begin{bmatrix} (1,1) & (3,2) & (0,3) & (1,0) \\ (0,3) & (2,3) & (0,1) & (0,0) \\ (0,1) & (2,0) & (2,3) & (2,0) \\ (1,1) & (2,1) & (0,2) & (3,0) \end{bmatrix}$$

$$(\phi, \psi) \downarrow$$

$$\begin{bmatrix} (b,b) & (a,3) & (e,c) & (b,2) \\ (e,c) & (5,c) & (e,b) & (e,2) \\ (e,b) & (5,2) & (5,c) & (5,2) \\ (b,b) & (5,b) & (e,2) & (a,2) \end{bmatrix} \begin{array}{l} \longrightarrow (211, 1111) \\ \longrightarrow (31, 211) \\ \\ \\ \end{array}$$

$$\downarrow \qquad \downarrow$$

$$(22, 31) \quad (31, 1111)$$

# Mixing bijections

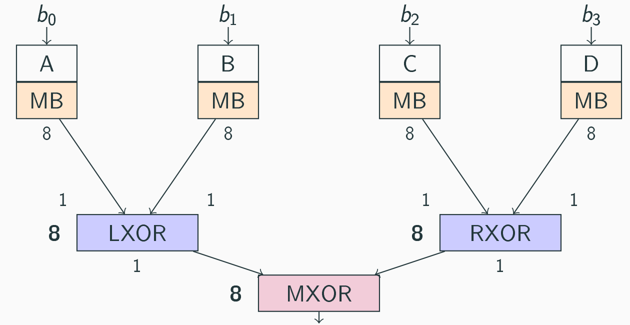
# Mixing bijections

- Echec des encodages seuls, une permutation aurait suffi...

# Mixing bijections

- Echec des encodages seuls, une permutation aurait suffi...
- analogie avec confusion (encodages) et diffusion (mixing bijections) de Shannon.

# Mixing bijections



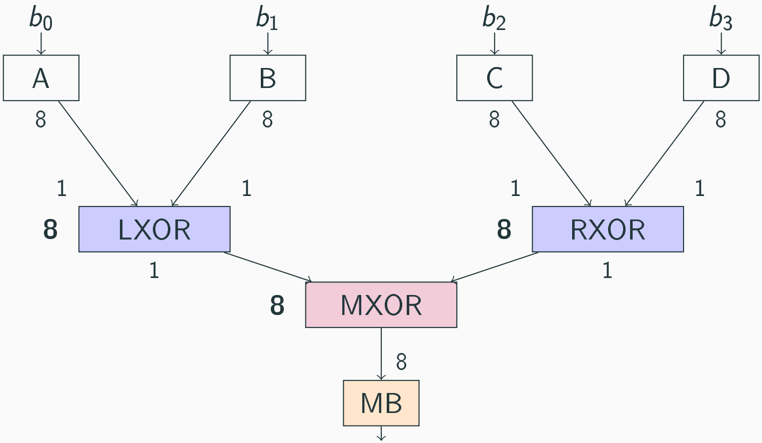

$$\big(\mathrm{MB}(A[b_0]) \oplus \mathrm{MB}(B[b_1])\big) \oplus \big(\mathrm{MB}(C[b_2]) \oplus \mathrm{MB}(D[b_3])\big)$$

$$=$$

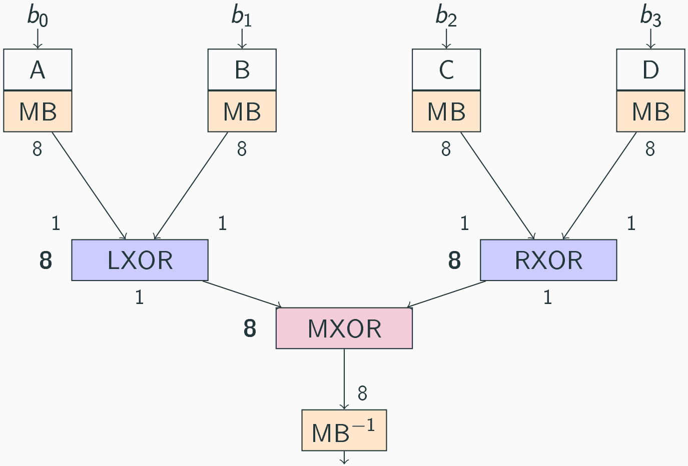
$$\mathrm{MB}\big(\,(A[b_0] \oplus B[b_1]) \oplus (C[b_2] \oplus D[b_3])\,\big)$$

# Mixing bijections

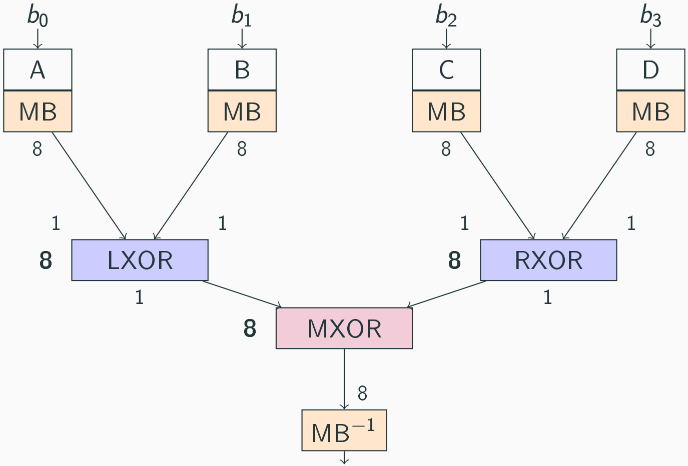
$$\mathrm{MB}\big(\,(A[b_0] \oplus B[b_1]) \oplus (C[b_2] \oplus D[b_3])\,\big)$$



# Mixing bijections



# Mixing bijections

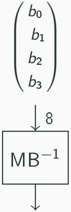


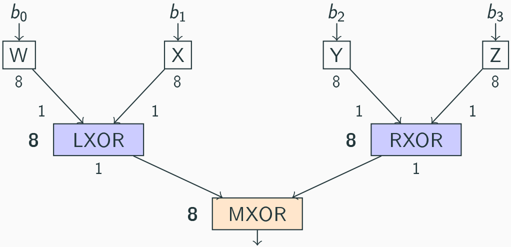

- Problème : $MB^{-1}$ a pour entrée un mot.

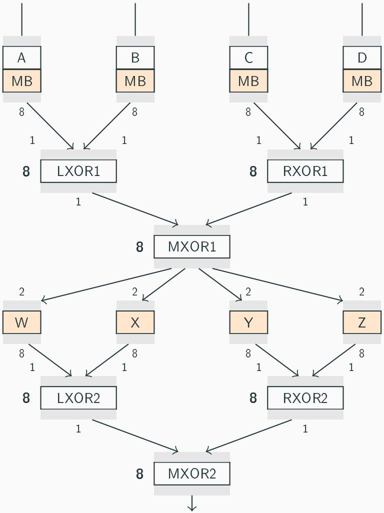
# Mixing bijections

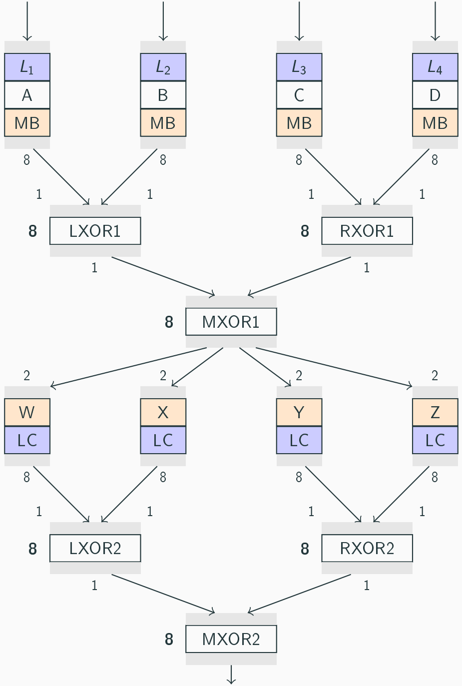
$$\mathrm{MB}^{-1} = (W \; X \; Y \; Z)$$

$$\mathrm{MB}^{-1} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = (b_0 \cdot W \oplus b_1 \cdot X) \oplus (b_2 \cdot Y \oplus b_3 \cdot Z)$$



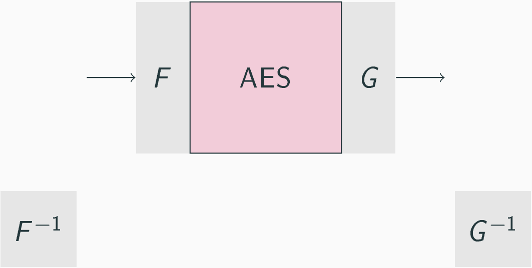




A
MB
B
MB
C
MB
D
MB
8
8
8
8
1
1
1
1
8
LXOR1
8
RXOR1
1
1
8
MXOR1
2
2
2
2
W
X
Y
Z
8
8
8
8
1
1
1
1
8
LXOR2
8
RXOR2
1
1
8
MXOR2



$L_1$
A
MB
$L_2$
B
MB
$L_3$
C
MB
$L_4$
D
MB
8
8
8
8
1
1
1
1
8
LXOR1
8
RXOR1
1
1
8
MXOR1
2
2
2
2
W
LC
X
LC
Y
LC
Z
LC
8
8
8
8
1
1
1
1
8
LXOR2
8
RXOR2
1
1
8
MXOR2

# Encodages externes




- attaque BGE due à O. Billet, H. Gilbert et C. Ech-Chatbi (2005)

## Et aujourd'hui ?

CHES 2017

- 94 implémentations proposées ;
- 13 résistèrent plus d'un jour, la plus solide tint 28 jours.

Attaques principales :

- Differential Computation Analysis (DCA)
- Differential Fault Analysis (DFA)

Toutefois

- La cryptographie whitebox reste utilisée
- l'existence d'une obfuscation sécurisée reste une question ouverte