Cybersécurité hardware

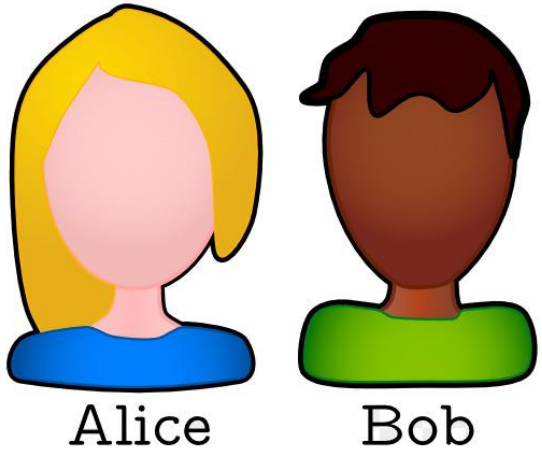
Chiffrement AES et attaques par canaux auxiliaires

Quentin Daval

TABLE DES MATIERES

01

INTRODUCTION



VOCABULAIRE

ENCODAGE

L'encodage est la transformation, par un protocole connu, de données en un format différent.

CHIFFREMENT

Le chiffrement est la transformation de donnée ayant pour but la dissimulation de ces données aux personnes non autorisées.

HACHAGE

Le hachage est une transformation irréversible d'une données quelconque en un texte de taille fixe

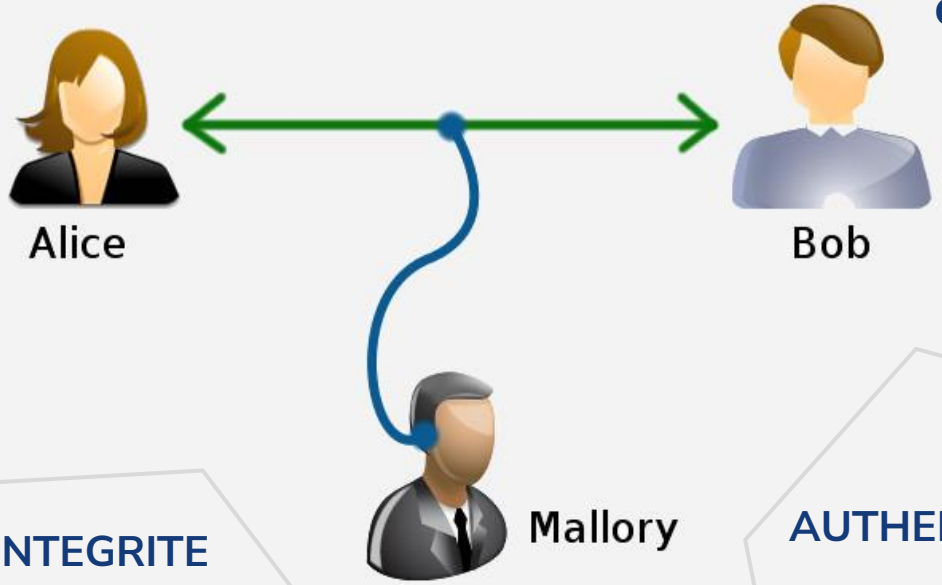
DECRYPTAGE

Le décryptage est l'action effectuée par une personne cherchant à déchiffrer des données sans avoir accès à la clef de déchiffrement.

CONFIDENTIALITE

Les systèmes et les données ne sont accessibles qu'aux utilisateurs autorisés

INTERET DU CHIFFREMENT



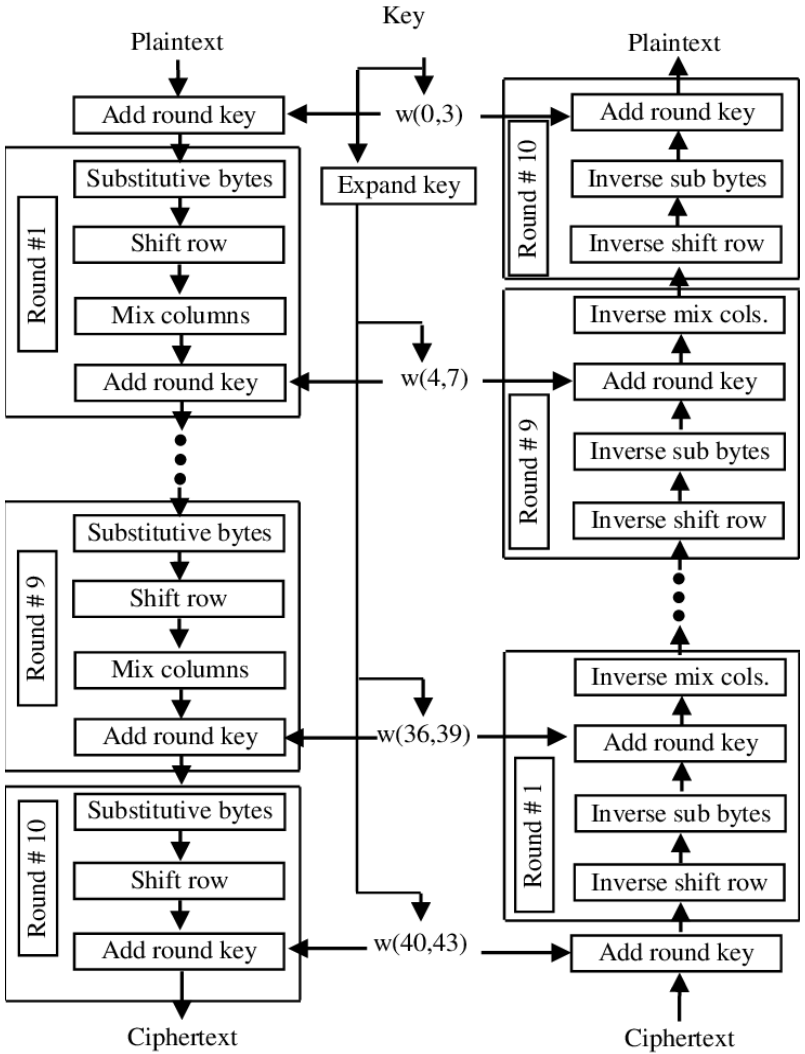
INTEGRITE

Les systèmes et les données sont fiables et complets

AUTHENTIFICATION

La personne accédant aux systèmes et aux données est bien celle qu'elle prétend être

TABLE DES MATIERES



02

CHIFFREMENT AES

NEWS

DONNEES

Les données seront représentée de manière équivalent comme des **octets**, des **caractères ASCII** et des **nombres hexadécimaux** à deux chiffres

STATE

Nom donné aux 16 octets de donnée manipulées à **n'importe quel moment** de l'algorithme

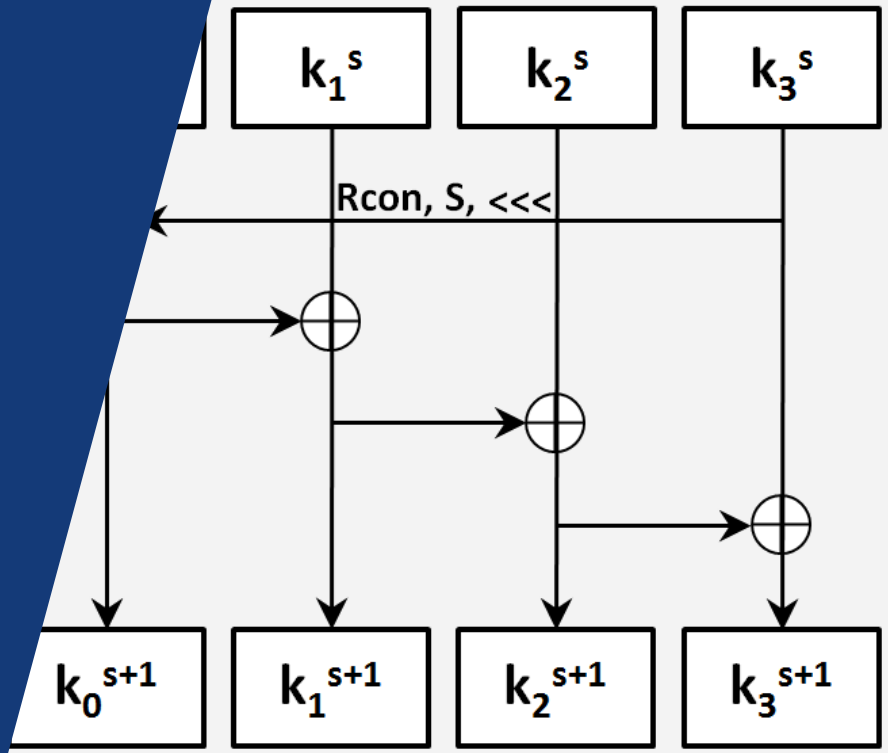
THE KEY

Clef de **128 bits** la plupart du temps (sinon de 192 ou 256 bits)

PLAIN/CIPHERED TEXT

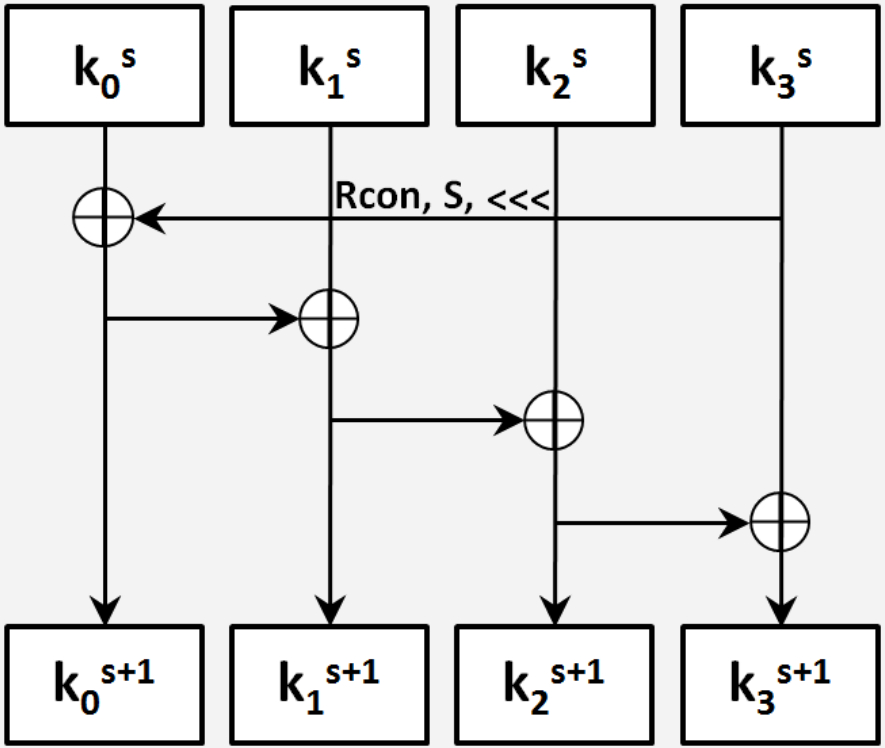
Correspond au **state** au **début** et à la **fin** de l'algorithme

ETAPE 1: LE “KEY SCHEDULE”



Lors de chacun des rounds de l'AES, la clef de départ est modifiée par un algorithme nommé key Schedule

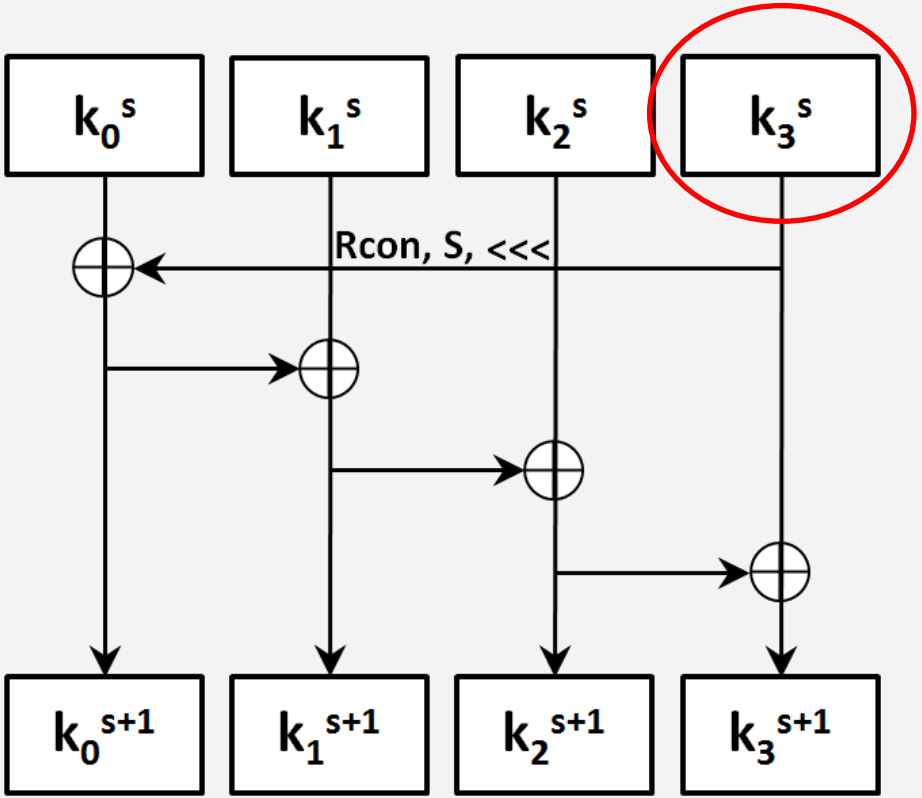
ETAPE 1: LE “KEY SCHEDULE”



ETAPE 1: LE “KEY SCHEDULE”

3 opérations sont effectuées sur les 4 derniers octets de la clef:

- RotWord
- SubWord
- Rcon



ETAPE 1: LE “KEY SCHEDULE”

3 opérations sont effectuées sur les 4 derniers octets de la clef:

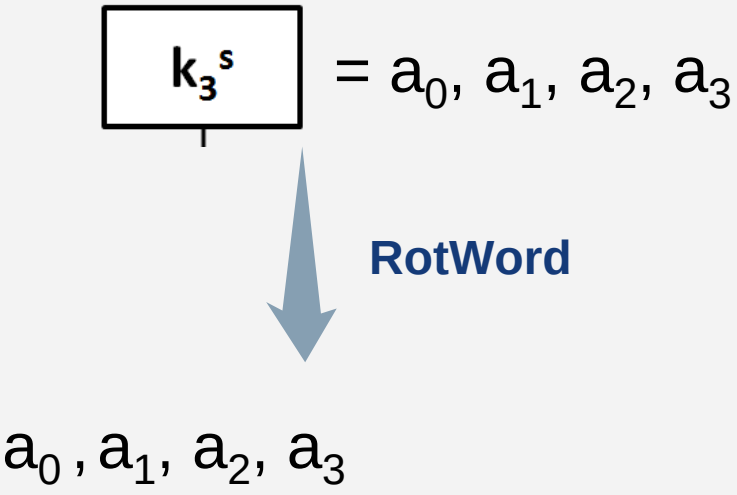
- RotWord
- SubWord
- Rcon

$k_3^s = a_0, a_1, a_2, a_3$

ETAPE 1: LE “KEY SCHEDULE”

3 opérations sont effectuées sur les 4 derniers octets de la clef:

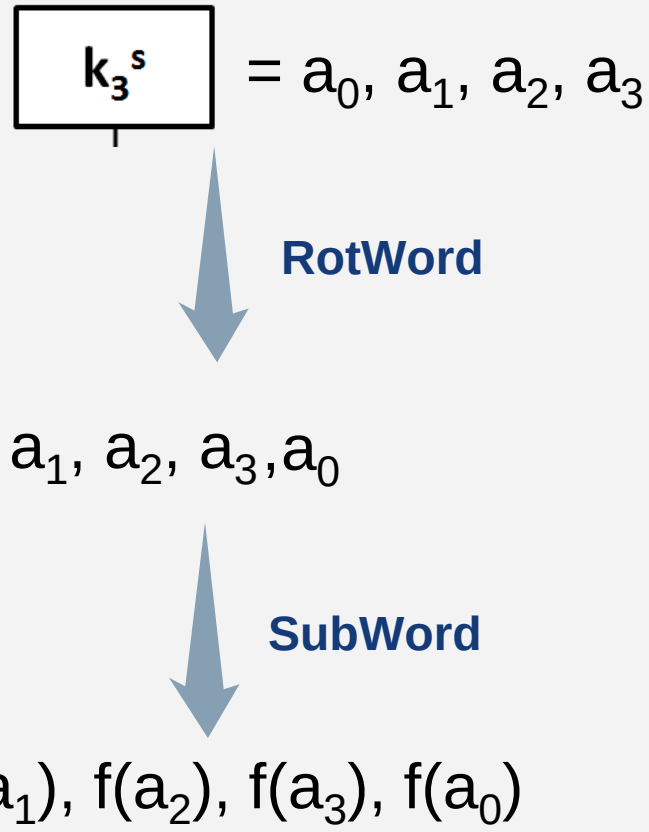
- RotWord
- SubWord
- Rcon



ETAPE 1: LE “KEY SCHEDULE”

3 opérations sont effectuées sur les 4 derniers octets de la clef:

- RotWord
- SubWord
- Rcon



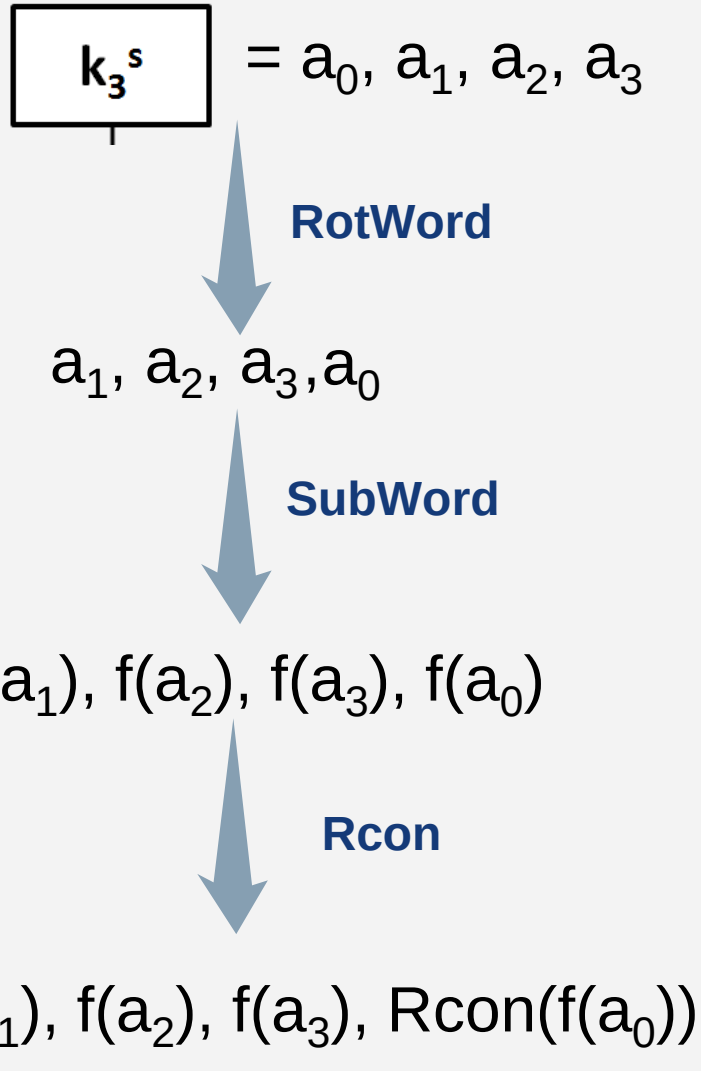
SBox

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

ETAPE 1: LE “KEY SCHEDULE”

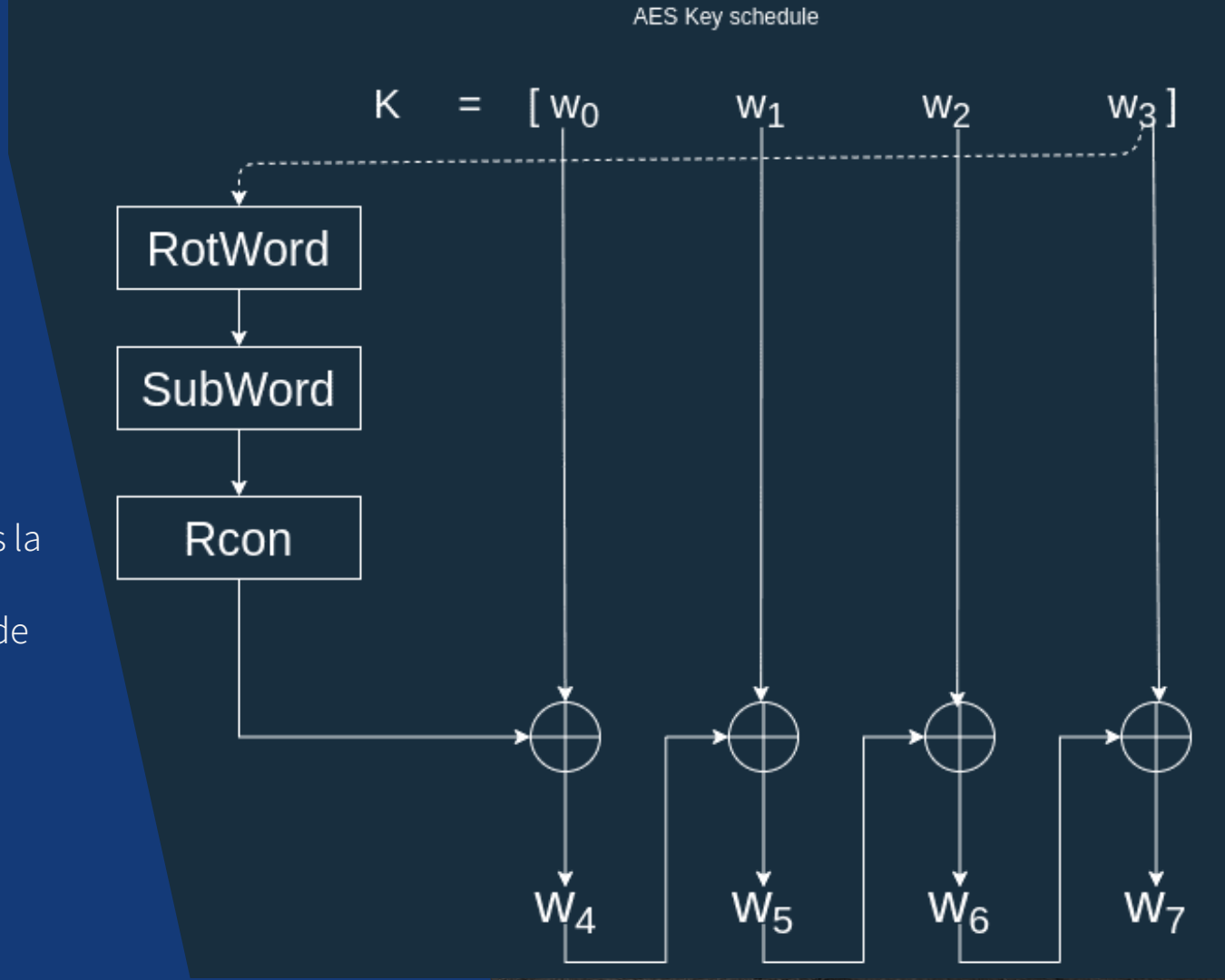
3 opérations sont effectuées sur les 4 derniers octets de la clef:

- RotWord
- SubWord
- Rcon

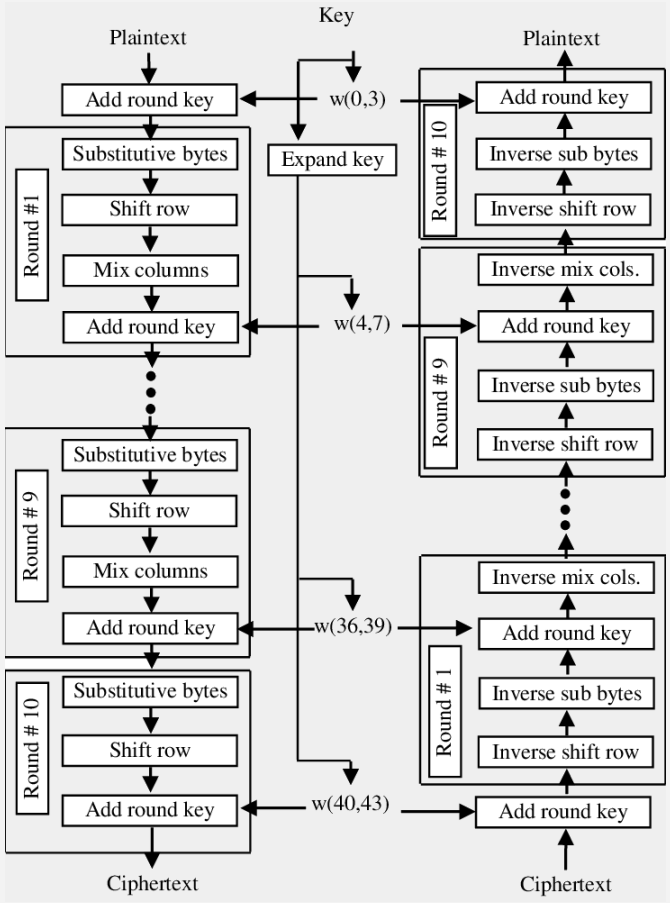


REATION DE LA LEF

ne fois les 3 opérations effectuées la ef est obtenue avec une série de OR entre les différents morceaux de clef

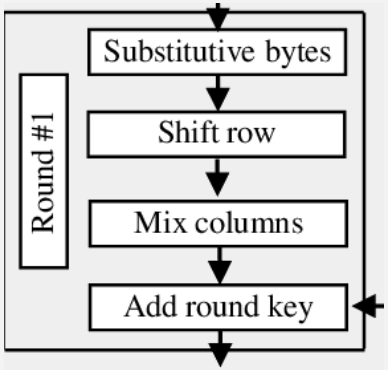


ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT

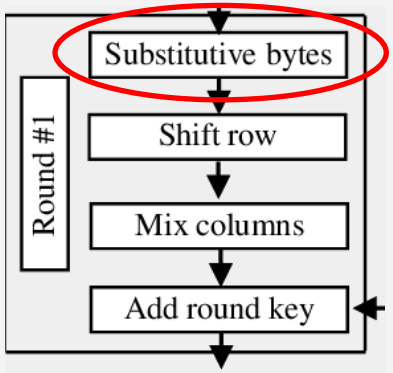


Le state est modifier lors de **10 rounds identiques** (sauf pour le dernier) et subit à chaque fois **4 opérations**.

ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT



ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT



SubBytes

$a_0, a_1, \ldots, a_{14}, a_{15}$

$f(a_0), f(a_1), \ldots, f(a_{14}), f(a_{15})$

Substitute bytes est la **généralisation** à 16 octets de la transformation **SubWord** du key schedule

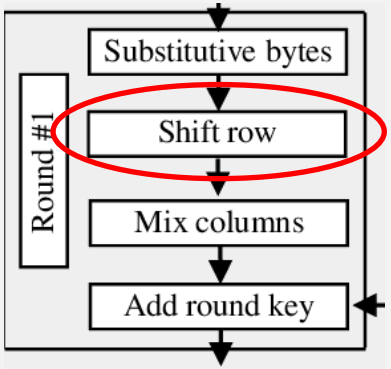
ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT

$$a_0, a_1, a_2, a_3, \ldots, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}$$

$$\begin{matrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{matrix}$$

Par simplicité de représentation on voit maintenant le state comme une **matrice 4x4**

ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT

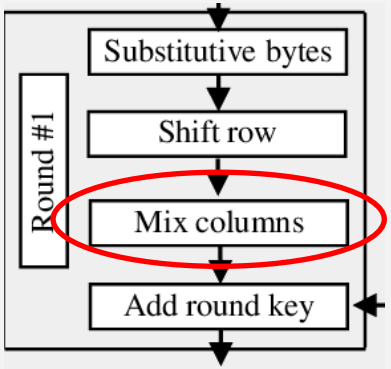


Shift row est un **décalage des lignes**: on décale de **1** la deuxième ligne, de **2** la troisième et de **3** la dernière

ShiftRow

$$\begin{matrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{matrix} \rightarrow \begin{matrix} a_0 & a_4 & a_8 & a_{12} \\ a_5 & a_9 & a_{13} & a_1 \\ a_{10} & a_{14} & a_2 & a_6 \\ a_{15} & a_3 & a_7 & a_{11} \end{matrix}$$

ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT



Mix columns est la **multiplication matricielle** du state et de la matrice mix

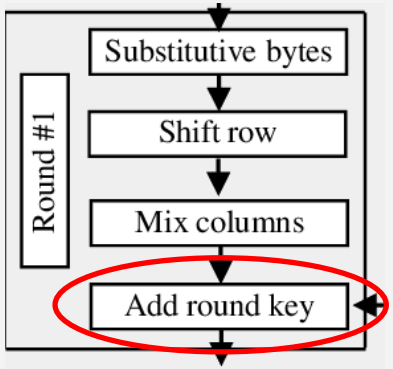
MixColumns

Mix:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

$$\begin{matrix} a_0 & a_4 & a_8 & a_{12} \\ a_5 & a_9 & a_{13} & a_1 \\ a_{10} & a_{14} & a_2 & a_6 \\ a_{15} & a_3 & a_7 & a_{11} \end{matrix}$$

ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT



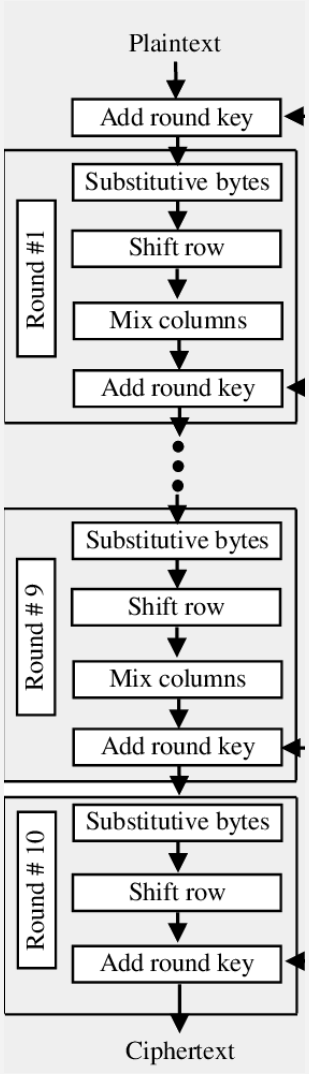
Add round key

$a_0, a_1, \ldots, a_{14}, a_{15}$

$k_0+a_0, \ldots, a_{14}+k_{14}, a_{15}+k_{15}$

Add round key consiste à ajouter la clef actuelle et le state (avec le **XOR** vu comme l'addition)

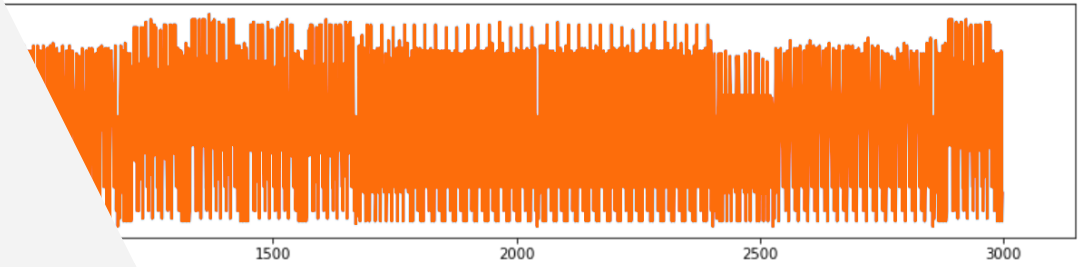
ETAPE 2: LES 10 ROUNDS DE CHIFFREMENT

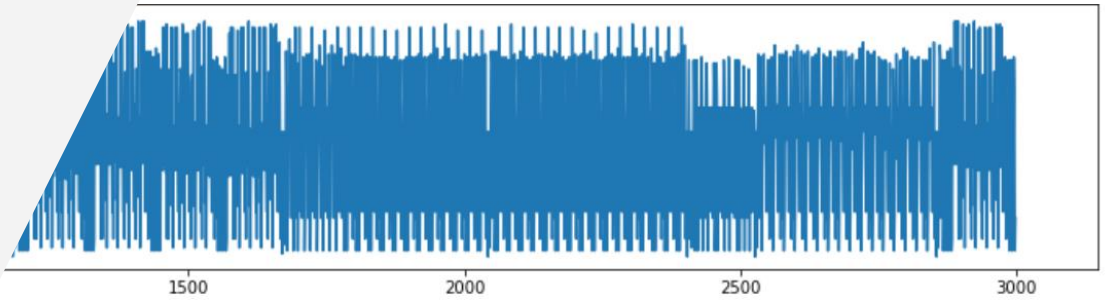


Lors du **dernier round** la seule différence est l'absence de la fonction **Mix columns**

03

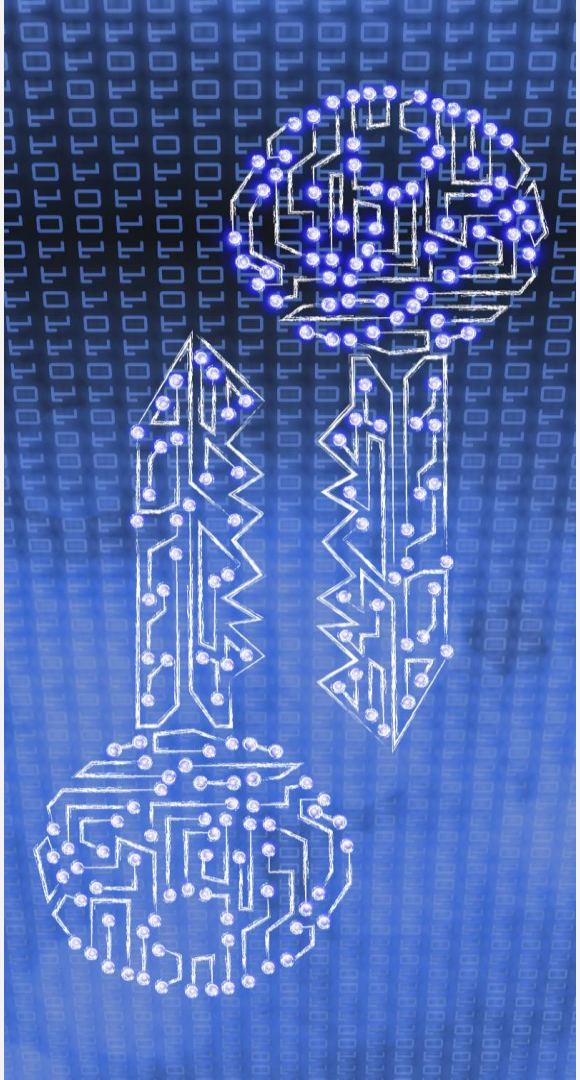
LES ATTAQUES A CANAUX AUXILIAIRES





CRYPTANALYSE

Décryptage d'un texte en ayant connaissance du texte chiffré et/ou du texte en clair

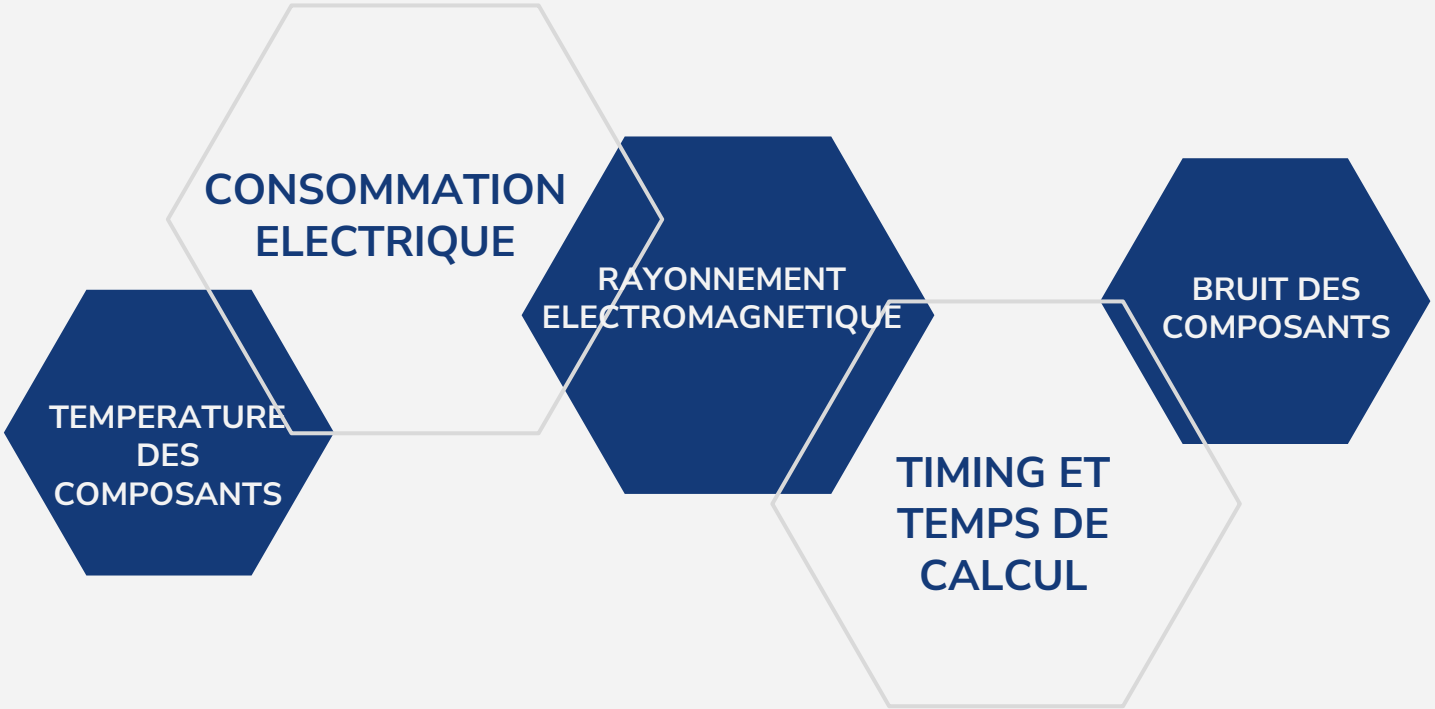


DISTINCTION

ATTAQUES PAR CANAUX AUXILIAIRES

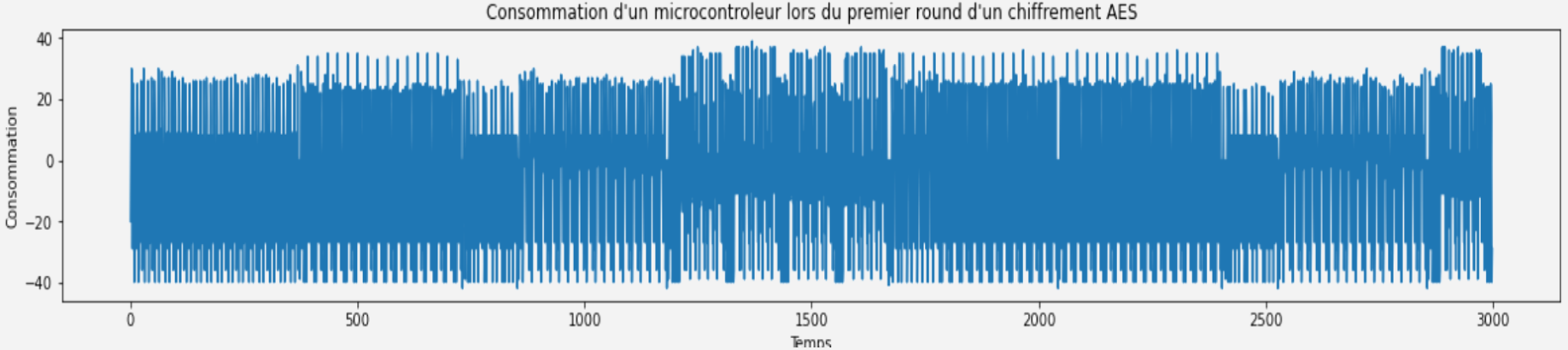
L'attaque de l'implémentation physique d'un algorithme de chiffrement

LES DIFFERENTES SOURCES DE FUITE D'INFORMATION



TRACES

On appelle **trace** l'ensemble des **points de mesure** récoltés pendant l'exécution d'un algorithme de chiffrement. On y associe souvent le texte en clair utilisé et/ou le texte chiffré obtenu



SPA

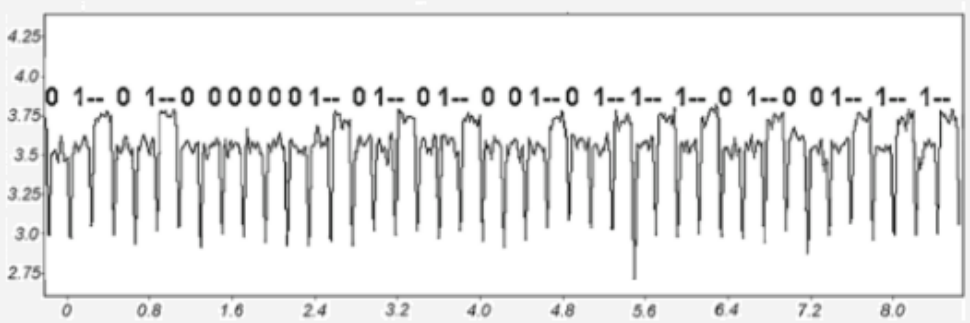
Si y a une **grande différence** entre deux consommation du circuit pour deux opérations différentes il est possible de **trouver directement** la clef

Algorithme 2 Algorithme d'exponentiation binaire

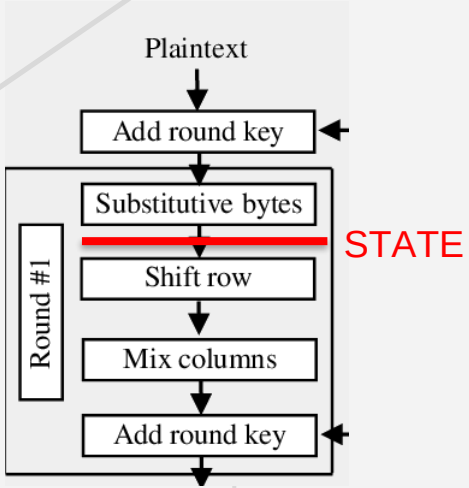
Entrée(s) : $c, n \in \mathbf{N}, c < n, d = \sum_{i=0}^{n-1} a_i 2^i, a_i \in \{0,1\}$

Sortie(s) : $x = c^d \ mod(n)$

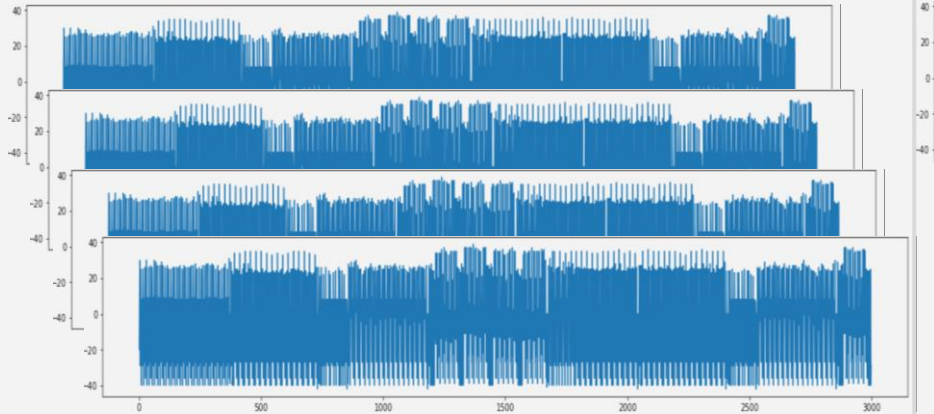
1: **pour** $i \in \{n-2, ..., 0\}$ **faire**
2: $x = x \times x \ mod(n)$ ▷ Mise au carré.
3: **si** $a_i = 1$ **alors**
4: $x = x \times c \ mod(n)$ ▷ Multiplication.
retourner x



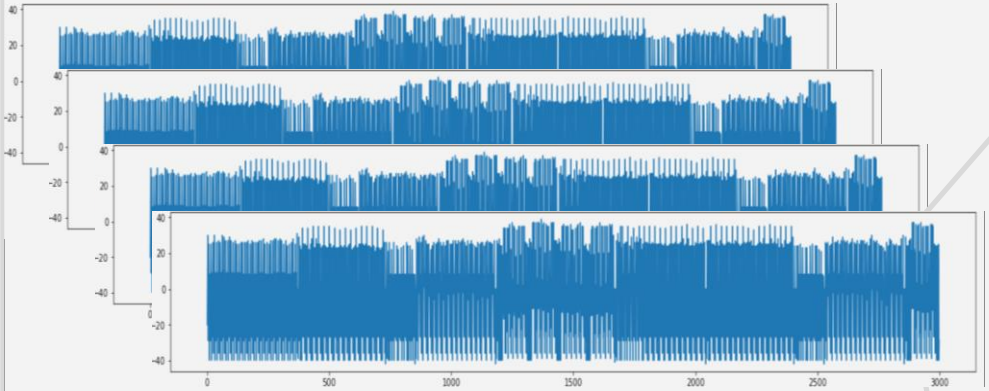
DPA



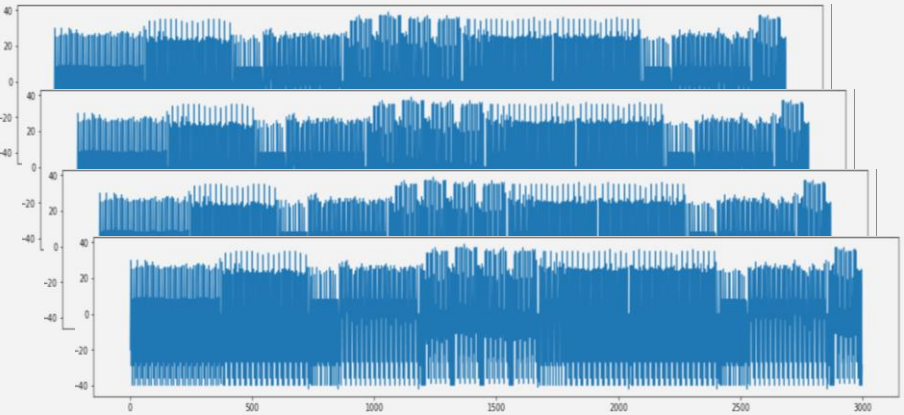
L'attaque DPA: **Differential Power Analysis** est une analyse **statistique** d'un ensemble de trace qui va permettre de retrouver la clef de chiffrement **octet par octet**.



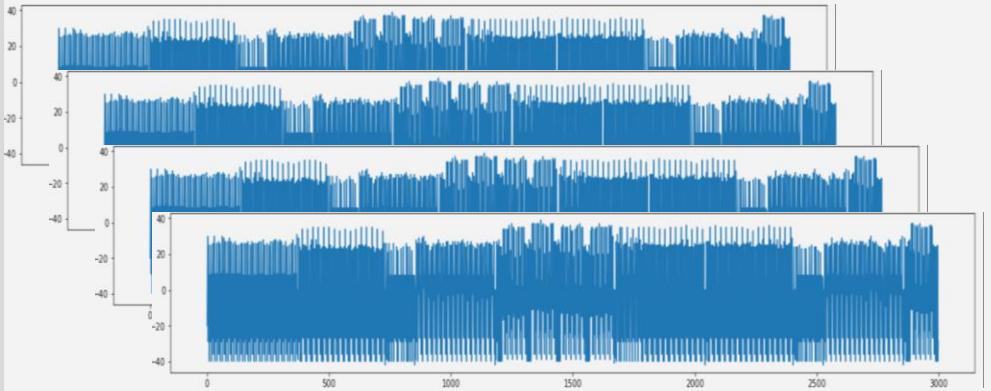
Hamming weight(Premier octet(STATE)) <4



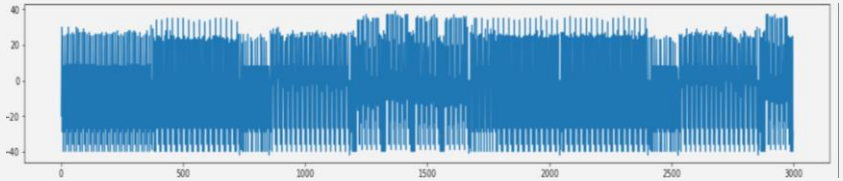
Hamming weight(Premier octet(STATE)) >= 4



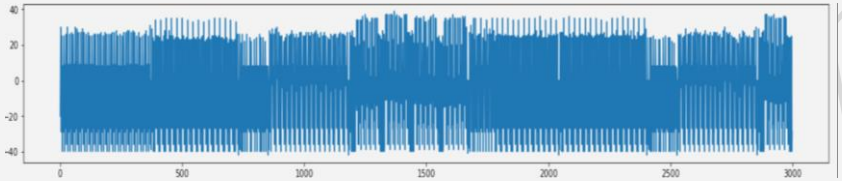
Hamming weight(Premier octet(STATE)) <4



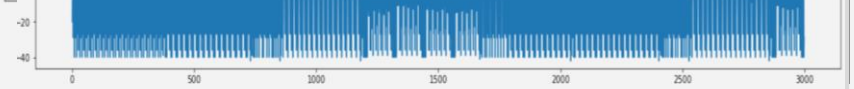
Hamming weight(Premier octet(STATE)) >=4



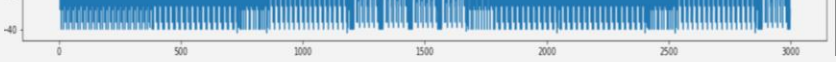
Moyenne des traces avec HW<4



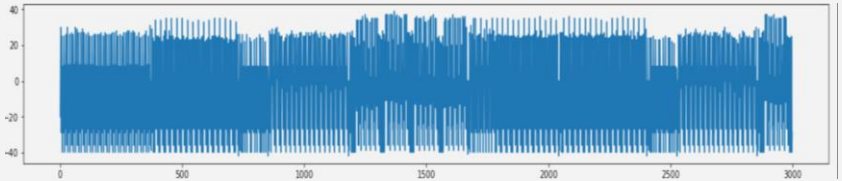
Moyenne des traces avec HW>=4



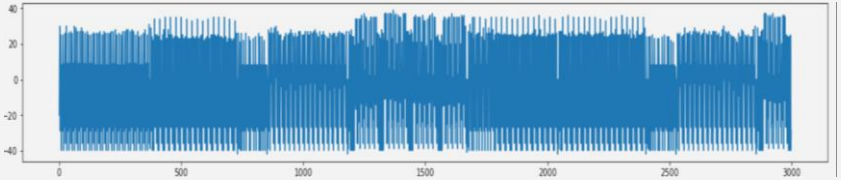
Hamming weight(Premier octet(STATE)) <4



Hamming weight(Premier octet(STATE)) >=4

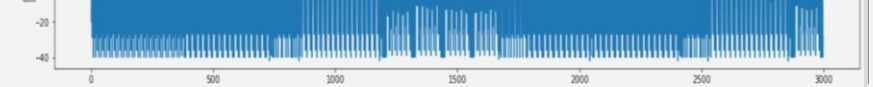


Moyenne des traces avec HW<4

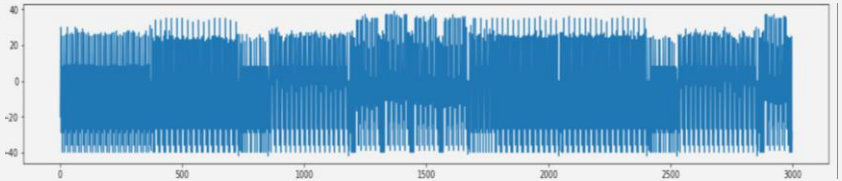


Moyenne des traces avec HW>=4

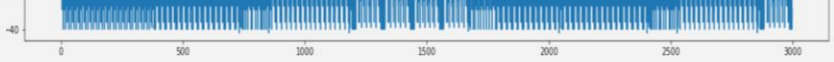
Soustraction



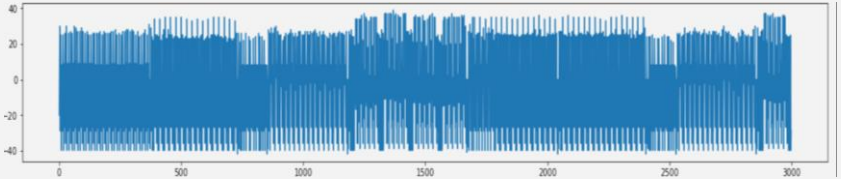
Hamming weight(Premier octet(STATE)) <4



Moyenne des traces avec HW<4

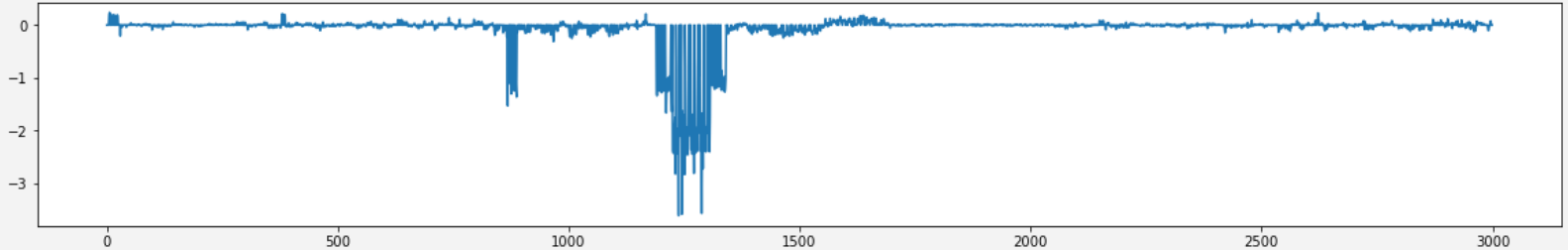


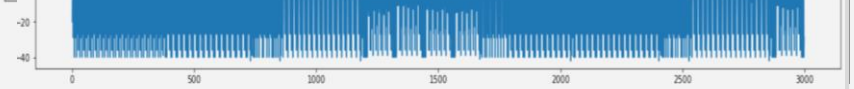
Hamming weight(Premier octet(STATE)) >=4



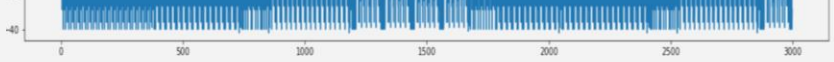
Moyenne des traces avec HW>=4

Soustraction

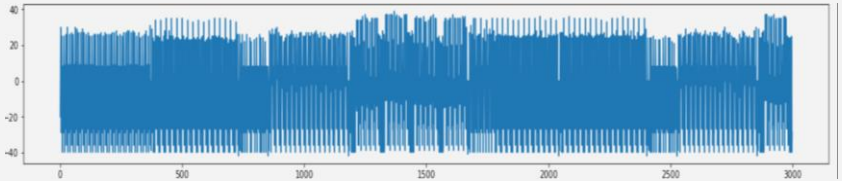




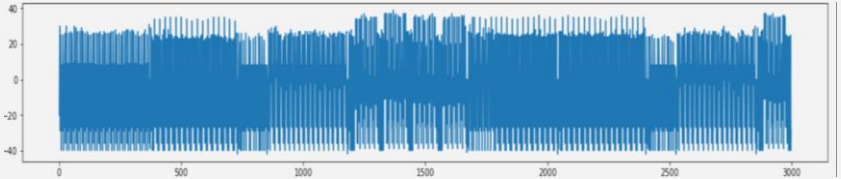
Hamming weight(Premier octet(STATE)) <4



Hamming weight(Premier octet(STATE)) >=4

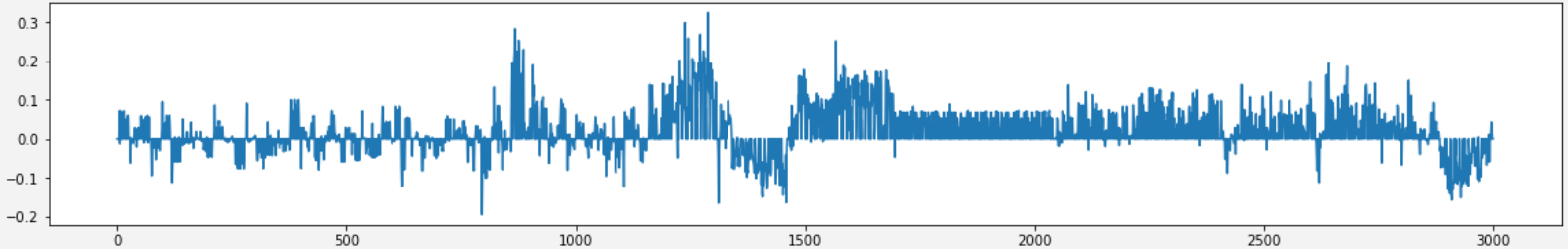


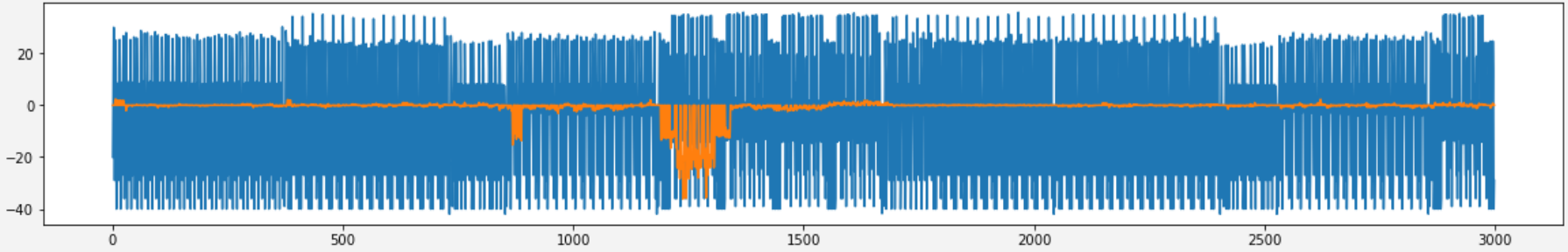
Moyenne des traces avec HW<4

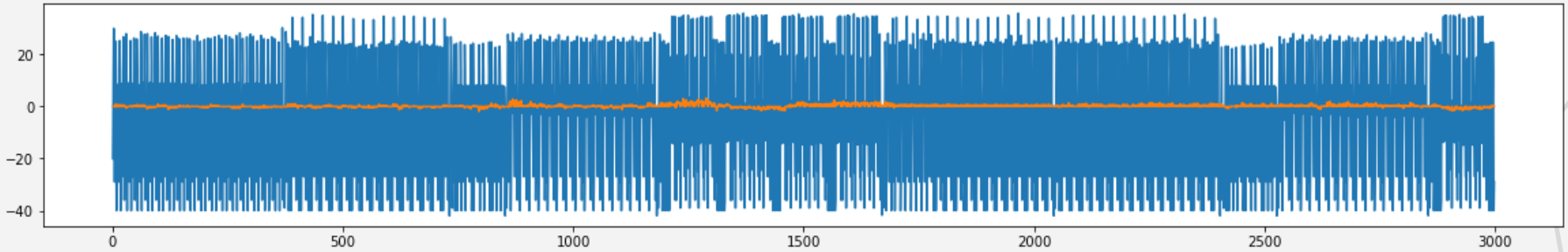


Moyenne des traces avec HW>=4

Soustraction

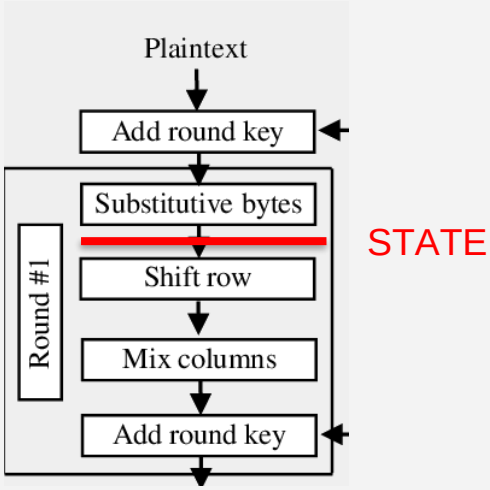


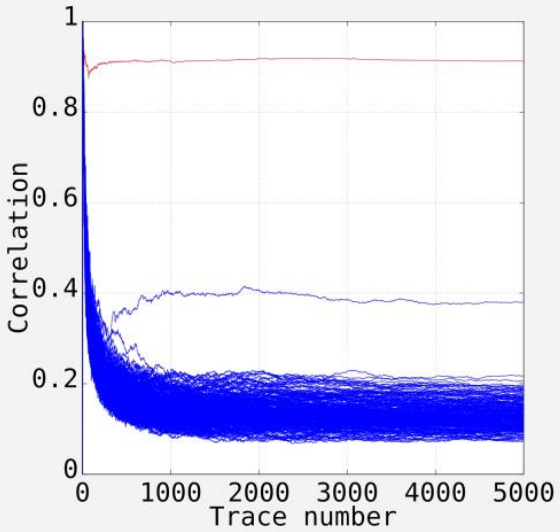

20
0
−20
−40
0
500
1000
1500
2000
2500
3000


20
0
−20
−40
0
500
1000
1500
2000
2500
3000

CPA

L'attaque CPA: **Correlation Power Analysis** est aussi une analyse **statistique** mais a l'avantage d'être plus rapide c'est-à-dire nécessite moins de trace pour obtenir des informations sur la clef.





04

A VOTRE TOUR!