AES

Peter Seibt, Andreea Dragut Cours de cryptographie Chapitre V

5.1 L'arithmétique des corps de restes $\mathbb{F}_2[x]/(p(x))$

5.1.1 Anneaux des polynômes à coefficients dans $\mathbb{F}_2$

Soit $\mathbb{F}_2[x]$ l'anneau des polynômes à coefficients dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Il est un anneau euclidien (on dispose de l'algorithme de division euclidienne), tout comme $\mathbb{Z}$, l'anneau des entiers. Dans cet anneau les polynômes irréductibles se ressemblent aux "nombres premiers" dans $\mathbb{F}_2[x]$.

Definition. *$p(x)$ est un polynôme* **irréductible** $\iff$ *$p(x)$ n'a pas de diviseur nontrivial (c.àd. 1 et $p(x)$ sont les seuls diviseurs de $p(x)$).*

Exemple. *Trouvez les polynômes irréductibles de degré ≤ 4.*

(1) degré 1 : x, $x+1$.

(2) degré 2 : $x^2 + x + 1$

(noter que $x^2 + 1 = (x+1)^2$, puisque $1 + 1 = 0$)

(3) degré 3 : $x^3 + x + 1$, $x^3 + x^2 + 1$

(un polynôme de degré 3 est irréductible $\iff$ il n'admet ni 0 ni 1 comme racine.)

(4) degré 4 : $x^4 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$

(l'absence d'un facteur linéaire et un nombre impair de termes additifs ne sont plus suffisants pour décrire un polynôme irreductible : $(x^2 + x + 1)^2 = x^4 + x^2 + 1$).

Exercice. *Montrer que $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, $m(x) = x^8 + x^4 + x^3 + x + 1$ sont des polynômes binaires irréductibles.*

Il faut tester par division euclidienne si $p(x)$ est divisible par les polynômes irréductibles de degré plus petit.

5.1.2 Anneaux de restes $\mathbb{F}_2[x]/(p(x))$.

Soit $p(x) = x^n + \beta_{n-1}x^{n-1} + \ldots \beta_1 x + \beta_0 \ \in \mathbb{F}_2[x]$ un polynôme fixe. Dans l'anneau des restes modulo $p(x)$, noté avec $\mathbb{F}_2[x]/(p(x))$, les operations se font selon les règles suivantes :

- L'addition des restes s'effectue "coefficient par coefficient", en respectant $1 + 1 = 0$.

- La multiplication des restes se fait en deux temps :
  - . Multiplication des restes en tant que polynômes binaires
  - . Réduction du résultat à un reste (un polynôme de degré $< n$), selon la règle de réduction $x^n = \beta_{n-1}x^{n-1} + \ldots \beta_1 x + \beta_0$

L'arithmétique du corps de restes $\mathbb{F}_2[x]/(x^4 + x + 1)$.

Exemple. *Soit $p(x) = x^4 + x + 1$ un polynôme irréductible. $\mathbb{F}_2[x]/(x^4 + x + 1) = ?$*

$\mathbb{F}_2[x]/(x^4+x+1) = \{ [0] , \ [1] , \ [x] , \ [x+1] , \ [x^2] , \ [x^2+1] , \ [x^2+x] , \ [x^2+x+1], [x^3] , \ [x^3 + 1] , \ [x^3 + x] , \ [x^3 + x + 1] , \ [x^3 + x^2] , \ [x^3 + x^2 + 1] , \ [x^3 + x^2 + x] , [x^3 + x^2 + x + 1]\}$.

L'addition des restes est similaire à **ou exclusif XOR**, bit par bit :

$$[x^3 + 1] + [x^3 + x^2 + 1] = [x^2], \ 1001 \quad \oplus \quad 1101 = \quad 0100$$

La multiplication des restes :

$$[x^3 + x + 1] \cdot [x^3 + x^2] = [x^6 + x^5 + x^4 + x^2]$$

La division d'un polynôme par $x^4 + x + 1$:

$$\begin{array}{l} x^6 + x^5 + x^4 \qquad + x^2 : (x^4 + x + 1) = x^2 + x + 1 \\ \underline{x^6 \qquad\quad + x^3 + x^2} \\ \quad x^5 + x^4 + x^3 \\ \quad \underline{x^5 \qquad\quad + x^2 + x} \\ \qquad x^4 + x^3 + x^2 + x \\ \qquad \underline{x^4 \qquad\quad + x + 1} \\ \qquad\quad x^3 + x^2 \qquad + 1 \end{array}$$

Donc :

$$[x^3 + x + 1] \cdot [x^3 + x^2] = [x^3 + x^2 + 1]$$

On peut éviter des divisions euclidiennes dans le calcul des produits en réduisant succesivement à l'aide de la relation :

$$[x^4] = [x+1] \Leftrightarrow [x^4 + x + 1] = [0]$$

Pour la simplicité on abandonne la notation en crochets et on remplace l'équivalence par égalité $x^4 = x + 1$. On dérive aussi $x^5 = x^2 + x$, $x^6 = x^3 + x^2$ et on obtient à nouveau

$$x^6 + x^5 + x^4 + x^2 = (x^3 + x^2) + (x^2 + x) + (x + 1) + x^2 = x^3 + x^2 + 1$$

.

Exercice. *Soit $p(x)$ de degré n, alors $\mathbb{F}_2[x]/(p(x))$ admet 2^n éléments*

Un reste de division a le degré $< n$, et donc au plus $a_0, \ldots, a_{n-1}$ coefficients non-nuls. Comme les coefficients sont dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = 0, 1$, il y a 2^n restes distincts de la division par $p(x)$.

Le polynôme irreductible $p(x)$ est pour $\mathbb{F}_2[x]/(p(x))$ comme p premier pour $\mathbb{Z}/p\mathbb{Z}$.

Proposition. *L'anneau de restes $\mathbb{F}_2[x]/(p(x))$ est un corps si et seulement si $p(x)$ est un polynôme irréductible.*

Comme dans le cas des entiers, la preuve utilise l'équivalence : $[a(x)]$ est inversible dans l'anneau $\mathbb{F}_2[x]/(p(x)) \iff pgcd(a(x), p(x)) = 1$.

Proposition. *Soit donc $p(x) = x^n + \cdots + 1$ un polynôme irréductible de degré n. Alors le groupe multiplicatif $G = (\mathbb{F}_2[x]/(p(x)))^*$ est un groupe cyclique d'ordre $2^n - 1$. Si $\omega = x$ est un générateur de ce groupe, alors on dit que le polynôme irréductible $p(x)$ est primitif.*

Notation : Soit $p(x)$ est un polynôme binaire irréductible de degré n. Comme tous les corps à 2^n éléments sont **isomorphes** $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(p(x))$

Exercice. *Les polynômes (binaires) suivants sont irréductibles et primitifs :*

- $x^2 + x + 1$
- $x^3 + x + 1$
- $x^4 + x + 1$
- $x^5 + x^2 + 1$
- $x^6 + x + 1$
- $x^7 + x^3 + 1$
- $x^8 + x^4 + x^3 + x^2 + 1$

Notation : $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$

$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$

$\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$

$\mathbb{F}_{64} = \mathbb{F}_2[x]/(x^6 + x + 1)$

$\mathbb{F}_{256} = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x^2 + 1)$

Exercice. *Vérifiez que le groupe multiplicatif de* $\mathbb{F}_2[x]/(x^4 + x + 1)$ *est un groupe cyclique en calculant les puissances successives de* $\omega = x$ *dans* $\mathbb{F}_2[x]/(x^4 + x + 1)$.

$\omega = x$, $\omega^2 = x^2$, $\omega^3 = x^3$

$\omega^4 = x + 1$, $\omega^5 = x^2 + x$, $\omega^6 = x^3 + x^2$

$\omega^7 = x^3 + x + 1$, $\omega^8 = x^2 + 1$, $\omega^9 = x^3 + x$

$\omega^{10} = x^2 + x + 1$, $\omega^{11} = x^3 + x^2 + x$, $\omega^{12} = x^3 + x^2 + x + 1$

$\omega^{13} = x^3 + x^2 + 1$, $\omega^{14} = x^3 + 1$, $\omega^{15} = 1$

Les puissances de $\omega = x$ génèrent tous les 15 restes nonnuls dans $\mathbb{F}_2[x]/(x^4 + x + 1)$.

Exercice. $\mathbb{F}_2[x]/(x^4 + x + 1)$ *est un corps (à 16 éléments), donc chaque reste nonnul admet un inverse multiplicatif. Calculez* $(x^3 + x^2)^{-1}$ *à l'aide du Th. petit de Fermat. Vérifiez le resultat avec l'algorithme d'Euclide étendu.*

$(x^3 + x^2)^{-1} = (\omega^6)^{-1} = \omega^{-6} = \omega^9 = x^3 + x.$

L'arithmétique du corps de restes AES $\mathbb{R}_{256} = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$.

On considère les octets binaires comme des restes de division, selon le schéma :

$$00100111 = x^5 + x^2 + x + 1.$$

Le polynôme AES $m(x) = (x^8 + x^4 + x^3 + x + 1)$ est irréductible et l'anneau de restes $\mathbb{F}_2[x]/(m(x))$ est un corps. Le groupe multiplicatif est un groupe cyclique d'ordre $255 = 2^8 - 1$, $(\mathbb{F}_2[x]/(m(x)))^* = \mathbf{R}_{256}$. La liste des 255 restes nonnuls dans $\mathbf{R}_{256}$, en fonction des puissances successives de $\xi = x + 1$ se trouve dans l'annexe.

Exercice. $\mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$ *est un corps (à* $256 = 2^8$ *éléments), donc chaque reste nonnul admet un inverse multiplicatif. Calculez* $(x^7 + x^6 + x^3 + x + 1)^{-1}$ *avec l'algorithme d'Euclide étendu et aussi en uitilisant la structure cyclique de* $\mathbf{R}_{256}$ *et le Petit Th. de Fermat.*

Utilisant l'algorithme d'Euclide :

$$(x^8 + x^4 + x^3 + x + 1) = (x + 1)(x^7 + x^6 + x^3 + x + 1) + \boxed{x^6 + x^2 + x}$$
$$(x^7 + x^6 + x^3 + x + 1) = (x + 1)(x^6 + x^2 + x) + 1$$

$$1 = (x^7 + x^6 + x^3 + x + 1) + (x + 1)\boxed{(x^6 + x^2 + x)} \tag{5.1.1}$$
$$1 = (x^7 + x^6 + x^3 + x + 1) + (x + 1)[(x^8 + x^4 + x^3 + x + 1) + (x + 1)(x^7 + x^6 + x^3 + x + 1)] \tag{5.1.2}$$
$$1 = [1 + (x + 1)(x + 1)] \cdot (x^7 + x^6 + x^3 + x + 1) + (x + 1)(x^8 + x^4 + x^3 + x + 1)] \tag{5.1.3}$$
$$1 = x^2(x^7 + x^6 + x^3 + x + 1) + (x + 1)(x^8 + x^4 + x^3 + x + 1)], \tag{5.1.4}$$

On réduit modulo $(x^8 + x^4 + x^3 + x + 1)$ et alors l'inverse recherché est x^2.

$$x^2(x^7 + x^6 + x^3 + x + 1) \equiv 1 \pmod{(x^8 + x^4 + x^3 + x + 1)}$$

.

Utilisant la structure cyclique + Petit Th. Fermat :

Comme $(\mathbb{F}_2[x]/(m(x)))^* = \mathbf{R}_{256}$ est un groupe cyclique genéré par $\xi = x + 1$ tout polynôme est une puissance de $\xi = x + 1$. En utilisant la liste de puissances successives de $\xi = x + 1$ qui se trouve dans l'annexe :

$$(x^7 + x^6 + x^3 + x + 1) = \xi^{205}$$

On sait que

$$\xi^{255} = 1$$

donc

$$1 = \xi^{205} \cdot \xi^{55} = (x^7 + x^6 + x^3 + x + 1) \cdot \xi^{55}$$

Selon la définition de l'inverse $(x^7 + x^6 + x^3 + x + 1)^{-1} = \xi^{55} = x^2$.

Remarque. *Comment peut-on implementer rapidement la multiplication de* $\mathbb{R}_{256}$ *?*

En utilisant l'addition XOR (ou exclusif) de bits $(x^7 + x^6 + x^3 + x + 1)x = 11001011$ (shift gauche et rajout de $0 \Rightarrow 110010110 \Rightarrow 110010110$ XOR 100011011 (soustraire $x^8 + x^4 + x^3 + x + 1$ si le premier bit est 1)=010001101

Proposition. *Le polynôme irréductible* $m(x) = x^8 + x^4 + x^3 + x + 1$ *n'est pas primitif, donc même si le sous-groupe multiplicatif* $\mathbf{R}_{256}^* = \mathbb{F}_2[x]/(m(x))^*$ *est cyclique, ordre(x)=51. Mais ordre*$(x + 1)$*=255.*

Exercice. $\mathbf{R}_{256} = \mathbb{F}_2[x]/(m(x))$ *est un corps (à 256 éléments), donc chaque reste nonnul admet un inverse multiplicatif. Calculez dans* $\mathbf{R}_{256} = \mathbb{F}_2[x]/(m(x))$ *les inverses multiplicatifs suivants de* 11101010^{-1} *,* 01010101^{-1}*,* 11111111^{-1} *à l'aide du Th. petit de Fermat.*

5.2 L'algorithme de chiffrement AES - Rijndael.

5.2.1 Généralités.

AES chiffre un bloc de texte clair de 128 bits (16 octets binaires) en un bloc chiffré de 128 bits (16 octets binaires). Nous considérons que la version d'AES-128 où les clés des utilisateurs ont 128 bits.

Le bloc de texte clair subit alors 10 itérations d'une transformation qui dépend, à chaque tour, d'une autre clé de tour déduite de la clé de chiffrement de l'utilisateur.

Noter que la clé de tour $K_i, \quad 0 \leq i \leq 10$ aura 128 bits, c.àd. elle aura le même format que le bloc texte en cours de chiffrement.

Les clés de tour sont fournies par un algorithme auxiliaire à partir de la clé de chiffrement de l'utilisateur.

5.2.2 L'arithméthique du système AES - Rijndael

(a)Les octets binaires.

Notation syntaxique : 10100111
Notation hexadécimale : $\{a7\} \quad (\ 1010 \equiv a \quad 0111 \equiv 7\ )$
Notation polynômiale : $x^7+x^5+x^2+x+1$ dans le corps $\mathbf{R}_{256} = \mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$, c.àd. un reste de division par $m(x) = x^8 + x^4 + x^3 + x + 1$.
Donc une suite de 8 bits est considéré en étant à la fois un octet et un polynôme :

$$\beta_7\beta_6 \ldots \beta_1\beta_0 = \{(\beta_7 \ldots \beta_4)_{16}(\beta_3 \ldots \beta_0)_{16}\} = \beta_7 x^7 + \beta_6 x^6 + \cdots + \beta_1 x + \beta_0$$

(b)Présentation externe et présentation interne d'un bloc de 128 bits

La présentation externe des 128 bits du bloc de texte clair (et du bloc chiffré) est séquentielle :

$$\beta_0\beta_1\beta_2 \quad \ldots \quad \beta_{127} \quad \equiv \quad a_0a_1a_2 \quad \ldots \quad a_{15}$$

avec les relations suivantes

$$\begin{gathered} a_0 = \beta_0\beta_1 \ldots \beta_7 \\ a_1 = \beta_8\beta_9 \ldots \beta_{15} \\ \vdots \\ a_{15} = \beta_{120}\beta_{121} \ldots \beta_{127} \end{gathered}$$

Remarque. *Chaque octet aura la numérotation décroissante des positions :* $7, 6, 5, 4, 3, 2, 1, 0$.

La présentation interne des 128 bits du bloc texte en clair(ou du bloc chiffré en cours de déchiffrement) est **matricielle**. On l'appelle **état** du système, en anglais "state array".

$$\begin{pmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{pmatrix} = \begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}$$

Chaque état est un quadruplet de 4 octets "verticaux" chacun :

$$w_0 = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} s_{0,0} \\ s_{1,0} \\ s_{2,0} \\ s_{3,0} \end{pmatrix} \qquad w_1 = \begin{pmatrix} a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = \begin{pmatrix} s_{0,1} \\ s_{1,1} \\ s_{2,1} \\ s_{3,1} \end{pmatrix}$$

$$w_2 = \begin{pmatrix} a_8 \\ a_9 \\ a_{10} \\ a_{11} \end{pmatrix} = \begin{pmatrix} s_{0,2} \\ s_{1,2} \\ s_{2,2} \\ s_{3,2} \end{pmatrix} \qquad w_3 = \begin{pmatrix} a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \end{pmatrix} = \begin{pmatrix} s_{0,3} \\ s_{1,3} \\ s_{2,3} \\ s_{3,3} \end{pmatrix}$$

5.2.3 L'algorithme de chiffrement AES

Tour $n°0$: Addition de $K_0 \equiv$ la clé de l'utilisateur (en écriture d'état) à l'état initial du texte clair (OU EXCLUSIF, bit par bit).

Tour $n°1$: Il y a quatre étapes :

- La boîte - S de substitution octet par octet (SubBytes) : Les 16 octets de l'état sont traités indépendamment, c.àd. en parallèle par 16 d'une boîtes - S identiques
- La rotation des lignes de l'état (ShiftRows :) : Décalage cyclique à gauche des 4 lignes de l'état, de
  0, 1, 2, 3 positions respectivement.
- Mélange sur les colonnes de l'état ou filtrage arithmétique (MixColumns) : Les 4 colonnes de l'état subissent simultanément une convolution circulaire (sur $\mathbf{R}_{256}$).
- Addition de la clé de tour (AddRoundKey) : la clé de tour s'additionne à l'état (addition de deux matrices 4×4 sur $\mathbf{R}_{256}$).

Tour $n°2$: Comme le tour $n°1$.

$\vdots$

Tour $n°9$: Comme le tour $n°1$.

Tour $n°10$: Seulement trois étapes : On se passe du filtrage des colonnes de l'état.

AES n'est pas un réseau de Feistel et le déchiffrement utilise une méthode différente du chiffrement. Pour chaque fonction de tour on peut calculer la fonction inverse nécessaire dans le processus de décryptage.

L'étape de substitution rajoute de la confusion dans le chiffrement. La confusion sert à rendre la relation entre la clef et le chiffré aussi complexe que possible.

Les étapes de permutation dans un tour AES rajoutent de la diffusion dans le chiffrement. Le but est d'étaler les propriétés de redondance du texte clair sur tout le chiffré.

5.3 Example AES

Chaque chiffre hexa correspond à quatre chiffres binaires ainsi :

0	0000	2	0010	4	0100	6	0110	8	1000	a	1010	c	1100	e	1110
1	0001	3	0011	5	0101	7	0111	9	1001	b	1011	d	1101	f	1111

Exemple (Chiffrement AES)**.**

- *Le texte clair : 4a a3 3c 69 4f 4f 3b ad 59 7f f3 d9 ec e8 32 0c.*
- *La clé de chiffrement : 43 c6 84 53 33 25 0c 80 1d 2b c3 97 e2 cc 40 b3.*
- *Trouver l'état initial du deuxième tour.*

D'abord le tour $n°0$:

4a	4f	59	ec		43	33	1d	e2		09	7c	44	0e
a3	4f	7f	e8	$\oplus$	c6	25	2b	cc	=	65	6a	54	24
3c	3b	f3	32		84	0c	c3	40		b8	37	30	72
69	ad	d9	0c		53	80	97	b3		3a	2d	4e	bf

Maintenant le tour $n°1$:

5.3.1 La boîte - S :SubBytes

La boîte - S est la composante non-linéaire de la transformation d'un tour. Elle est basée sur opérations dans le corps Rijndael $\mathbb{R}_{2^8} = R_{256} = \mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$.

Il y a 16 boîtes - S identiques qui opèrent en parallèle.

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \Longrightarrow \begin{pmatrix} b'_0 & b'_1 & b'_2 & b'_3 \\ b'_4 & b'_5 & b'_6 & b'_7 \\ b'_8 & b'_9 & b'_{10} & b'_{11} \\ b'_{12} & b'_{13} & b'_{14} & b'_{15} \end{pmatrix} \Longrightarrow \begin{pmatrix} b_0 & b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 & b_7 \\ b_8 & b_9 & b_{10} & b_{11} \\ b_{12} & b_{13} & b_{14} & b_{15} \end{pmatrix}$$

Substitution Octet par Octet (SubBytes) :

$$S(a) = \text{Transf Affine}(\text{Inverse}(a))$$

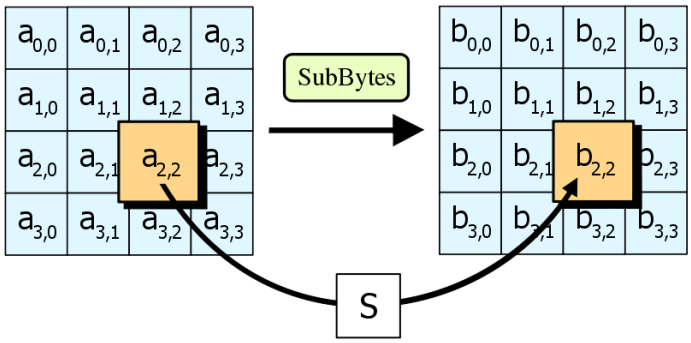

FIGURE 5.1 – AES-SubBytes

[Premier pas] : Trouver l'inverse multiplicatif dans $\mathbb{F}_2$ mod $m(x) = x^8+x^4+x^3+x+1$

[Deuxième pas] : Appliquer unr transformation affine dans $(\mathbb{F}_2)^8 = \{0,1\}^8$

La complexité de la boîte - S est équivalente à la complexité de l'opération d'inversion multiplicative dans $\mathbf{R}_{256} = \mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$; la transformation affine "superposée" a seulement la fonction de créer une transformation booléenne **sans points fixes**.

09	7c	44	0e
65	6a	54	24
b8	37	30	72
3a	2d	4e	bf

$\Rightarrow$

S(09)	S(7c)	S(44)	S(0e)
S(65)	S(6a)	S(54)	S(24)
S(b8)	S(37)	S(30)	S(72)
S(3a)	S(2d)	S(4e)	S(bf)

$=$

01	10	1b	ab
4d	02	20	36
6c	9a	04	40
80	d8	2f	08

[Premier pas] : Trouver l'inverse multiplicatif mod $m(x) = x^8 + x^4 + x^3 + x + 1$

Exercice. *Calcul de* $(bf)^{-1}$ *mod* $m(x) = x^8+x^4+x^3+x+1$ *dans* $\mathbb{F}_2[x]/m(x)$ *avec l'algorithme d'Euclide étendu et aussi en utilisant la structure cyclique de* $\mathbf{R}_{256}$ *et le Petit Th. de Fermat.*

Utilisant l'algorithme d'Euclide : On note avec $p(x) = (x^7 + x^5 + x^4 + x^3 + x^2 + x + 1)$.

$$\underline{(x^8 + x^4 + x^3 + x + 1)} = x\underline{(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1)} + \boxed{x^6 + x^5 + x^2 + 1}$$

$$\underline{(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1)} = (x + 1)\underline{(x^6 + x^5 + x^2 + 1)} + \boxed{x^4}$$

$$\underline{(x^6 + x^5 + x^2 + 1)} = (x^2 + x) \cdot \underline{x^4} + \boxed{x^2 + 1}$$

$$\underline{x^4} = (x^2 + 1) \cdot \underline{(x^2 + 1)} + \boxed{1}$$

$$1 = \underline{x^4} + (x^2 + 1)\boxed{(x^2 + 1)} \tag{5.3.5}$$

$$1 = \underline{x^4} + (x^2 + 1)[\underline{(x^6 + x^5 + x^2 + 1)} + (x^2 + x)\underline{x^4}] \tag{5.3.6}$$

$$1 = [1 + (x^2 + 1)(x^2 + x)] \cdot \underline{x^4} + (x^2 + 1)\underline{(x^6 + x^5 + x^2 + 1)} \tag{5.3.7}$$

$$1 = \boxed{x^4}(x^4 + x^3 + x^2 + x + 1) + (x^2 + 1)\underline{(x^6 + x^5 + x^2 + 1)}, \tag{5.3.8}$$

$$1 = (x^2 + 1)\underline{(x^6 + x^5 + x^2 + 1)} + (x^4 + x^3 + x^2 + x + 1)[\underline{p(x)} + (x + 1)\underline{(x^6 + x^5 + x^2 + 1)}] \tag{5.3.9}$$

$$1 = [(x^2 + 1) + (x^4 + x^3 + x^2 + x + 1)(x + 1)]\underline{(x^6 + x^5 + x^2 + 1)} + (x^4 + x^3 + x^2 + x + 1)\underline{p(x)} \tag{5.3.10}$$

$$1 = (x^2 + x^5)\boxed{(x^6 + x^5 + x^2 + 1)} + (x^4 + x^3 + x^2 + x + 1)\underline{p(x)} \tag{5.3.11}$$

$$1 = (x^2 + x^5)[\underline{m(x)} + x \cdot \underline{p(x)}] + (x^4 + x^3 + x^2 + x + 1)\underline{p(x)} \tag{5.3.12}$$

$$1 = (x^2 + x^5)\underline{m(x)} + (x^6 + x^4 + x^2 + x + 1)\underline{p(x)}, \tag{5.3.13}$$

On réduit modulo $(x^8+x^4+x^3+x+1)$ et alors l'inverse recherché est $x^6+x^4+x^2+x+1 = 57$.

$$(x^6 + x^4 + x^2 + x + 1)(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1) \equiv 1 \pmod{(x^8 + x^4 + x^3 + x + 1)}.$$

Utilisant la structure cyclique + Petit Th. Fermat :
Comme $(\mathbb{F}_2[x]/(m(x)))^* = \mathbf{R}_{256}$ est un groupe cyclique genéré par $\xi = x + 1$ tout polynôme est une puissance de $\xi = x + 1$. En utilisant la liste de puissances successives de $\xi = x + 1$ qui se trouve dans l'annexe :

$$(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1) = \xi^{157}$$

On sait que

$$\xi^{255} = 1$$

donc

$$1 = \xi^{157} \cdot \xi^{98} = (x^7 + x^5 + x^4 + x^3 + x^2 + x + 1) \cdot \xi^{98}$$

Selon la définition de l'inverse $(x^7{+}x^5{+}x^4{+}x^3{+}x^2{+}x{+}1)^{-1} = \xi^{98} = (x^6{+}x^4{+}x^2{+}x{+}1) = 57$.

La table AES de l'inverse multiplicatif mod $m(x) = x^8 + x^4 + x^3 + x + 1$ dans $\mathbb{F}_2[x]/m(x)$ nous confirme :

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

[Deuxième pas] : Transformation affine

Soit un élément b' de l'état du système après avoir pris l'inverse modulo $m(x)$:

$$b' = \beta'_7\beta'_6 \dots \beta'_0, \text{ c.à-d. } b'(x) = \beta'_7 x^7 + \beta'_6 x^6 + \cdots + \beta'_0.$$

Le résultat du premier pas, b' subit une transformation affine de l'espace $(\mathbb{F}_2)^8$ pour eliminer les points fixes de l'inverse multiplicatif : "00","01" :

$$(\beta'_0\beta'_1 \dots \beta'_7)^T \longmapsto A \times (\beta'_0\beta'_1 \dots \beta'_7)^T + c$$

où

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \text{ et } c = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Attention le vecteur b‘ est écrit comme un vecteur dans l'ordre inverse.

Exercice. *(Continuation d'AES Tour 1 SubBytes) Appliquez au résultat du premier pas,* $(bf)^{-1} = 57$ *la transformation affine de l'espace* $(\mathbb{F}_2)^8$ *indiqué par l'algorithme AES.*

Attention : $57_{16} = 01010111$ est écrit comme un vecteur dans l'ordre inverse :

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \longmapsto A \times \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + c$$

où A et c sont des constantes AES.

Alors :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Le résultat final $08_{16} = 00010000$.

Remarque (Implementation)**.** *Soit un élément b' de l'état du système après avoir pris l'inverse modulo $m(x)$:*

$$b' = \beta'_7\beta'_6 \dots \beta'_0, \text{ c.à-d. } b'(x) = \beta'_7 x^7 + \beta'_6 x^6 + \cdots + \beta'_0.$$

La description polynômiale de la transformation affine integré dans la boîte S est donnée par

$$b(x) = \beta_7 x^7 + \cdots + \beta_0 = [(\beta'_7 x^7 + \cdots + \beta'_0)(x^4 + x^3 + x^2 + x + 1) + x^6 + x^5 + x + 1] \bmod (x^8 + 1)$$

Une autre description de la transformation affine dans $(\mathbb{F}_2)^8 = \{0,1\}^8$ integré dans la boîte - S est donnée par :

$$\beta_k = \beta'_k \oplus \beta'_{k+4 \pmod 8} \oplus \beta'_{k+5 \pmod 8} \oplus \beta'_{k+6 \pmod 8} \oplus \beta'_{k+7 \pmod 8} \oplus c_k$$

où $c = 63_{16} = 01100011_2$ et k indique le bit numèro k des octets c, $b = \beta_7 \dots \beta_1\beta_0$ et respectivement $b' = \beta'_7 \dots \beta'_1\beta'_0$.

Exercice. *Vérifiez que $(09)^{-1} = 4f \ mod\, m(x) = x^8 + x^4 + x^3 + x + 1$ dans $\mathbb{F}_2[x]/m(x))$ avec l'algorithme d'Euclide étendu et aussi en utilisant la structure cyclique de $\mathbf{R}_{256}$ et le Petit Th. de Fermat. Vérifiez après que $S(09) = TransfAffine(4f) = 01$.*

Le résultat du premier pas $4f$ subit une transformation affine de l'espace $(\mathbb{F}_2)^8$ pour eliminer les points fixes de l'inverse multiplicatif : "00","01" :

$4f_{16} = 01001111$ est écrit comme un vecteur dans l'ordre inverse.

$$\begin{pmatrix}1\\1\\1\\1\\0\\0\\1\\0\end{pmatrix} \longmapsto A \times \begin{pmatrix}1\\1\\1\\1\\0\\0\\1\\0\end{pmatrix} + c$$

Alors :

$$\begin{pmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{pmatrix} \times \begin{pmatrix}1\\1\\1\\1\\0\\0\\1\\0\end{pmatrix} + \begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

Le résultat final est $01_{16} = 00000001$.
La valeur d'un octet uv après SubBytes s'obtient à l'aide du tableau de la boîte - S .

La boîte - S :

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

Remarque (Transformation affine inverse)**.** *L'étape SubBytes est inversible. L'inverse modulo $m(x)$ est inversible. La transformation* **inverse** *de la transformation affine ci-dessus est :*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

c.à-d.

$$\begin{pmatrix} \beta'_0 \\ \beta'_1 \\ \beta'_2 \\ \beta'_3 \\ \beta'_4 \\ \beta'_5 \\ \beta'_6 \\ \beta'_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \beta_0 + 1 \\ \beta_1 + 1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 + 1 \\ \beta_6 + 1 \\ \beta_7 \end{pmatrix}$$

La boîte - S **inverse** :

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

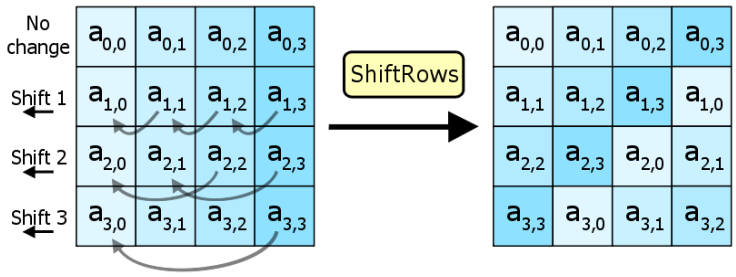

FIGURE 5.2 – AES-ShiftRows

5.3.2 ShiftRows : le décalage cyclique des lignes de l'état

La procédure consiste à opérer une rotation à gauche sur chaque ligne du tableau d'entrèèe. On décale la ligne i de i cases $\pmod 8$ à gauche. Ceci donne :

01	10	1b	ab
4d	02	20	36
6c	9a	04	40
80	d8	2f	08

$\longmapsto$

01	10	1b	ab
02	20	36	4d
04	40	6c	9a
08	80	d8	2f

La transformation inverse est immédiate à calculer.

5.3.3 MixColumns : Mélange sur les colonnes du "carré"

L'état d'AES aprés SubBytes est une matrice 4×4 sur le corps des octets $\mathbf{R}_{256}$. Le mélange sur les colonnes consiste à multiplier chaque colonne du tableau des données avec une matrice circulante $\mathbf{C}(x)$. On dit que la transformation algébrique associé à la matrice est un filtrage arithmétique.

$$\mathbf{C}(x) \times \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \longmapsto \begin{pmatrix} b_0 & b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 & b_7 \\ b_8 & b_9 & b_{10} & b_{11} \\ b_{12} & b_{13} & b_{14} & b_{15} \end{pmatrix}$$

où

$$\mathbf{C}(x) = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} = \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix}$$

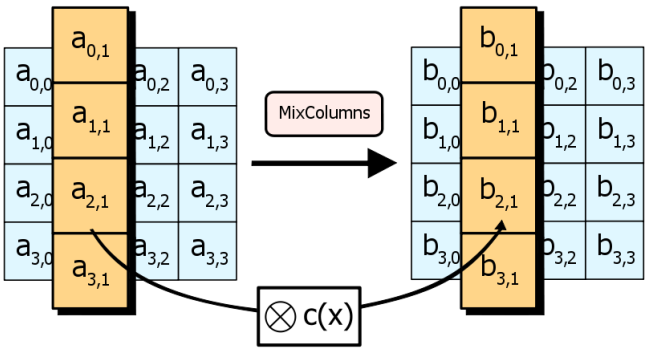

FIGURE 5.3 – AES-MixColumns

est la matrice circulante associée au vecteur $x = \begin{pmatrix} 02 \\ 01 \\ 01 \\ 03 \end{pmatrix} = \begin{pmatrix} x \\ 1 \\ 1 \\ x+1 \end{pmatrix}$

Definition. *Une matrice circulante ou de convolution circulaire est une matrice carrée dans laquelle on passe d'une ligne à la suivante par permutation circulaire (décalage vers la droite) des coefficients.Elle a la forme :*

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & & c_{n-3} \\ \vdots & & & \ddots & \vdots \\ c_1 & c_2 & c_3 & \dots & c_0 \end{pmatrix}$$

Exemple. *Effectuer MixColumns pour l'état actuel, qui est :*

01	*10*	*1b*	*ab*
02	*20*	*36*	*4d*
04	*40*	*6c*	*9a*
08	*80*	*d8*	*2f*

$$= \begin{pmatrix} 1 & x^4 & x^8 & x^{12} \\ x & x^5 & x^9 & x^{13} \\ x^2 & x^6 & x^{10} & x^{14} \\ x^3 & x^7 & x^{11} & x^{15} \end{pmatrix}$$

La multiplication des éléments de la matrice est la multiplication polynômiale. Pour l'effectuer soit on utilise la structure cyclique du sous-groupe multiplicatif $\mathbf{R}^*_{256} = (\mathbb{F}_2[x]/(m(x)))^*$ (l'ordre(x)=51 et l'ordre$(x+1)$=255), soit aprés la multiplication des polynômes on réduit modulo $m(x) = x^8 + x^4 + x^3 + x + 1 = 0$. Après la une multiplication des polynômes de degré ≤ 7 le degré maximal peut être 14. Parce que dans $(\mathbb{F}_2[x]/(m(x)))^*$, $m(x) = x^8 + x^4 + x^3 + x + 1 = 0$ nous pouvons faire les substitutions suivantes :

$x^8 = x^4 + x^3 + x + 1 = 1\text{b}.$
$x^9 = x^5 + x^4 + x^2 + x = 36.$
$x^{10} = x^6 + x^5 + x^3 + x^2 = 6\text{c}.$
$x^{11} = x^7 + x^6 + x^4 + x^3 = \text{d}8.$
$x^{12} = x^7 + x^5 + x^3 + x + 1 = \text{ab}.$
$x^{13} = x^6 + x^3 + x^2 + 1 = 4\text{d}.$
$x^{14} = x^7 + x^4 + x^3 + x = 9\text{a}.$
$x^{15} = x^5 + x^3 + x^2 + x + 1 = 2\text{f}.$

$$\begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} \cdot \begin{pmatrix} 1 & x^4 & x^8 & x^{12} \\ x & x^5 & x^9 & x^{13} \\ x^2 & x^6 & x^{10} & x^{14} \\ x^3 & x^7 & x^{11} & x^{15} \end{pmatrix} =$$

$$= \begin{pmatrix} x^3 & x^7 & x^{11} & x^{15} \\ 1 & x^4 & x^8 & x^{12} \\ x^4+x+1 & x^5+x^3+x+1 & x^7+x^2+x & x^7+x^5+x^4+x^3 \\ x^4+x^2+1 & x^6+x^3+x+1 & x^7+x^6+x^4+x^3+x^2 & x^6+x^5+x^3+x^2+x+1 \end{pmatrix} =$$

$$= \begin{array}{|c|c|c|c|} \hline 08 & 80 & \text{d}8 & 2\text{f} \\ \hline 01 & 10 & 1\text{b} & \text{ab} \\ \hline 13 & 2\text{b} & 86 & \text{b}8 \\ \hline 15 & 4\text{b} & \text{dc} & 6\text{f} \\ \hline \end{array}$$

<u>Exercice</u>.

1. *Calculer*
$$\begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} \cdot \begin{pmatrix} x^3+x^2+x \\ x^3+1 \\ x^3+x^2+1 \\ x^3+x+1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2. *Vérifiez que*
$$\begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} \cdot \begin{pmatrix} x^3+x^2+x & x^3+x+1 & x^3+x^2+1 & x^3+1 \\ x^3+1 & x^3+x^2+x & x^3+x+1 & x^3+x^2+1 \\ x^3+x^2+1 & x^3+1 & x^3+x^2+x & x^3+x+1 \\ x^3+x+1 & x^3+x^2+1 & x^3+1 & x^3+x^2+x \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

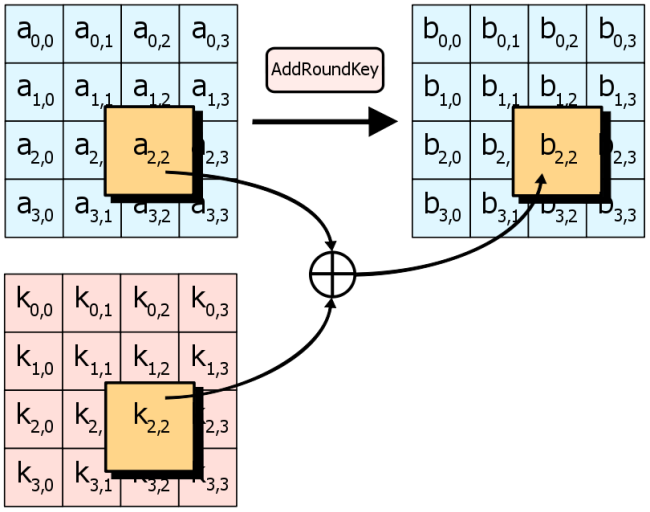

FIGURE 5.4 – AES-AddRoundKey

Remarque. *Il existe* $\mathbf{B} = \mathbf{C^{-1}}$*, (c.à-d.* $C \cdot B = I_4$*), donc l'étape MixColumns est inversible*

$$\mathbf{B} = \begin{pmatrix} x^3+x^2+x & x^3+x+1 & x^3+x^2+1 & x^3+1 \\ x^3+1 & x^3+x^2+x & x^3+x+1 & x^3+x^2+1 \\ x^3+x^2+1 & x^3+1 & x^3+x^2+x & x^3+x+1 \\ x^3+x+1 & x^3+x^2+1 & x^3+1 & x^3+x^2+x \end{pmatrix}$$

Donc

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} = \mathbf{B} \cdot \begin{pmatrix} b_0 & b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 & b_7 \\ b_8 & b_9 & b_{10} & b_{11} \\ b_{12} & b_{13} & b_{14} & b_{15} \end{pmatrix}$$

La description polynômiale de la transformation est donnée par une multiplication avec un polynôme $c(x) \in \mathbb{F}_2[x]$:

$$b(x) = A(x) \cdot c(x), \text{ modulo } (x^4+1),$$

où $A(x) = 03.x^3 + 01.x^2 + 01.x + 02$, modulo $1 + x^4$ et $a(x) = a_0 + a_1x + a_2x^2 + a_3x^3$, $b(x) = b_0 + b_1x + b_2x_2 + b_3x^3$. Le polynôme $A(x)$ est premier avec $x^4 + 1$ et il est donc inversible modulo $x^4 + 1$ est son inverse est $b(x) = 0b.x^3 + 0d.x^2 + 09.x + 0e$.

5.3.4 AddRoundKey : XOR de la clé de tour à l'état

La procédure AddRoundKey est très simple. Elle consiste à faire un OU exclusif (XOR) entre les 128 bits de l'état et les 128 bits de la clé de tour K_1. On obtient une nouvelle valeur de l'état.

Pour terminer notre exemple, il faut donc :

08	80	d8	2f	$\oplus$					=						
01	10	1b	ab												
13	2b	86	b8												
15	4b	dc	6f												

état actuel *clé de tour* *état en fin de tour*

5.4 La génération des clés de tour.

Les clés de tour se calculent à partir de la clé de chiffrement de l'utilisateur.

`Algorithme de génération des clés de tour:`

- La clé de chiffrement K de l'utilisateur génère une clé multiple K^* qui est un vecteur de 44 mots (une matrice 4×44 d'octets binaires).
- Les 11 clés de tour sont obtenus séquentiellement à partir de la clé multiple :
  - K_0 les 4 premiers mots de la clé multiple
  - K_1 les 4 mots suivants de la clé multiple
  - $\vdots$
  - K_{10} les 4 derniers mots de la clé multiple
- $K^* = (K_0, K_1, \ldots, K_{10})$

Dans notre cas :

43	33	1d	e2						
c6	25	2b	cc						
84	0c	c3	40						
53	80	97	b3						

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]	w[8]	w[9]
la clé de l'utilisateur				*clé de tour n°1*				*clé de tour n°2*	
K_0				K_1				K_2	

Calcul récursif des mots $w[i] \quad 0 \leq i \leq 43$ qui sont les composantes de **la clé multiple**.

$w[0]w[1]w[2]w[3]$ est simplement la clé de chiffrement de l'utilisateur

$$w[4] = w[0] \oplus w[3]^\sharp$$
$$w[5] = w[1] \oplus w[4]$$
$$w[6] = w[2] \oplus w[5]$$
$$w[7] = w[3] \oplus w[6]$$
$$w[8] = w[4] \oplus w[7]^\sharp$$
$$w[9] = w[5] \oplus w[8]$$
$$w[10] = w[6] \oplus w[9]$$
$$w[11] = w[7] \oplus w[10]$$
$$w[12] = w[8] \oplus w[11]^\sharp$$

$\vdots$

Reste à définir $w[3]^\sharp$, $w[7]^\sharp$, $w[11]^\sharp$, ... $w[39]^\sharp$.

$$\text{Si } w[4k-1] = \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} \text{ alors } w[4k-1]^\sharp = \begin{pmatrix} S(B) \\ S(C) \\ S(D) \\ S(A) \end{pmatrix} \oplus \begin{pmatrix} x^{k-1} \\ 00 \\ 00 \\ 00 \end{pmatrix}$$

Plus concrètement :

Si $w[3] = \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix}$ alors $w[3]^\sharp = \begin{pmatrix} S(B) \\ S(C) \\ S(D) \\ S(A) \end{pmatrix} \oplus \begin{pmatrix} 01 \\ 00 \\ 00 \\ 00 \end{pmatrix}$

Si $w[7] = \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix}$ alors $w[7]^\sharp = \begin{pmatrix} S(B) \\ S(C) \\ S(D) \\ S(A) \end{pmatrix} \oplus \begin{pmatrix} 02 \\ 00 \\ 00 \\ 00 \end{pmatrix}$

$\vdots$

Si $w[39] = \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix}$ alors $w[39]^\sharp = \begin{pmatrix} S(B) \\ S(C) \\ S(D) \\ S(A) \end{pmatrix} \oplus \begin{pmatrix} 36 \\ 00 \\ 00 \\ 00 \end{pmatrix}$ Dans notre cas, pour le calcul de la clé de tour K_1, il nous faut

$w[3]^\sharp = \begin{pmatrix} S(cc) \\ S(40) \\ S(b3) \\ S(e2) \end{pmatrix} \oplus \begin{pmatrix} 01 \\ 00 \\ 00 \\ 00 \end{pmatrix}$ $\left[\text{ Exercice : } w[3]^\sharp = \begin{pmatrix} 4a \\ 09 \\ 6d \\ 98 \end{pmatrix} \right]$

Exercice : Calculer K_1.

Réponse : $K_1 =$

09	3a	27	c5
cf	ea	c1	0d
e9	e5	26	66
cb	4b	dc	6f

Maintenant on peut finir le tour (Exercice) :

08	80	d8	2f
01	10	1b	ab
13	2b	86	b8
15	4b	dc	6f

$\oplus$

09	3a	27	c5
cf	ea	c1	0d
e9	e5	26	66
cb	4b	dc	6f

$=$

01	ba	ff	ea
ce	fa	da	a6
fa	ce	a0	de
de	00	00	00

état actuel *clé de tour* *état en fin de tour*

5.5 Plus d'exemples du Standard AES

Exercice. *Calcul d'une clé multiple :*

La clé de l'utilisateur $K = 2b\ 7e\ 15\ 16\ 28\ ae\ d2\ a6\ ab\ f7\ 15\ 88\ 09\ cf\ 4f\ 3c$.

Ceci donne :

$w_0 = 2b7e1516 \qquad w_1 = 28aed2a6 \qquad w_2 = abf71588 \qquad w_3 = 09cf4f3c$

indice	$w[i-1]$	*rotation*	$S(\ )$	$C^\sharp$	$\oplus C^\sharp$	$w[i-4]$	$w[i]$
4	09cf4f3c	cf4f3c09	8a84eb01	01000000	8b84eb01	2b7e1516	a0fafe17
5	a0fafe17					28aed2a6	88542cb1
6	88542cb1					abf71588	23a33939
7	23a33939					09cf4f3c	2a6c7605
8	2a6c7605	6c76052a	50386be5	02000000	52386be5	a0fafe17	f2c295f2
9	f2c295f2					88542cb1	7a96b943
10	7a96b943					23a33939	5935807a
11	5935807a					2a6c7605	7359f67f
12	7359f67f	59f67f73	cb42d28f	04000000	cf42d28f	f2c295f2	3d80477d
13	3d80477d					7a96b943	4716fe3e
14	4716fe3e					5935807a	1e237e44
15	1e237e44					7359f67f	6d7a883b
16	6d7a883b	7a883b6d	dac4e23c	08000000	d2c4e23c	3d80477d	ef44a541
17	ef44a541					4716fe3e	a8525b7f
18	a8525b7f					1e237e44	b671253b
19	b671253b					6d7a883b	db0bad00
20	db0bad00	0bad00db	2b9563b9	10000000	3b9563b9	ef44a541	d4d1c6f8
21	d4d1c6f8					a8525b7f	7c839d87
22	7c839d87					b671253b	caf2b8bc
23	caf2b8bc					db0bad00	11f915bc
24	11f915bc	f915bc11	99596582	20000000	b9596582	d4d1c6f8	6d88a37a
25	6d88a37a					7c839d87	110b3efd
26	110b3efd					caf2b8bc	dbf98641
27	dbf98641					11f915bc	ca0093fd
28	ca0093fd	0093fdca	63dc5474	40000000	23dc5474	6d88a37a	4e54f70e
29	4e54f70e					110b3efd	5f5fc9f3

indice	$w[i-1]$	*rotation*	$S(\ )$	$C^\sharp$	$\oplus\, C^\sharp$	$w[i-4]$	$w[i]$
30	5f5fc9f3					dbf98641	84a64fb2
31	84a64fb2					ca0093fd	4ea6dc4f
32	4ea6dc4f	a6dc4f4e	2486842f	80000000	a486842f	4e54f70e	ead27321
33	ead27321					5f5fc9f3	b58dbad2
34	b58dbad2					84a64fb2	312bf560
35	312bf560					4ea6dc4f	7f8d292f
36	7f8d292f	8d292f7f	5da515d2	1b000000	46a515d2	ead27321	ac7766f3
37	ac7766f3					b58dbad2	19fadc21
38	19fadc21					312bf560	28d12941
39	28d12941					7f8d292f	575c006e
40	575c006e	5c006e57	4a639f5b	36000000	7c639f5b	ac7766f3	d014f9a8
41	d014f9a8					19fadc21	c9ee2589
42	c9ee2589					28d12941	e13f0cc8
43	e13f0cc8					575c006e	b6630ca6

Exercice. *Soit un chiffrement en AES-128 :*

Le bloc de texte clair : 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34 .

La clé de l'utilisateur : 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c .

tour	état initial	après S( )	après ←	après $a*(\ )$		clé de tour	
0	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34				$\oplus$	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	=
1	19 a0 9a e9 3d f4 c6 f8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 ae f1 e5 30	d4 e0 b8 1e bf b4 41 27 5d 52 11 98 30 ae f1 e5	04 e0 48 28 66 cb f8 06 81 19 d3 26 e5 9a 7a 4c	$\oplus$	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	=
2	a4 68 6b 02 9c 9f 5b 6a 7f 35 ea 50 f2 2b 43 49	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	$\oplus$	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	=
3	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	$\oplus$	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	=

tour	état initial	après S( )	après ←	après $a*(\ )$		clé de tour	
4	48 67 4d d6 6c 1d e3 5f 4e 9d b1 58 ee 0d 38 e7	52 85 e3 f6 50 a4 11 cf 2f 5e c8 6a 28 d7 07 94	52 85 e3 f6 a4 11 cf 50 c8 6a 2f 5e 94 28 d7 07	0f 60 6f 5e d6 31 c0 b3 da 38 10 13 a9 bf 6b 01	$\oplus$	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	=
5	e0 c8 d9 85 92 63 b1 b8 7f 63 35 be e8 c0 50 01	e1 e8 35 97 4f fb c8 6c d2 fb 96 ae 9b ba 53 7c	e1 e8 35 97 fb c8 6c 4f 96 ae d2 fb 7c 9b ba 53	25 bd b6 4c d1 11 3a 4c a9 d1 33 c0 ad 68 8e b0	$\oplus$	d4 7c ca 11 d1 83 f2 f9 c6 9d b8 15 f8 87 bc bc	=
6	f1 c1 7c 5d 00 92 c8 b5 6f 4c 8b d5 55 ef 32 0c	a1 78 10 4c 63 4f e8 d5 d8 29 3d 03 fc df 23 fe	a1 78 10 4c 4f e8 d5 63 3d 03 a8 29 fe fc df 23	4b 2c 33 37 86 4a 9d d2 8d 89 f4 18 6d 80 e8 d8	$\oplus$	6d 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	=
7	26 3d e8 fd 0e 41 64 d2 2e b7 72 8b 17 7d a9 25	f7 27 9b 54 ab 83 43 b5 31 a9 40 3d f0 ff d3 3f	f7 27 9b 54 83 43 b5 ab 40 3d 31 a9 3f f0 ff d3	14 46 27 34 15 16 46 2a b5 15 56 d8 bf ec d7 43	$\oplus$	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	=
8	5a 19 a3 7a 41 49 e0 8c 42 dc 19 04 b1 1f 65 0c	be d4 0a da 83 3b e1 64 2c 86 d4 f2 c8 c0 4d fe	be d4 0a da 3b e1 64 83 d4 f2 2c 86 fe c8 c0 4d	00 b1 54 fa 51 c8 76 1b 2f 89 6d 99 d1 ff cd ea	$\oplus$	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	=
9	ea 04 65 85 83 45 5d 96 5c 33 98 b0 f0 2d ad c5	87 f2 4d 97 ec 6e 4c 90 4a c3 46 e7 8c d8 95 a6	87 f2 4d 97 6e 4c 90 ec 46 e7 4a c3 a6 8c d8 95	47 40 a3 4c 37 d4 70 9f 94 e4 3a 42 ed a5 a6 bc	$\oplus$	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	=
10	eb 59 8b 1b 40 2e a1 c3 f2 38 13 42 1e 84 e7 d2	e9 cb 3d af 09 31 32 2e 89 07 7d 2c 72 5f 94 b5	e9 cb 3d af 31 32 2e 09 7d 2c 89 07 b5 72 5f 94		$\oplus$	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	=
	39 02 dc 19 25 dc 11 6a 84 09 85 0b 1d fb 97 32						

Le chiffré : 39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32 .

5.6 Bibliographie

- The Design of Rijndael : AES - The Advanced Encryption Standard (Information Security and Cryptography) (1996)- Joan Daemen, Vincent Rijmen
- Applied Cryptography (1996) - Bruce Schneier
- NIST Federal Information Processing Standards Publication 197 AES :
- http ://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- Algorithmic Information Theory. Mathematics of Digital Information Processing (2006) -Peter Seibt
- Traitement algorithmique de l'information (2009)-Poly de cours de Peter Seibt

Appendix $\mathbf{R}_{256}$ est un groupe cyclique d'ordre $2^8 - 1$. La liste des 255 restes nonnuls dans $\mathbf{R}_{256}$, en fonction des puissances successives de $\xi = x + 1$.

$\xi^2 = x^2 + 1$
$\xi^3 = x^3 + x^2 + x + 1$
$\xi^4 = x^4 + 1$
$\xi^5 = x^5 + x^4 + x + 1$
$\xi^6 = x^6 + x^4 + x^2 + 1$
$\xi^7 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\xi^8 = x^4 + x^3 + x$
$\xi^9 = x^5 + x^3 + x^2 + x$
$\xi^{10} = x^6 + x^5 + x^4 + x$
$\xi^{11} = x^7 + x^4 + x^2 + x$
$\xi^{12} = x^7 + x^5 + 1$
$\xi^{13} = x^7 + x^6 + x^5 + x^4 + x^3$
$\xi^{14} = x^4 + x + 1$
$\xi^{15} = x^5 + x^4 + x^2 + 1$
$\xi^{16} = x^6 + x^4 + x^3 + x^2 + x + 1$
$\xi^{17} = x^7 + x^6 + x^5 + 1$

$\xi^{18} = x^5 + x^4 + x^3$
$\xi^{19} = x^6 + x^3$
$\xi^{20} = x^7 + x^6 + x^4 + x^3$
$\xi^{21} = x^6 + x^5 + x^4 + x + 1$
$\xi^{22} = x^7 + x^4 + x^2 + 1$
$\xi^{23} = x^7 + x^5 + x^2$
$\xi^{24} = x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$
$\xi^{25} = x$
$\xi^{26} = x^2 + x$
$\xi^{27} = x^3 + x$
$\xi^{28} = x^4 + x^3 + x^2 + x$
$\xi^{29} = x^5 + x$
$\xi^{30} = x^6 + x^5 + x^2 + x$
$\xi^{31} = x^7 + x^5 + x^3 + x$
$\xi^{32} = x^7 + x^6 + x^5 + x^2 + 1$
$\xi^{33} = x^5 + x^4 + x^2$
$\xi^{34} = x^6 + x^4 + x^3 + x^2$
$\xi^{35} = x^7 + x^6 + x^5 + x^2$
$\xi^{36} = x^5 + x^4 + x^2 + x + 1$
$\xi^{37} = x^6 + x^4 + x^3 + 1$
$\xi^{38} = x^7 + x^6 + x^5 + x^3 + x + 1$
$\xi^{39} = x^5 + x^2 + x$
$\xi^{40} = x^6 + x^5 + x^3 + x$
$\xi^{41} = x^7 + x^5 + x^4 + x^3 + x^2 + x$
$\xi^{42} = x^7 + x^6 + x^4 + x^3 + 1$
$\xi^{43} = x^6 + x^5 + x^4$
$\xi^{44} = x^7 + x^4$
$\xi^{45} = x^7 + x^5 + x^3 + x + 1$
$\xi^{46} = x^7 + x^6 + x^5 + x^2 + x$
$\xi^{47} = x^5 + x^4 + 1$
$\xi^{48} = x^6 + x^4 + x + 1$
$\xi^{49} = x^7 + x^6 + x^5 + x^4 + x^2 + 1$
$\xi^{50} = x^2$
$\xi^{51} = x^3 + x^2$
$\xi^{52} = x^4 + x^2$
$\xi^{53} = x^5 + x^4 + x^3 + x^2$
$\xi^{54} = x^6 + x^2$
$\xi^{55} = x^7 + x^6 + x^3 + x^2$
$\xi^{56} = x^6 + x^3 + x^2 + x + 1$
$\xi^{57} = x^7 + x^6 + x^4 + 1$
$\xi^{58} = x^6 + x^5 + x^2$
$\xi^{59} = x^7 + x^5 + x^4 + x^3$
$\xi^{60} = x^7 + x^6 + x^4 + x + 1$
$\xi^{61} = x^6 + x^5 + x^3 + x^2 + x$
$\xi^{62} = x^7 + x^5 + x^4 + x$
$\xi^{63} = x^7 + x^6 + x^3 + x^2 + 1$
$\xi^{64} = x^6 + x^3 + x^2$
$\xi^{65} = x^7 + x^6 + x^4 + x^2$
$\xi^{66} = x^6 + x^5 + x^2 + x + 1$
$\xi^{67} = x^7 + x^5 + x^3 + 1$
$\xi^{68} = x^7 + x^6 + x^5$
$\xi^{69} = x^5 + x^4 + x^3 + x + 1$
$\xi^{70} = x^6 + x^3 + x^2 + 1$
$\xi^{71} = x^7 + x^6 + x^4 + x^2 + x + 1$
$\xi^{72} = x^6 + x^5 + x$
$\xi^{73} = x^7 + x^5 + x^2 + x$
$\xi^{74} = x^7 + x^6 + x^5 + x^4 + 1$
$\xi^{75} = x^3$
$\xi^{76} = x^4 + x^3$
$\xi^{77} = x^5 + x^3$
$\xi^{78} = x^6 + x^5 + x^4 + x^3$
$\xi^{79} = x^7 + x^3$
$\xi^{80} = x^7 + x + 1$
$\xi^{81} = x^7 + x^4 + x^3 + x^2 + x$
$\xi^{82} = x^7 + x^5 + x^4 + x^3 + 1$
$\xi^{83} = x^7 + x^6 + x^4$
$\xi^{84} = x^6 + x^5 + x^3 + x + 1$
$\xi^{85} = x^7 + x^5 + x^4 + x^3 + x^2 + 1$
$\xi^{86} = x^7 + x^6 + x^4 + x^3 + x^2$
$\xi^{87} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\xi^{88} = x^7 + 1$
$\xi^{89} = x^7 + x^4 + x^3$
$\xi^{90} = x^7 + x^5 + x^4 + x + 1$
$\xi^{91} = x^7 + x^6 + x^3 + x^2 + x$
$\xi^{92} = x^6 + x^3 + 1$
$\xi^{93} = x^7 + x^6 + x^4 + x^3 + x + 1$
$\xi^{94} = x^6 + x^5 + x^4 + x^2 + x$
$\xi^{95} = x^7 + x^4 + x^3 + x$
$\xi^{96} = x^7 + x^5 + x^4 + x^2 + 1$
$\xi^{97} = x^7 + x^6 + x^2$
$\xi^{98} = x^6 + x^4 + x^2 + x + 1$
$\xi^{99} = x^7 + x^6 + x^5 + x^4 + x^3 + 1$

$\xi^{100} = x^4$
$\xi^{101} = x^5 + x^4$
$\xi^{102} = x^6 + x^4$
$\xi^{103} = x^7 + x^6 + x^5 + x^4$
$\xi^{104} = x^3 + x + 1$
$\xi^{105} = x^4 + x^3 + x^2 + 1$
$\xi^{106} = x^5 + x^2 + x + 1$
$\xi^{107} = x^6 + x^5 + x^3 + 1$
$\xi^{108} = x^7 + x^5 + x^4 + x^3 + x + 1$
$\xi^{109} = x^7 + x^6 + x^4 + x^2 + x$
$\xi^{110} = x^6 + x^5 + 1$
$\xi^{111} = x^7 + x^5 + x + 1$
$\xi^{112} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$
$\xi^{113} = x^4 + x^3 + 1$
$\xi^{114} = x^5 + x^3 + x + 1$
$\xi^{115} = x^6 + x^5 + x^4 + x^3 + x^2 + 1$
$\xi^{116} = x^7 + x^2 + x + 1$
$\xi^{117} = x^7 + x^4 + x$
$\xi^{118} = x^7 + x^5 + x^3 + x^2 + 1$
$\xi^{119} = x^7 + x^6 + x^5 + x^3 + x^2$
$\xi^{120} = x^5 + x^3 + x^2 + x + 1$
$\xi^{121} = x^6 + x^5 + x^4 + 1$
$\xi^{122} = x^7 + x^4 + x + 1$
$\xi^{123} = x^7 + x^5 + x^3 + x^2 + x$
$\xi^{124} = x^7 + x^6 + x^5 + x^3 + 1$
$\xi^{125} = x^5$
$\xi^{126} = x^6 + x^5$
$\xi^{127} = x^7 + x^5$
$\xi^{128} = x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$
$\xi^{129} = x^4 + x^2 + x$
$\xi^{130} = x^5 + x^4 + x^3 + x$
$\xi^{131} = x^6 + x^3 + x^2 + x$
$\xi^{132} = x^7 + x^6 + x^4 + x$
$\xi^{133} = x^6 + x^5 + x^3 + x^2 + 1$
$\xi^{134} = x^7 + x^5 + x^4 + x^2 + x + 1$
$\xi^{135} = x^7 + x^6 + x$
$\xi^{136} = x^6 + x^4 + x^3 + x^2 + 1$
$\xi^{137} = x^7 + x^6 + x^5 + x^2 + x + 1$
$\xi^{138} = x^5 + x^4 + x$
$\xi^{139} = x^6 + x^4 + x^2 + x$
$\xi^{140} = x^7 + x^6 + x^5 + x^4 + x^3 + x$
$\xi^{141} = x^4 + x^2 + 1$
$\xi^{142} = x^5 + x^4 + x^3 + x^2 + x + 1$
$\xi^{143} = x^6 + 1$
$\xi^{144} = x^7 + x^6 + x + 1$
$\xi^{145} = x^6 + x^4 + x^3 + x^2 + x$
$\xi^{146} = x^7 + x^6 + x^5 + x$
$\xi^{147} = x^5 + x^4 + x^3 + x^2 + 1$
$\xi^{148} = x^6 + x^2 + x + 1$
$\xi^{149} = x^7 + x^6 + x^3 + 1$
$\xi^{150} = x^6$
$\xi^{151} = x^7 + x^6$
$\xi^{152} = x^6 + x^4 + x^3 + x + 1$
$\xi^{153} = x^7 + x^6 + x^5 + x^3 + x^2 + 1$
$\xi^{154} = x^5 + x^3 + x^2$
$\xi^{155} = x^6 + x^5 + x^4 + x^2$
$\xi^{156} = x^7 + x^4 + x^3 + x^2$
$\xi^{157} = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\xi^{158} = x^7 + x^6 + x^4 + x^3 + x$
$\xi^{159} = x^6 + x^5 + x^4 + x^2 + 1$
$\xi^{160} = x^7 + x^4 + x^3 + x^2 + x + 1$
$\xi^{161} = x^7 + x^5 + x^4 + x^3 + x$
$\xi^{162} = x^7 + x^6 + x^4 + x^2 + 1$
$\xi^{163} = x^6 + x^5 + x^2$
$\xi^{164} = x^7 + x^5 + x^3 + x^2$
$\xi^{165} = x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
$\xi^{166} = x^5 + x^3 + x$
$\xi^{167} = x^6 + x^5 + x^4 + x^3 + x^2 + x$
$\xi^{168} = x^7 + x$
$\xi^{169} = x^7 + x^4 + x^3 + x^2 + 1$
$\xi^{170} = x^7 + x^5 + x^4 + x^3 + x^2$
$\xi^{171} = x^7 + x^6 + x^4 + x^3 + x^2 + x + 1$
$\xi^{172} = x^6 + x^5 + x^4 + x^3 + x$
$\xi^{173} = x^7 + x^3 + x^2 + x$
$\xi^{174} = x^7 + x^3 + 1$
$\xi^{175} = x^7$
$\xi^{176} = x^7 + x^4 + x^3 + x + 1$
$\xi^{177} = x^7 + x^5 + x^4 + x^2 + x$
$\xi^{178} = x^7 + x^6 + 1$
$\xi^{179} = x^6 + x^4 + x^3$
$\xi^{180} = x^7 + x^6 + x^5 + x^3$
$\xi^{181} = x^5 + x + 1$

$\xi^{182} = x^6 + x^5 + x^2 + 1$
$\xi^{183} = x^7 + x^5 + x^3 + x^2 + x + 1$
$\xi^{184} = x^7 + x^6 + x^5 + x^3 + x$
$\xi^{185} = x^5 + x^2 + 1$
$\xi^{186} = x^6 + x^5 + x^3 + x^2 + x + 1$
$\xi^{187} = x^7 + x^5 + x^4 + 1$
$\xi^{188} = x^7 + x^6 + x^3$
$\xi^{189} = x^6 + x + 1$
$\xi^{190} = x^7 + x^6 + x^2 + 1$
$\xi^{191} = x^6 + x^4 + x^2$
$\xi^{192} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2$
$\xi^{193} = x^4 + x^3 + x^2 + x + 1$
$\xi^{194} = x^5 + 1$
$\xi^{195} = x^6 + x^5 + x + 1$
$\xi^{196} = x^7 + x^5 + x^2 + 1$
$\xi^{197} = x^7 + x^6 + x^5 + x^4 + x^2$
$\xi^{198} = x^2 + x + 1$
$\xi^{199} = x^3 + 1$
$\xi^{200} = x^4 + x^3 + x + 1$
$\xi^{201} = x^5 + x^3 + x^2 + 1$
$\xi^{202} = x^6 + x^5 + x^4 + x^2 + x + 1$
$\xi^{203} = x^7 + x^4 + x^3 + 1$
$\xi^{204} = x^7 + x^5 + x^4$
$\xi^{205} = x^7 + x^6 + x^3 + x + 1$
$\xi^{206} = x^6 + x^2 + x$
$\xi^{207} = x^7 + x^6 + x^3 + x$
$\xi^{208} = x^6 + x^2 + 1$
$\xi^{209} = x^7 + x^6 + x^3 + x^2 + x + 1$
$\xi^{210} = x^6 + x^3 + x$
$\xi^{211} = x^7 + x^6 + x^4 + x^3 + x^2 + x$
$\xi^{212} = x^6 + x^5 + x^4 + x^3 + 1$
$\xi^{213} = x^7 + x^3 + x + 1$
$\xi^{214} = x^7 + x^2 + x$
$\xi^{215} = x^7 + x^4 + 1$
$\xi^{216} = x^7 + x^5 + x^3$
$\xi^{217} = x^7 + x^6 + x^5 + x + 1$
$\xi^{218} = x^5 + x^4 + x^3 + x^2 + x$
$\xi^{219} = x^6 + x$
$\xi^{220} = x^7 + x^6 + x^2 + x$
$\xi^{221} = x^6 + x^4 + 1$
$\xi^{222} = x^7 + x^6 + x^5 + x^4 + x + 1$
$\xi^{223} = x^3 + x^2 + x$
$\xi^{224} = x^4 + x$
$\xi^{225} = x^5 + x^4 + x^2 + x$
$\xi^{226} = x^6 + x^4 + x^3 + x$
$\xi^{227} = x^7 + x^6 + x^5 + x^3 + x^2 + x$
$\xi^{228} = x^5 + x^3 + 1$
$\xi^{229} = x^6 + x^5 + x^4 + x^3 + x + 1$
$\xi^{230} = x^7 + x^3 + x^2 + 1$
$\xi^{231} = x^7 + x^3 + x^2$
$\xi^{232} = x^7 + x^3 + x^2 + x + 1$
$\xi^{233} = x^7 + x^3 + x$
$\xi^{234} = x^7 + x^2 + 1$
$\xi^{235} = x^7 + x^4 + x^2$
$\xi^{236} = x^7 + x^5 + x^2 + x + 1$
$\xi^{237} = x^7 + x^6 + x^5 + x^4 + x$
$\xi^{238} = x^3 + x^2 + 1$
$\xi^{239} = x^4 + x^2 + x + 1$
$\xi^{240} = x^5 + x^4 + x^3 + 1$
$\xi^{241} = x^6 + x^3 + x + 1$
$\xi^{242} = x^7 + x^6 + x^4 + x^3 + x^2 + 1$
$\xi^{243} = x^6 + x^5 + x^4 + x^3 + x^2$
$\xi^{244} = x^7 + x^2$
$\xi^{245} = x^7 + x^4 + x^2 + x + 1$
$\xi^{246} = x^7 + x^5 + x$
$\xi^{247} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
$\xi^{248} = x^4 + x^3 + x^2$
$\xi^{249} = x^5 + x^2$
$\xi^{250} = x^6 + x^5 + x^3 + x^2$
$\xi^{251} = x^7 + x^5 + x^4 + x^2$
$\xi^{252} = x^7 + x^6 + x^2 + x + 1$
$\xi^{253} = x^6 + x^4 + x$
$\xi^{254} = x^7 + x^6 + x^5 + x^4 + x^2 + x$
$\xi^{255} = 1$