Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber1 - CFA CCI Avignon

4 juin 2024

Chiffrement AES

AES = *Advanced Encryption Standard*

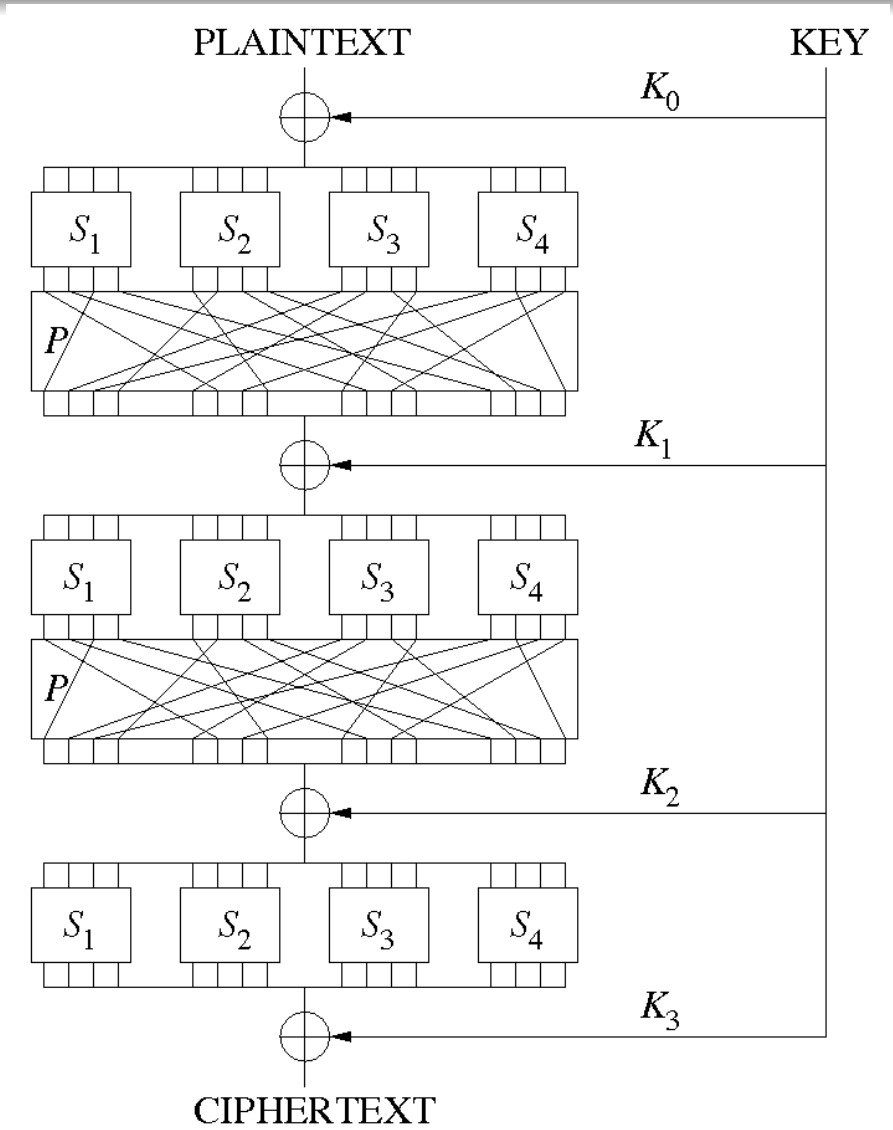
système de chiffrement retenu en 2000 par le NIST (*National Institude of Standards and Tecnology)*

AES conçu à partir de l'algorithme Rijndael des belges Joan Daemen et Vincent Rijmen.

l'AES est un chiffrement de type réseau de substitutions-permutations qui opère sur des blocs de 128 bits.

Les clés peuvent être de 128, 192 ou 256 bits.

Réseau de substitutions-permutations - SPN

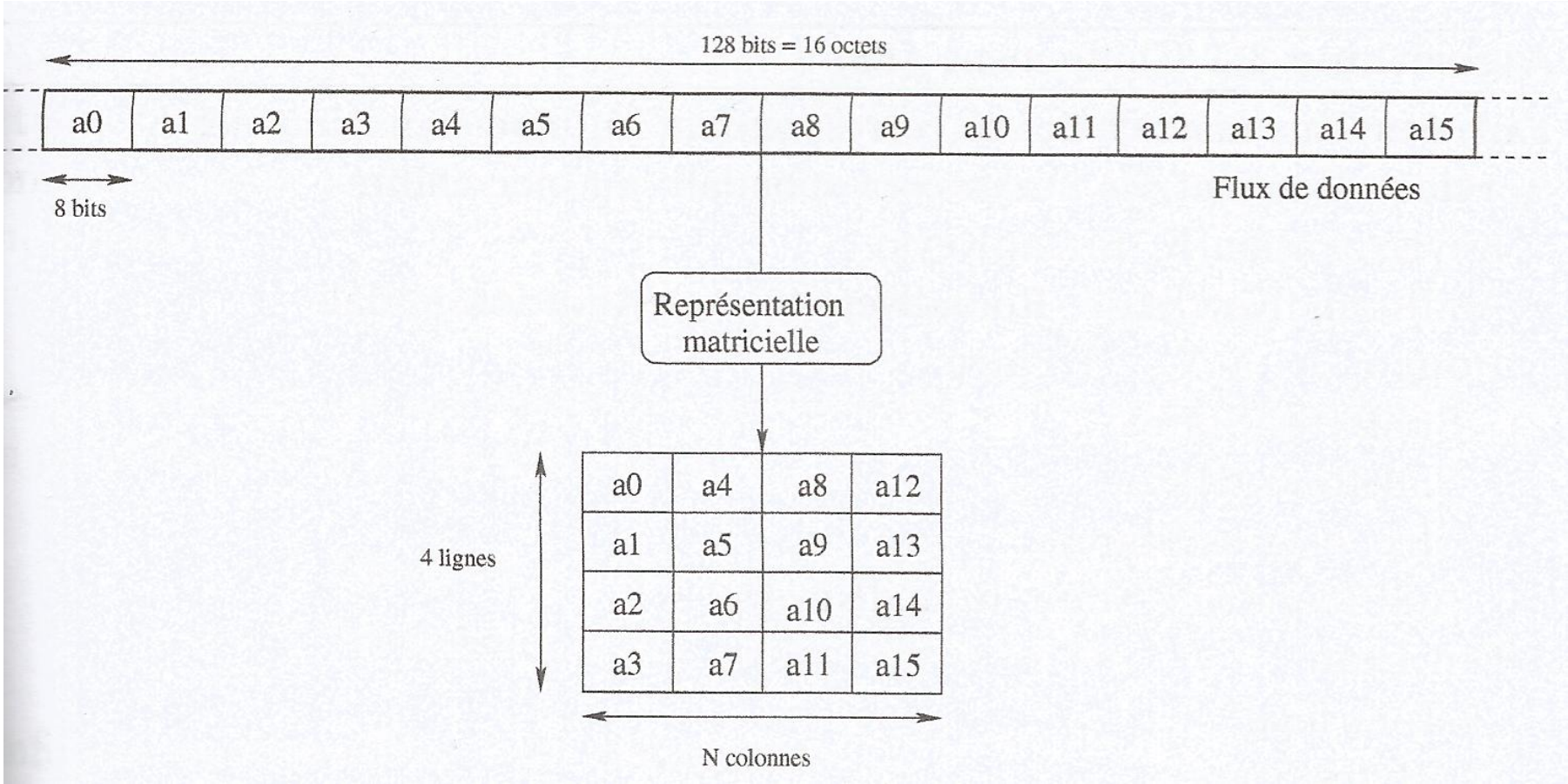


Sbox/PBox : confusion / diffusion

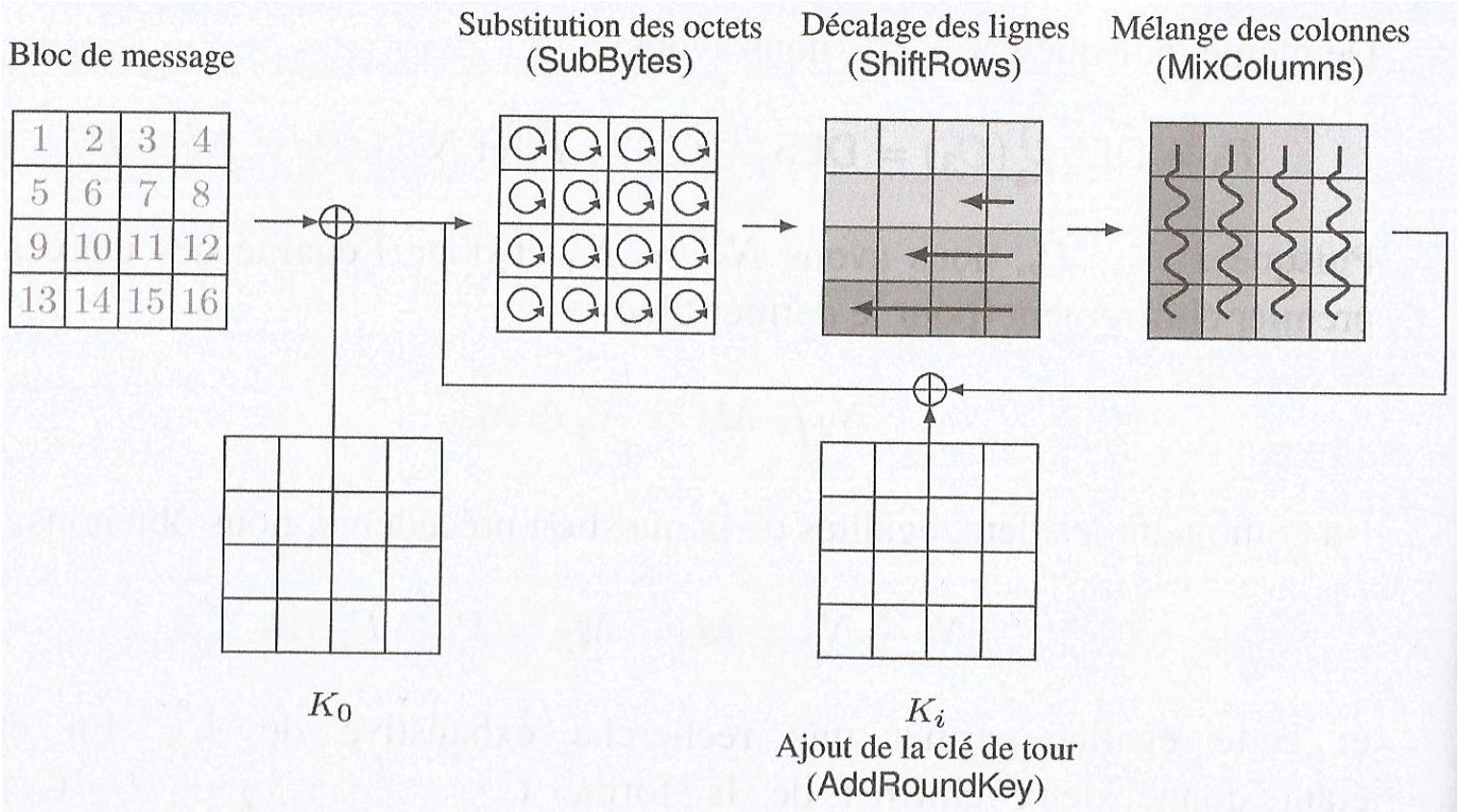
Chiffrement AES

Le chiffrement découpe les blocs de 128 bits en 16 octets.

Les blocs sont représentés sous la forme d'une matrice carrée 4×4 où les octets sont numérotés de 1 à 16.

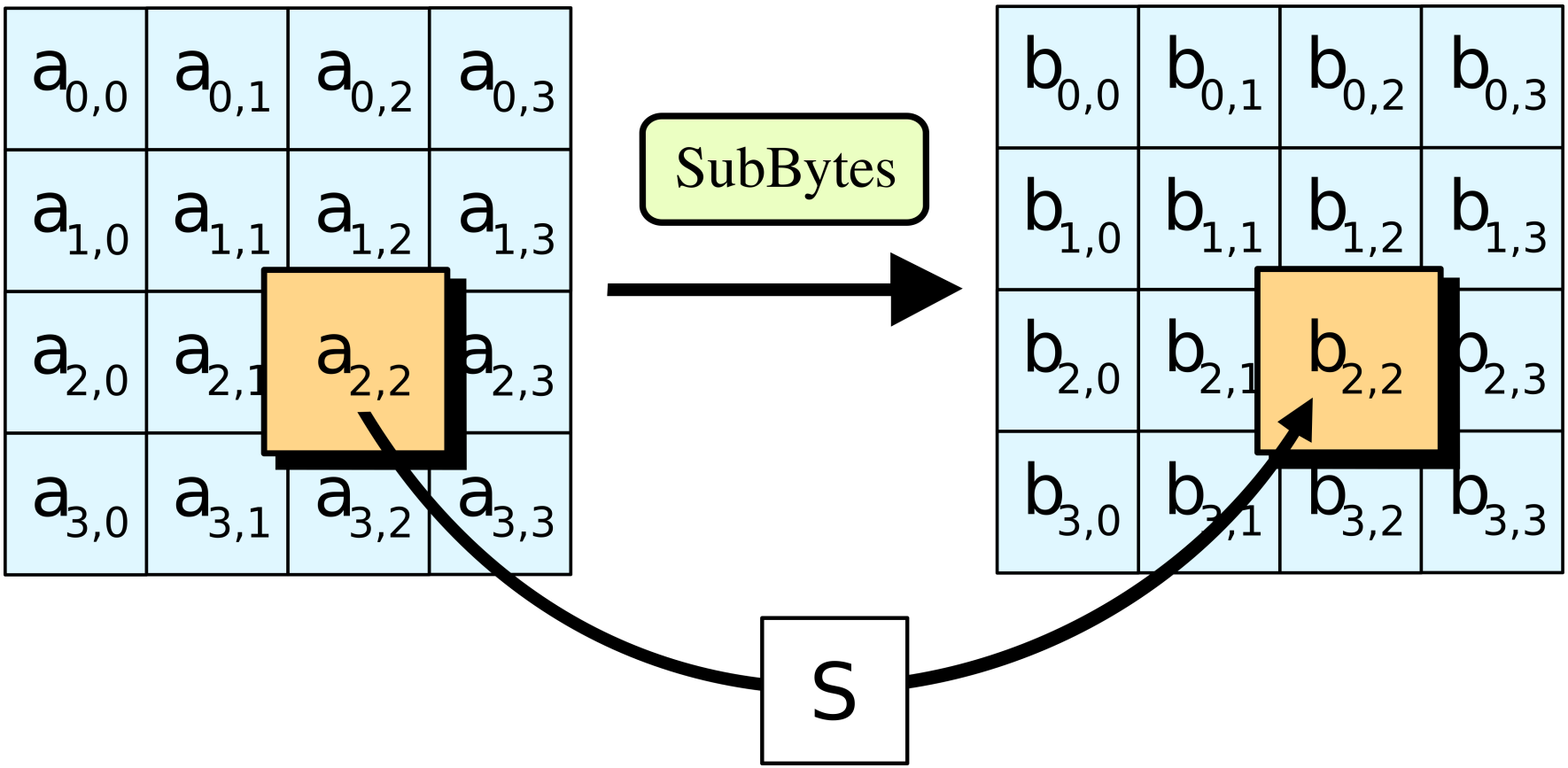


Chiffrement AES



Le nombre de tours dépend de la taille de la clé.
clé de 128 bits/10 tours - 192 bits/12 tours - 256 bits/14 tours
La procédure `MixColumns` est omise lors du dernier tour.

Chiffrement AES - SubBytes



Chiffrement AES - 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

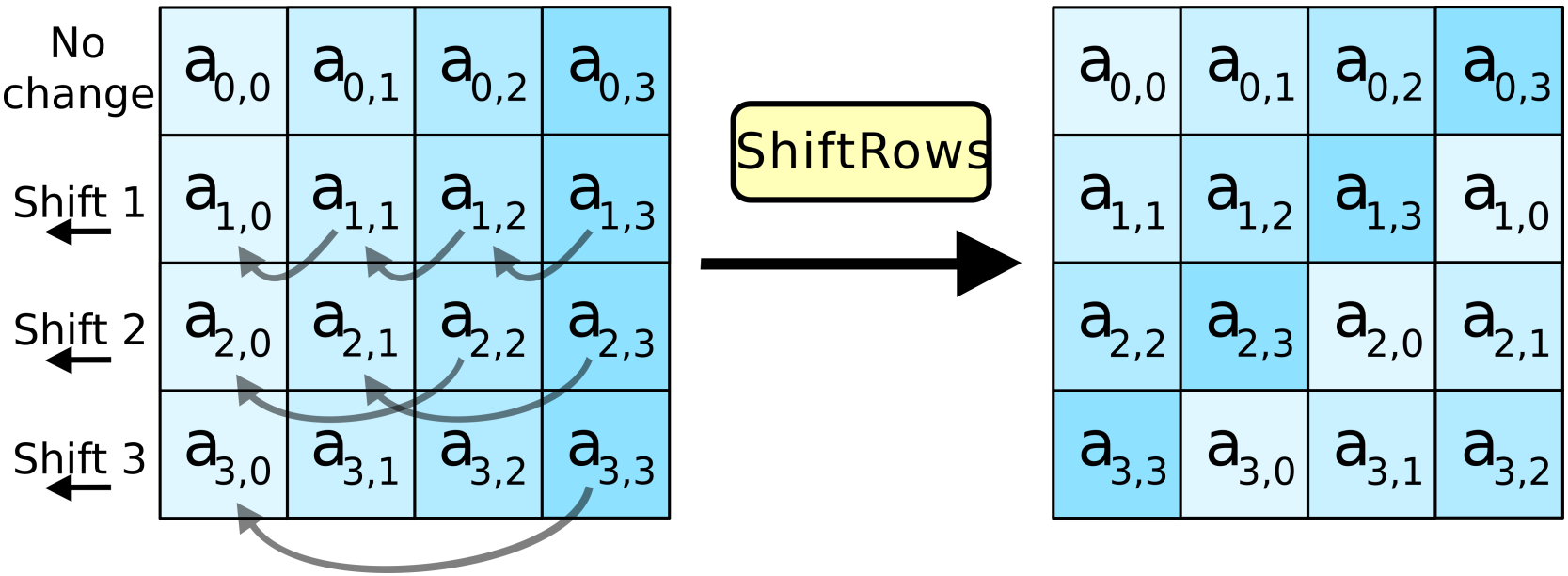
Chiffrement AES - SBox

SBox conçue mathématiquement pour avoir de bonnes propriétés.

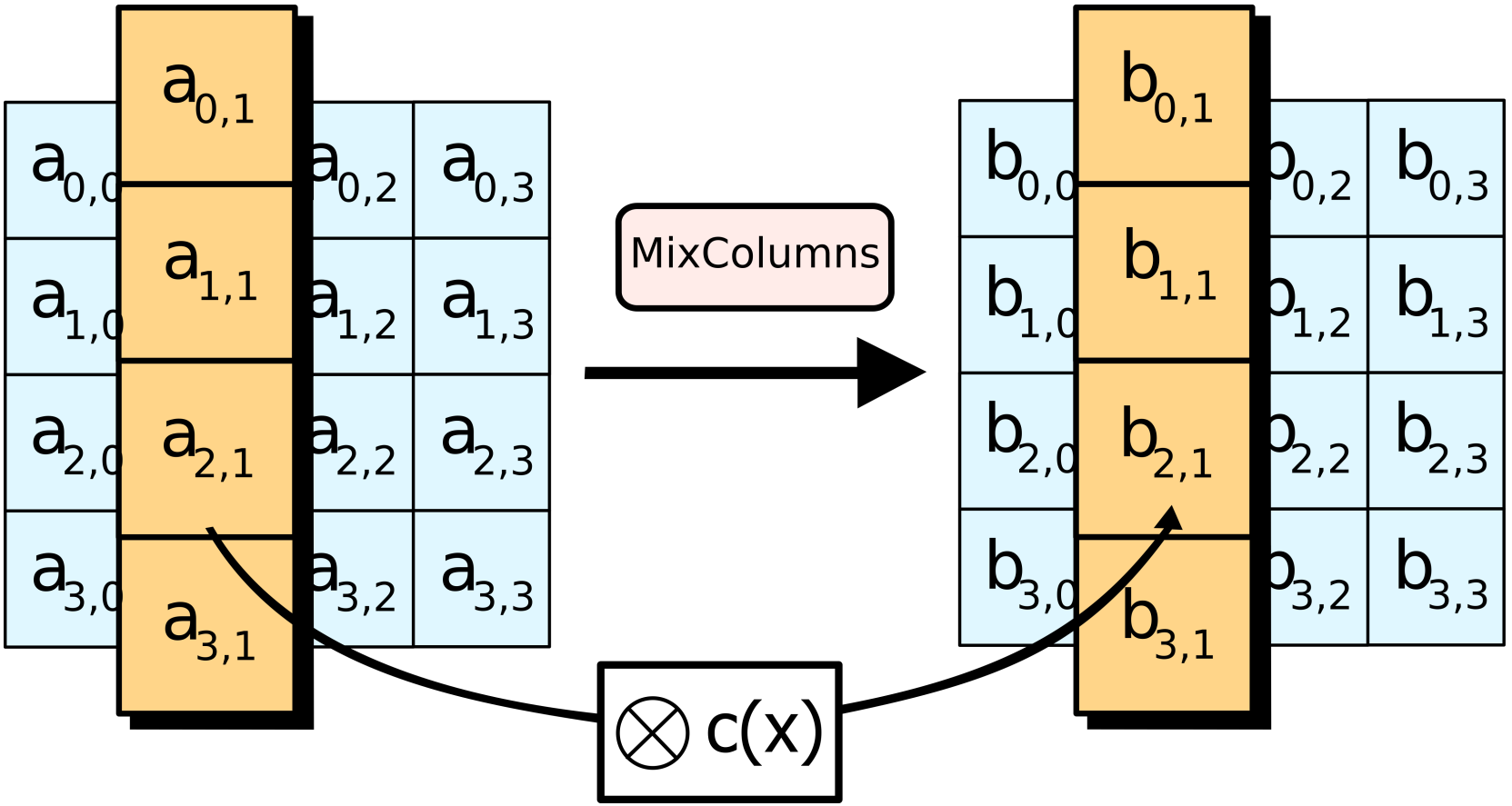
Pour effectuer ces différentes opérations, chaque octet est vu comme un polynôme de degré 7 dans le corps fini $\mathbb{F}_{2^8}$ où

- l'addition de deux polynômes correspond à l'opération ou exclusif sur les octets: addition terme à terme des coefficients dans $\mathbb{Z}/2\mathbb{Z}$
- la multiplication est la multiplication des polynômes modulo le polynôme irréductible $m(x) = x^8 + x^4 + x^3 + x + 1$

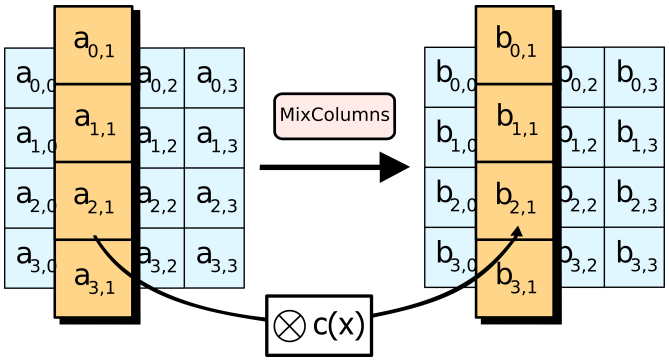
Chiffrement AES - ShiftRows



Chiffrement AES - MixColumns



Chiffrement AES - MixColumns



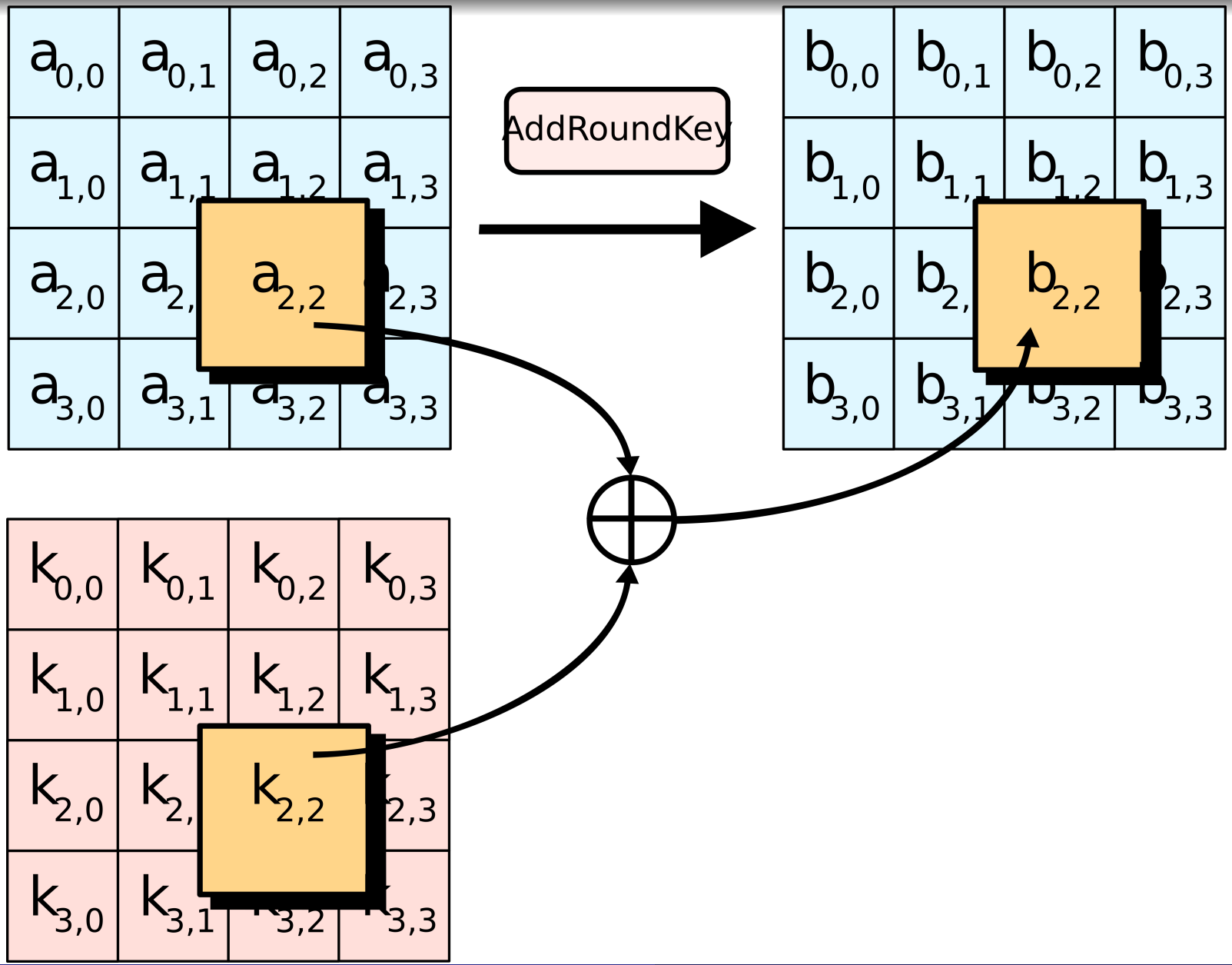
Chaque colonne est vue comme un polynôme a(X) de degré 3 à coefficients dans $\mathbb{F}_{2^8}$

Chaque colonne est multipliée par le polynôme
$c(X) = 03X^3 + X^2 + X + 02$ modulo le polynôme $X^4 + 1$

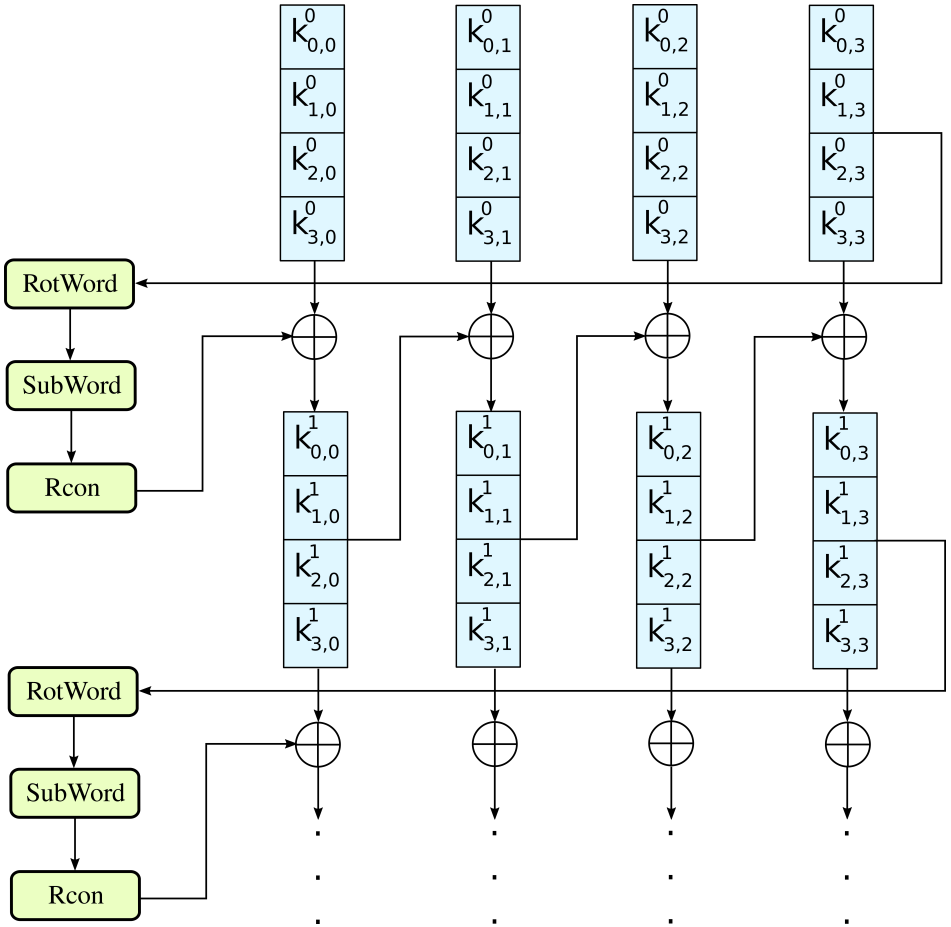
Ceci s'écrit matriciellement:

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \qquad 0 \leq j \leq 3$$

Chiffrement AES - AddRoundKey



Chiffrement AES - Diversification de clé - *key schedule*



Chiffrement AES - Sécurité

Sbox conçue pour être résistante à la cryptanalyse linéaire et différentielle.

ShiftRows + MixColumns: diffusion

2^{128} ou 2^{192} ou 2^{256} clés: brute force irréaliste

Attaques sur des nombres de tours inférieurs à ceux recommandés

Attaques exploitant les faiblesses du système qui implémente l'algorithme de chiffrement