Cassage de codes avec des polynômes

Soutenance de projet

Mohamed Amine Najahi et Anissa Feukam

Université Pierre et Marie Curie

10 Juin 2010

Sommaire

1. Introduction
2. Rappels sur les chiffrements par bloc
3. La famille Katan/Ktantan
   - Algorithmes de cadencement de clef
   - Fonction de chiffrement
4. Cryptanalyse algébrique de Katan/Ktantan
5. Conclusion

Sommaire

1. Introduction
2. Rappels sur les chiffrements par bloc
3. La famille Katan/Ktantan
   - Algorithmes de cadencement de clef
   - Fonction de chiffrement
4. Cryptanalyse algébrique de Katan/Ktantan
5. Conclusion

Objectifs du projet

Objectifs

1. Implémenter les six chiffrements de la famille *Katan*/*Ktantan*.
2. Modéliser *Katan*_32 et *Ktantan*_32 sous forme de système algébrique.

Pour aller plus loin

- Proposer des attaques sur *Katan* et/ou *Ktantan*.

Rappels sur le chiffrement à clef secrète

Chiffrement symétrique (ou à clef secrète)

- Primitive de chiffrement dont la description est publique (Principe de Kerckhoffs).
- La confidentialité repose sur une clef partagée a priori.
- La même clef sert à chiffrer et déchiffrer.

Deux grandes catégories de chiffrements symétriques :

- Les chiffrements par bloc (*DES*, *AES*, *TripleDES*...).
- Les chiffrements par flot (*RC*4, *E*0, *Trivium*,...).

Sommaire

1 Introduction

2 Rappels sur les chiffrements par bloc

3 La famille Katan/Ktantan
- Algorithmes de cadencement de clef
- Fonction de chiffrement

4 Cryptanalyse algébrique de Katan/Ktantan

5 Conclusion

Chiffrement par bloc

- Agit sur un bloc de donnée de taille fixe.
- Paramétré par une clef K de taille fixe.
- Produit un bloc de même taille que le bloc d'entrée.

Un cryptosystème par bloc est constitué de 2 algorithmes :

- Un algorithme de chiffrement E_K.
- Un algorithme de déchiffrement D_K tel que $E_K \circ D_K = Id$.

Cryptosystème	taille du bloc	taille de clef
DES	64 *bits*	56 *bits*
AES	128 *bits*	128 *bits*
TripleDES	64 *bits*	168 *bits*
⋮	⋮	⋮

Caractéristiques des chiffrements les plus connus.

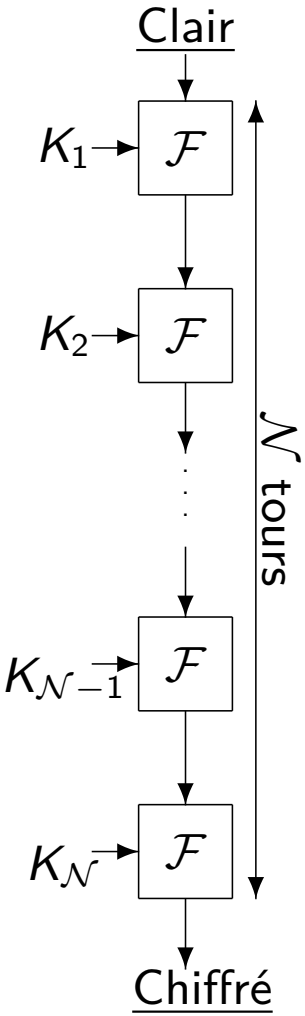
Construction itérative

Méthode répandue de construction de chiffrement :

1. Association d'un nombre de tours $\mathcal{N}$ à l'algorithme.
2. Description des transformations à effectuer pour un tour.
3. Description d'un algorithme de cadencement de clef.

Cryptosystème	Nombre de tours $\mathcal{N}$
DES	16
AES	10
TripleDES	48
Katan/Ktantan	254
⋮	⋮

Nombre de tours des chiffrements les plus connus



Construction itérative

Méthode répandue de construction de chiffrement :

1. Association d'un nombre de tours $\mathcal{N}$ à l'algorithme.
2. Description des transformations à effectuer pour un tour.
3. Description d'un algorithme de cadencement de clef.

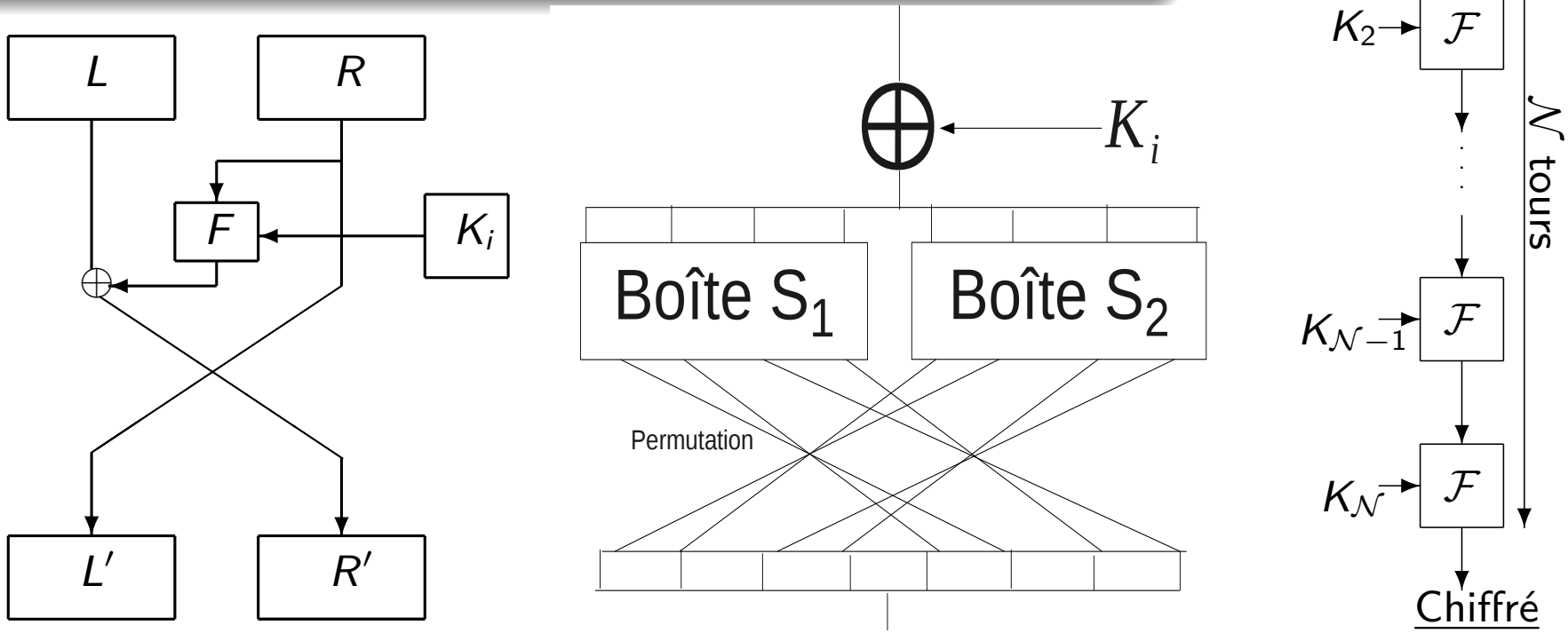
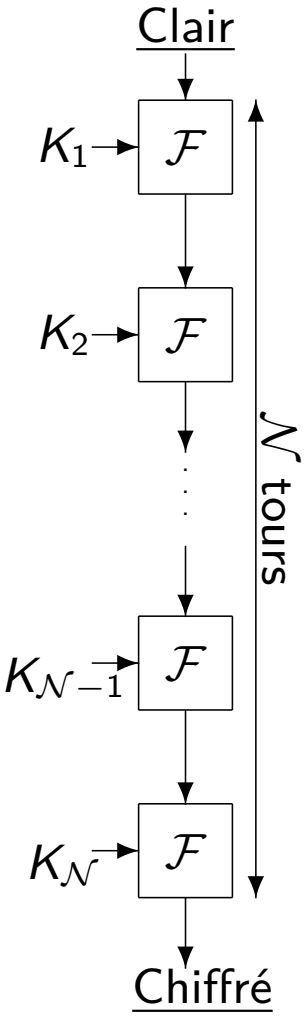


Schéma de Feistel (à gauche) et schéma SPN (à droite).

Construction itérative

Méthode répandue de construction de chiffrement :

1. Association d'un nombre de tours $\mathcal{N}$ à l'algorithme.
2. Description des transformations à effectuer pour un tour.
3. Description d'un algorithme de cadencement de clef.



Sommaire

1 Introduction

2 Rappels sur les chiffrements par bloc

3 La famille Katan/Ktantan
- Algorithmes de cadencement de clef
- Fonction de chiffrement

4 Cryptanalyse algébrique de Katan/Ktantan

5 Conclusion

Katan/*Ktantan*

Cryptosystème	Taille du bloc	Taille de clef	Type de schéma	Nombre de tours
Katan_32/*Ktantan_32*	32 *bits*	80 *bits*	*SPN*	254
Katan_48/*Ktantan_48*	48 *bits*			
Katan_64/*Ktantan_64*	64 *bits*			

Caractéristiques de *Katan*/*Ktantan*

Quelle différence alors entre *Katan_n* et *Ktantan_n* ?

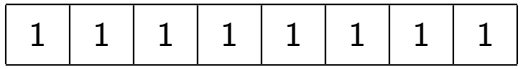
La seule différence réside dans l'algorithme de cadencement de clef.

- *Katan_n* utilise un LFSR (registre à décalage à rétroaction linéaire).
- *Ktantan_n* utilise deux multiplexeurs.

Compteur de tours Katan/Ktantan

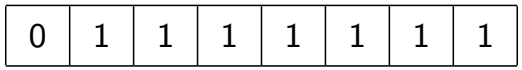
Un LFSR compteur.

- Initialiser les 8 bits d'un LFSR à 1.

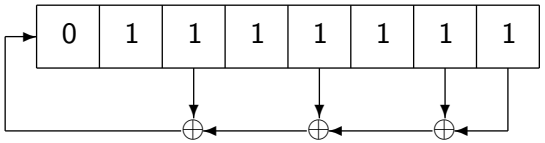


  - Son polynôme de rétroaction $P = x^8 + x^7 + x^5 + x^3 + 1$ est primitif. Sa période vaut $2^8 - 1 = 255$.

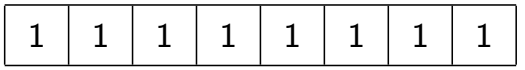
- Effectuer un seul décalage.



- Commencer le chiffrement.
  - Décaler le LFSR à chaque tour de chiffrement.



- Arrêter le chiffrement quand le LFSR retrouve l'état initial.

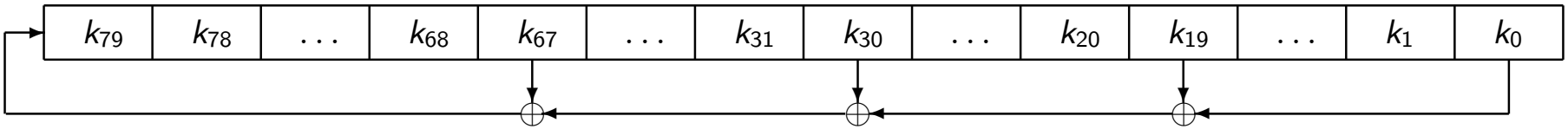


Cadencement de clef Katan

Le polynôme de rétroaction est :

$$P = x^{80} + x^{61} + x^{50} + x^{13} + 1$$

$$P \text{ est primitif} \Longrightarrow \text{La période du LFSR est de } 2^{80} - 1$$



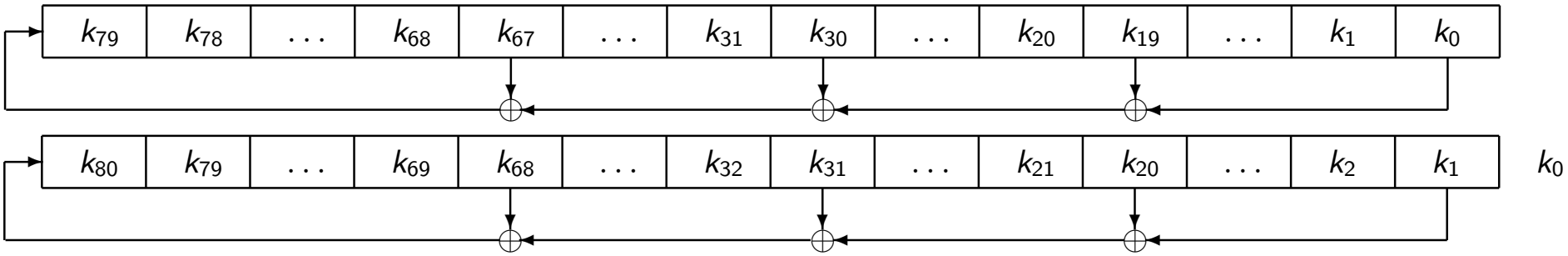
État initial.

Cadencement de clef Katan

Le polynôme de rétroaction est :

$$P = x^{80} + x^{61} + x^{50} + x^{13} + 1$$

$$P \text{ est primitif} \Longrightarrow \text{La période du LFSR est de } 2^{80} - 1$$



$$k_{80} = k_0 \oplus k_{19} \oplus k_{30} \oplus k_{67}$$

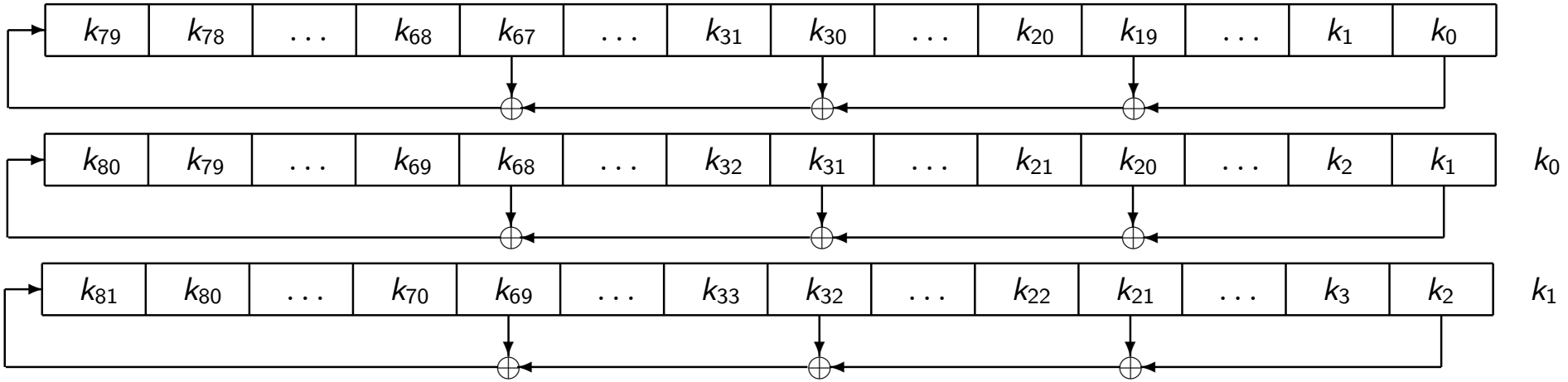
État du LFSR après un tic d'horloge.

Cadencement de clef Katan

Le polynôme de rétroaction est :

$$P = x^{80} + x^{61} + x^{50} + x^{13} + 1$$

$$P \text{ est primitif} \Longrightarrow \text{La période du LFSR est de } 2^{80} - 1$$



$$k_{81} = k_1 \oplus k_{20} \oplus k_{31} \oplus k_{68}$$

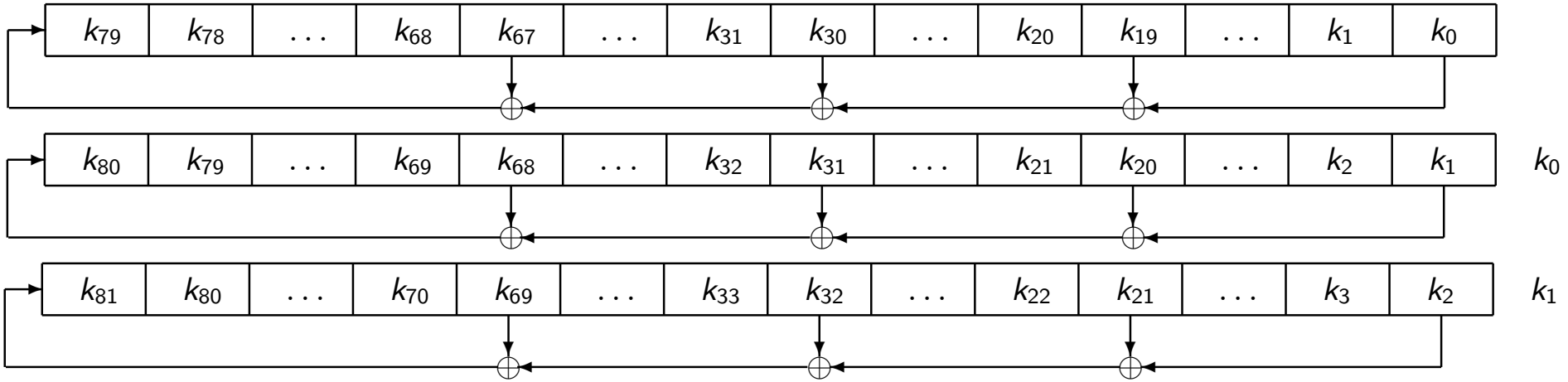
État du LFSR au bout d'un tour de *Katan*, après deux tics d'horloge.

Cadencement de clef Katan

Le polynôme de rétroaction est :

$$P = x^{80} + x^{61} + x^{50} + x^{13} + 1$$

$$P \text{ est primitif} \Longrightarrow \text{La période du LFSR est de } 2^{80} - 1$$



État du LFSR au bout d'un tour de *Katan*, après deux tics d'horloge.

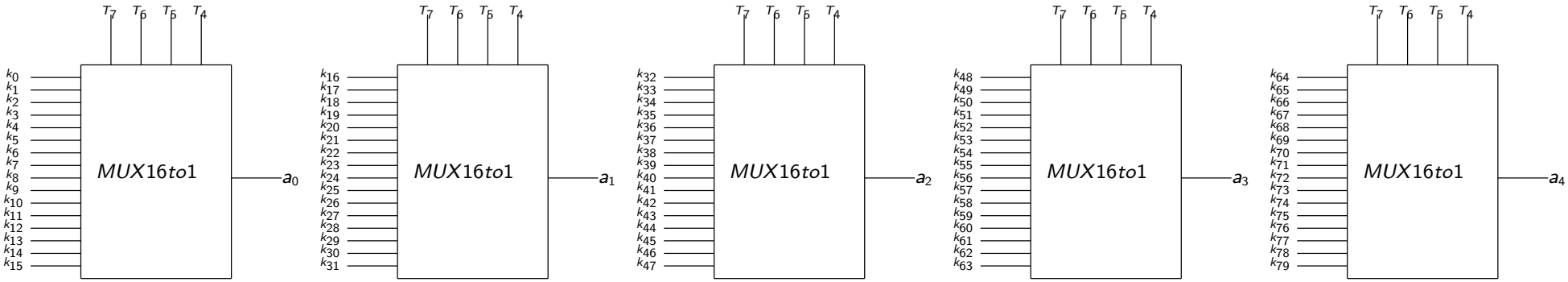
En notant K la clef maître, nous obtenons :

$$k_i = \begin{cases} K_i & \text{si } i = 0...79 \\ k_{i-80} \oplus k_{i-61} \oplus k_{i-50} \oplus k_{i-13} & \text{sinon} \end{cases}$$

Cadencement de clef Ktantan

L'algorithme utilise deux multiplexeurs : $Mux16to1$ et $Mux4to1$.
La séquence du LFSR qui sert de compteur est noté $T_7 \cdots T_0$(T_7 est le MSB, T_0 le LSB)

1. Découper la clef principale en 5 mots de 16 bits : $K = w_4||w_3||w_2||w_1||w_0$.
2. Calculer les 5 a_i où : $a_i = Mux16to1(w_i, T_7 T_6 T_5 T_4)$.

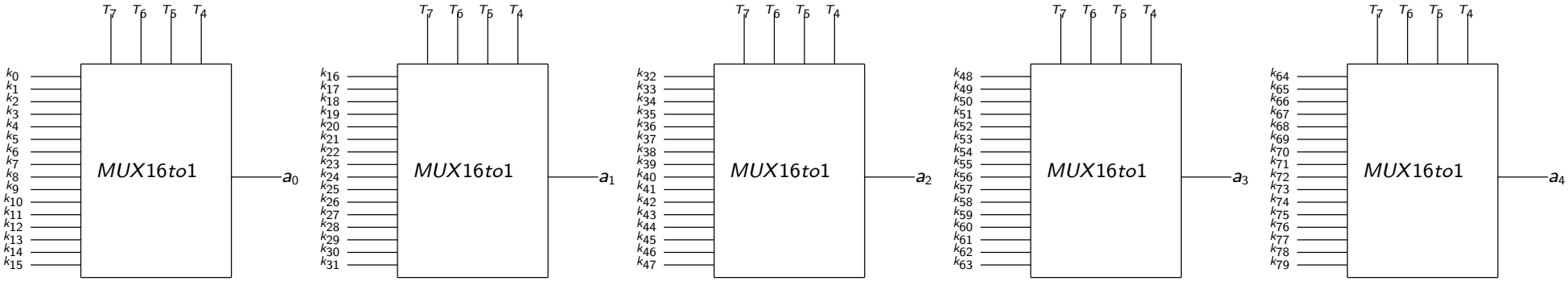


3. $k_a = \overline{T_3} \cdot \overline{T_2} \cdot (a_0) \oplus (T_3 \vee T2) \cdot MUX4to1(a_4 a_3 a_2 a_1, T_1 T_0)$,
   $k_b = \overline{T_3} \cdot T_2 \cdot (a_4) \oplus (T_3 \vee \overline{T2}) \cdot MUX4to1(a_3 a_2 a_1 a_0, \overline{T_1 T_0})$.

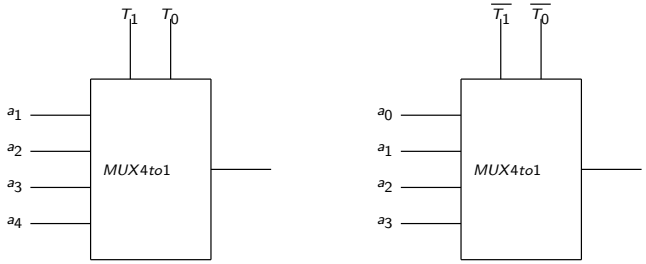
Cadencement de clef Ktantan

L'algorithme utilise deux multiplexeurs : $Mux16to1$ et $Mux4to1$.
La séquence du LFSR qui sert de compteur est noté $T_7 \cdots T_0$(T_7 est le MSB, T_0 le LSB)

1. Découper la clef principale en 5 mots de 16 bits : $K = w_4||w_3||w_2||w_1||w_0$.
2. Calculer les 5 a_i où : $a_i = Mux16to1(w_i, T_7 T_6 T_5 T_4)$.



3. $$k_a = \overline{T_3} \cdot \overline{T_2} \cdot (a_0) \oplus (T_3 \vee T2) \cdot MUX4to1(a_4 a_3 a_2 a_1, T_1 T_0),$$
   $$k_b = \overline{T_3} \cdot T_2 \cdot (a_4) \oplus (T_3 \vee \overline{T2}) \cdot MUX4to1(a_3 a_2 a_1 a_0, \overline{T_1 T_0}).$$



Fonctions de chiffrement

Début de l'algorithme $\Longrightarrow$ le texte clair $p_{31}p_{30}\cdots p_1p_0$ est chargé dans deux registre L_1 et L_2.

1. Au début de chaque tour, deux fonctions sont calculées :

$$f_a : L_1 \longrightarrow \mathbb{F}_2 \qquad \text{et} \qquad f_b : L_2 \longrightarrow \mathbb{F}_2$$

$$f_a(L_1) = L_1[x_1] \oplus L_1[x_2] \oplus (L_1[x_3] \cdot L_1[x_4]) \oplus (L_1[x_5] \cdot IR) \oplus k_a$$
$$f_b(L_2) = L_2[y_1] \oplus L_2[y_2] \oplus (L_2[y_3] \cdot L_2[y_4]) \oplus (L_2[y_5] \cdot L_2[y_6]) \oplus k_b$$

2. Les deux registres sont décalés vers la gauche.
3. $f_a(L_1)$ est inséré dans $L_2[0]$. $f_b(L_2)$ est inséré dans $L_1[0]$

p_{18}	p_{17}	p_{16}	p_{15}	p_{14}	p_{13}	p_{12}	p_{11}	p_{10}	p_9	p_8	p_7	p_6	p_5	p_4	p_3	p_2	p_1	p_0	L_2

p_{31}	p_{30}	p_{29}	p_{28}	p_{27}	p_{26}	p_{25}	p_{24}	p_{23}	p_{22}	p_{21}	p_{20}	p_{19}	L_1

Fonctions de chiffrement

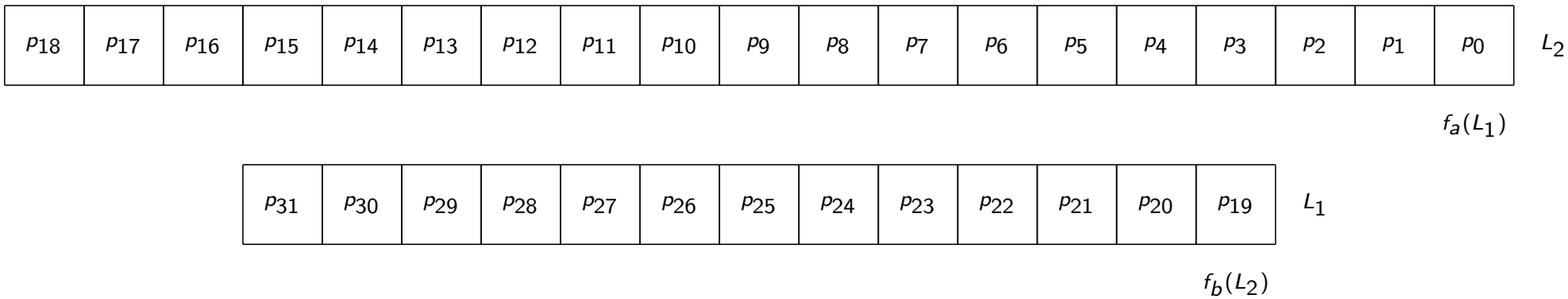
Début de l'algorithme $\Longrightarrow$ le texte clair $p_{31}p_{30}\cdots p_1p_0$ est chargé dans deux registre L_1 et L_2.

1. Au début de chaque tour, deux fonctions sont calculées :

$$f_a : L_1 \longrightarrow \mathbb{F}_2 \qquad \text{et} \qquad f_b : L_2 \longrightarrow \mathbb{F}_2$$

$$f_a(L_1) = L_1[x_1] \oplus L_1[x_2] \oplus (L_1[x_3] \cdot L_1[x_4]) \oplus (L_1[x_5] \cdot IR) \oplus k_a$$
$$f_b(L_2) = L_2[y_1] \oplus L_2[y_2] \oplus (L_2[y_3] \cdot L_2[y_4]) \oplus (L_2[y_5] \cdot L_2[y_6]) \oplus k_b$$

2. Les deux registres sont décalés vers la gauche.
3. $f_a(L_1)$ est inséré dans $L_2[0]$. $f_b(L_2)$ est inséré dans $L_1[0]$



Fonctions de chiffrement

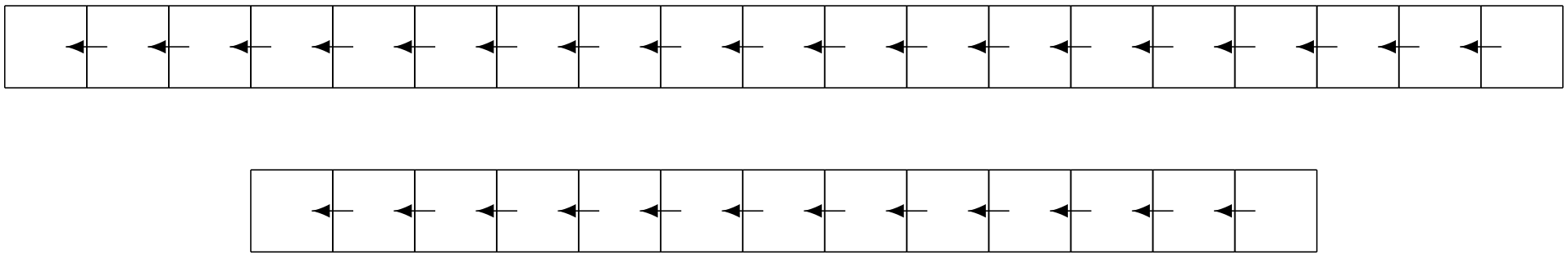
Début de l'algorithme $\Longrightarrow$ le texte clair $p_{31}p_{30}\cdots p_1p_0$ est chargé dans deux registre L_1 et L_2.

1. Au début de chaque tour, deux fonctions sont calculées :

$$f_a : L_1 \longrightarrow \mathbb{F}_2 \qquad \text{et} \qquad f_b : L_2 \longrightarrow \mathbb{F}_2$$

$$f_a(L_1) = L_1[x_1] \oplus L_1[x_2] \oplus (L_1[x_3] \cdot L_1[x_4]) \oplus (L_1[x_5] \cdot IR) \oplus k_a$$
$$f_b(L_2) = L_2[y_1] \oplus L_2[y_2] \oplus (L_2[y_3] \cdot L_2[y_4]) \oplus (L_2[y_5] \cdot L_2[y_6]) \oplus k_b$$

2. Les deux registres sont décalés vers la gauche.
3. $f_a(L_1)$ est inséré dans $L_2[0]$. $f_b(L_2)$ est inséré dans $L_1[0]$



Fonctions de chiffrement

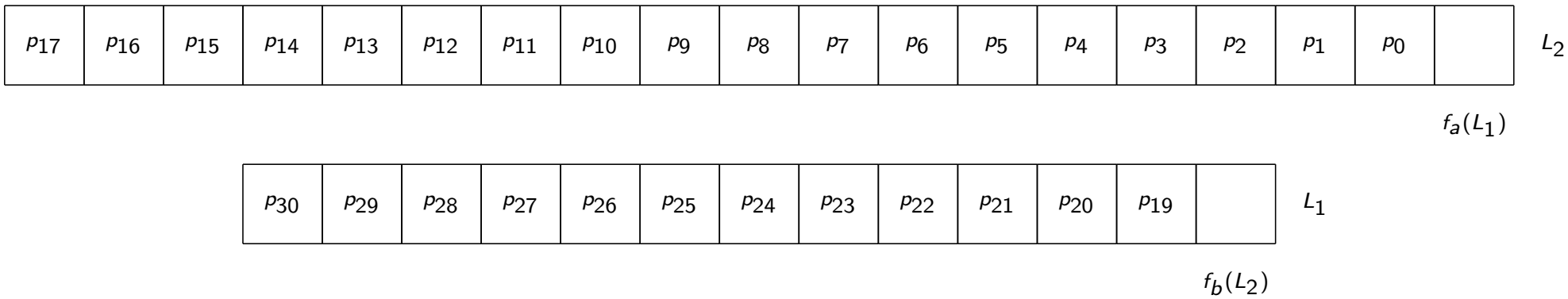
Début de l'algorithme $\Longrightarrow$ le texte clair $p_{31}p_{30}\cdots p_1p_0$ est chargé dans deux registre L_1 et L_2.

1. Au début de chaque tour, deux fonctions sont calculées :

$$f_a : L_1 \longrightarrow \mathbb{F}_2 \qquad \text{et} \qquad f_b : L_2 \longrightarrow \mathbb{F}_2$$

$$f_a(L_1) = L_1[x_1] \oplus L_1[x_2] \oplus (L_1[x_3] \cdot L_1[x_4]) \oplus (L_1[x_5] \cdot IR) \oplus k_a$$
$$f_b(L_2) = L_2[y_1] \oplus L_2[y_2] \oplus (L_2[y_3] \cdot L_2[y_4]) \oplus (L_2[y_5] \cdot L_2[y_6]) \oplus k_b$$

2. Les deux registres sont décalés vers la gauche.
3. $f_a(L_1)$ est inséré dans $L_2[0]$. $f_b(L_2)$ est inséré dans $L_1[0]$



Fonctions de chiffrement

Début de l'algorithme $\Longrightarrow$ le texte clair $p_{31}p_{30}\cdots p_1p_0$ est chargé dans deux registre L_1 et L_2.

1. Au début de chaque tour, deux fonctions sont calculées :

$$f_a : L_1 \longrightarrow \mathbb{F}_2 \qquad \text{et} \qquad f_b : L_2 \longrightarrow \mathbb{F}_2$$

$$f_a(L_1) = L_1[x_1] \oplus L_1[x_2] \oplus (L_1[x_3] \cdot L_1[x_4]) \oplus (L_1[x_5] \cdot IR) \oplus k_a$$
$$f_b(L_2) = L_2[y_1] \oplus L_2[y_2] \oplus (L_2[y_3] \cdot L_2[y_4]) \oplus (L_2[y_5] \cdot L_2[y_6]) \oplus k_b$$

2. Les deux registres sont décalés vers la gauche.
3. $f_a(L_1)$ est inséré dans $L_2[0]$. $f_b(L_2)$ est inséré dans $L_1[0]$

p_{17}	p_{16}	p_{15}	p_{14}	p_{13}	p_{12}	p_{11}	p_{10}	p_9	p_8	p_7	p_6	p_5	p_4	p_3	p_2	p_1	p_0	$f_a(L_1)$

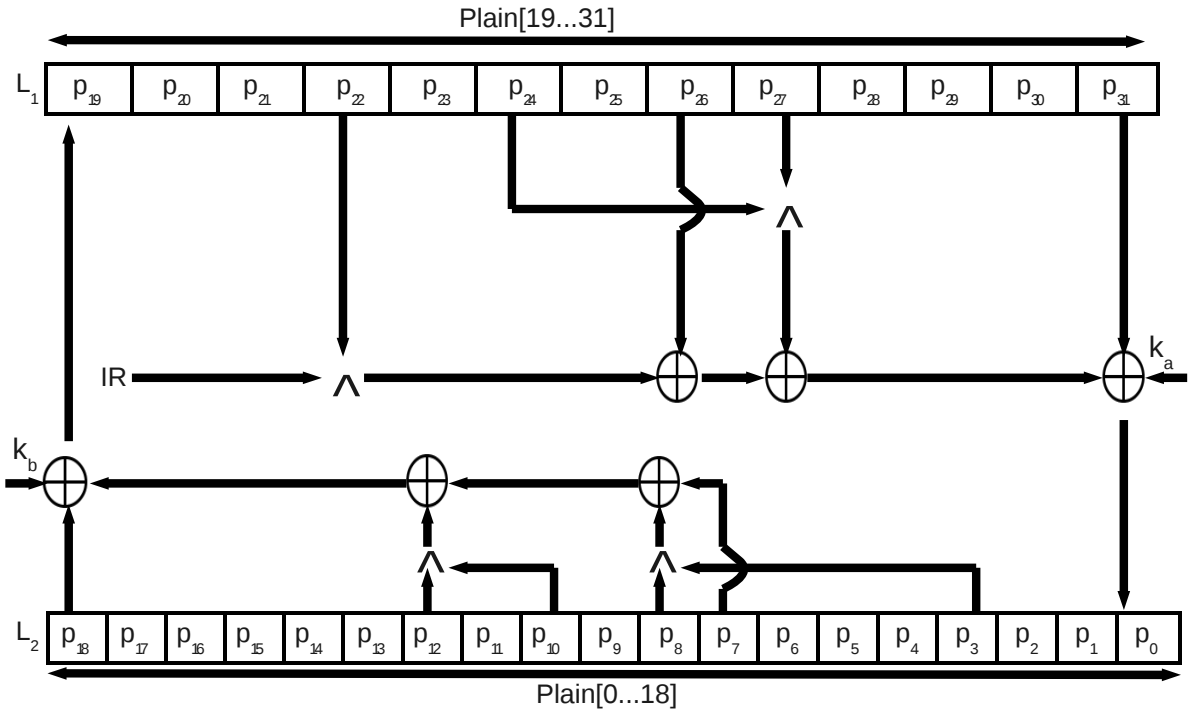
L_2

p_{30}	p_{29}	p_{28}	p_{27}	p_{26}	p_{25}	p_{24}	p_{23}	p_{22}	p_{21}	p_{20}	p_{19}	$f_b(L_2)$

L_1

Chiffrement	$\|L_1\|$	$\|L_2\|$	x_1	x_2	x_3	x_4	x_5
Katan_32/Ktantan_32	13	19	12	7	8	5	3
Katan_48/Ktantan_48	19	29	18	12	15	7	6
Katan_64/Ktantan_64	25	39	24	15	20	11	9

Chiffrement	y_1	y_2	y_3	y_4	y_5	y_6
Katan_32/Ktantan_32	18	7	12	10	8	3
Katan_48/Ktantan_48	28	19	21	13	15	6
Katan_64/Ktantan_64	38	25	33	21	14	9



Sommaire

1 Introduction

2 Rappels sur les chiffrements par bloc

3 La famille Katan/Ktantan
- Algorithmes de cadencement de clef
- Fonction de chiffrement

4 Cryptanalyse algébrique de Katan/Ktantan

5 Conclusion

La cryptanalyse algébrique

Principe

Modélisation du chiffrement par un système d'équations algébriques.
Résoudre ce système $\Longrightarrow$ Recouvrer une information secrète.

La cryptanalyse algébrique

Principe

Modélisation du chiffrement par un système d'équations algébriques.

Résoudre ce système $\Longrightarrow$ Recouvrer une information secrète.

2 étapes

- Modélisation :
  - Il est toujours possible d'écrire un chiffrement sous forme d'équations algébriques.
  - Il faut représenter la sortie en fonction de l'entrée et de la clef.

La cryptanalyse algébrique

Principe

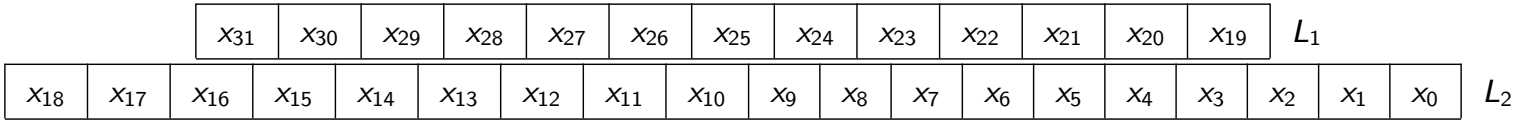
Modélisation du chiffrement par un système d'équations algébriques.
Résoudre ce système $\Longrightarrow$ Recouvrer une information secrète.

2 étapes

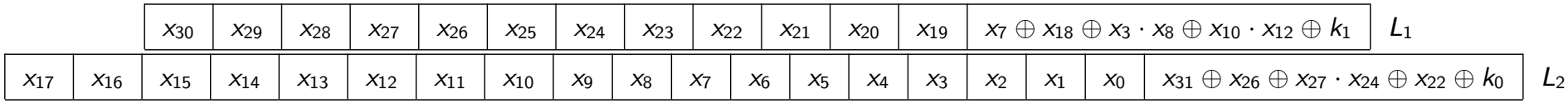
- Modélisation :
  - Il est toujours possible d'écrire un chiffrement sous forme d'équations algébriques.
  - Il faut représenter la sortie en fonction de l'entrée et de la clef.
- Résolution :
  - étape indépendante du chiffrement.
  - plusieurs algorithmes de résolution de systèmes algébriques (F4, F5, les SAT-solvers...).

Modélisation de Katan_32

L'état initial

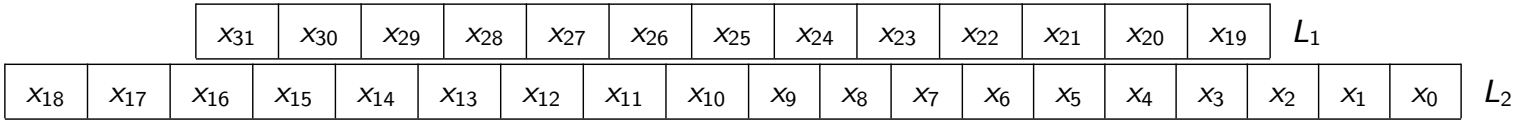


Après un tour

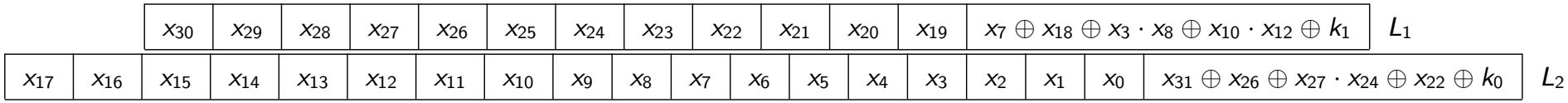


Modélisation de Katan_32

L'état initial

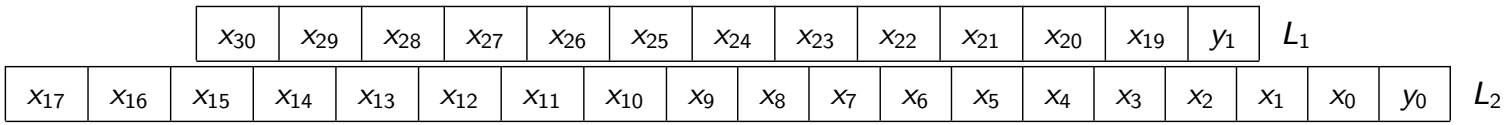


Après un tour



Idée : Introduire deux variables intermédiaires à chaque tour

1. Substituer les indices 0 des tableaux



2. Ajouter deux équations au système algébrique :

$$y_0 = x_{31} + x_{26} + x_{27} \cdot x_{24} + x_{22} + k_0 \iff x_{22} + x_{24} \cdot x_{27} + x_{26} + x_{31} + k_0 + y_0 = 0$$
$$y_1 = x_7 + x_{18} + x_3 \cdot x_8 + x_{10} \cdot x_{12} + k_1 \iff x_3 \cdot x_8 + x_7 + x_{10} \cdot x_{12} + x_{18} + k_1 + y_1 = 0$$

15 tours de Katan_32

Magma

Fichier Édition Affichage Terminal Aide

```
[
    x22 + x24*x27 + x26 + x31 + k0 + y0,
    x3*x8 + x7 + x10*x12 + x18 + k1 + y1,
    x21 + x23*x26 + x25 + x30 + k2 + y2,
    x2*x7 + x6 + x9*x11 + x17 + k3 + y3,
    x20 + x22*x25 + x24 + x29 + k4 + y4,
    x1*x6 + x5 + x8*x10 + x16 + k5 + y5,
    x19 + x21*x24 + x23 + x28 + k6 + y6,
    x0*x5 + x4 + x7*x9 + x15 + k7 + y7,
    x20*x23 + x22 + x27 + k8 + y0 + y8,
    x3 + x4*y1 + x6*x8 + x14 + k9 + y9,
    x19*x22 + x21 + x26 + k10 + y2 + y10,
    x2 + x3*y3 + x5*x7 + x13 + k11 + y11,
    x20 + x21*y0 + x25 + k12 + y4 + y12,
    x1 + x2*y5 + x4*x6 + x12 + k13 + y13,
    x19 + x20*y2 + x24 + k14 + y14,
    x0 + x1*y7 + x3*x5 + x11 + k15 + y15,
    x19*y4 + x23 + k16 + y0 + y16,
    x0*y9 + x2*x4 + x10 + k17 + y1 + y17,
    x22 + k18 + y0*y6 + y2 + y18,
    x1*x3 + x9 + k19 + y1*y11 + y3 + y19,
    x21 + k20 + y2*y8 + y4 + y12 + y20,
    x0*x2 + x8 + k21 + y3*y13 + y5 + y21,
    x20 + k22 + y4*y10 + y6 + y14 + y22,
    x1*y1 + x7 + k23 + y5*y15 + y7 + y23,
    x19 + k24 + y6*y12 + y8 + y24,
    x0*y3 + x6 + k25 + y7*y17 + y9 + y25,
    k26 + y0 + y8*y14 + y10 + y18 + y26,
    x5 + k27 + y1*y5 + y9*y19 + y11 + y27,
    k28 + y2 + y10*y16 + y12 + y28,
    x4 + k29 + y3*y7 + y11*y21 + y13 + y29
]
>
```

État des registres après 15 tours.

y_5	y_7	y_9	y_{11}	y_{13}	y_{15}	y_{17}	y_{19}	y_{21}	y_{23}	y_{25}	y_{27}	y_{29}	L_1	
x_3	x_2	x_1	x_0	y_0	y_2	y_4	y_6	y_8	y_{10}	y_{12}	y_{14}	y_{16}	y_{18}	y_{20}	y_{22}	y_{24}	y_{26}	y_{28}	L_2

Quelques chiffres

Soit N le nombre de tours.

- Nombre de variables du système :
  - 32 variables pour le clair.
  - $2 \times N$ variables de clef.
  - $2 \times N$ variables intermédiaires.
- Nombre d'équations du système :
  - une équation de corps pour chaque variable.
  - deux équations de cadencement de clef à chaque tour (pour $N > 40$).
  - 2 équations quadratiques à chaque tour.

Katan_32 avec 254 tours

- 1048 variables.
- 1984 équations.

15 tours de Katan_32

Magma

Fichier Édition Affichage Terminal Aide

```
[
    x22 + x24*x27 + x26 + x31 + k0 + y0,
    x3*x8 + x7 + x10*x12 + x18 + k1 + y1,
    x21 + x23*x26 + x25 + x30 + k2 + y2,
    x2*x7 + x6 + x9*x11 + x17 + k3 + y3,
    x20 + x22*x25 + x24 + x29 + k4 + y4,
    x1*x6 + x5 + x8*x10 + x16 + k5 + y5,
    x19 + x21*x24 + x23 + x28 + k6 + y6,
    x0*x5 + x4 + x7*x9 + x15 + k7 + y7,
    x20*x23 + x22 + x27 + k8 + y0 + y8,
    x3 + x4*y1 + x6*x8 + x14 + k9 + y9,
    x19*x22 + x21 + x26 + k10 + y2 + y10,
    x2 + x3*y3 + x5*x7 + x13 + k11 + y11,
    x20 + x21*y0 + x25 + k12 + y4 + y12,
    x1 + x2*y5 + x4*x6 + x12 + k13 + y13,
    x19 + x20*y2 + x24 + k14 + y14,
    x0 + x1*y7 + x3*x5 + x11 + k15 + y15,
    x19*y4 + x23 + k16 + y0 + y16,
    x0*y9 + x2*x4 + x10 + k17 + y1 + y17,
    x22 + k18 + y0*y6 + y2 + y18,
    x1*x3 + x9 + k19 + y1*y11 + y3 + y19,
    x21 + k20 + y2*y8 + y4 + y12 + y20,
    x0*x2 + x8 + k21 + y3*y13 + y5 + y21,
    x20 + k22 + y4*y10 + y6 + y14 + y22,
    x1*y1 + x7 + k23 + y5*y15 + y7 + y23,
    x19 + k24 + y6*y12 + y8 + y24,
    x0*y3 + x6 + k25 + y7*y17 + y9 + y25,
    k26 + y0 + y8*y14 + y10 + y18 + y26,
    x5 + k27 + y1*y5 + y9*y19 + y11 + y27,
    k28 + y2 + y10*y16 + y12 + y28,
    x4 + k29 + y3*y7 + y11*y21 + y13 + y29
]
>
```

État des registres après 15 tours.

y_5	y_7	y_9	y_{11}	y_{13}	y_{15}	y_{17}	y_{19}	y_{21}	y_{23}	y_{25}	y_{27}	y_{29}	L_1	
x_3	x_2	x_1	x_0	y_0	y_2	y_4	y_6	y_8	y_{10}	y_{12}	y_{14}	y_{16}	y_{18}	y_{20}	y_{22}	y_{24}	y_{26}	y_{28}	L_2

Quelques chiffres

Soit N le nombre de tours.

- Nombre de variables du système :
  - 32 variables pour le clair.
  - $2 \times N$ variables de clef.
  - $2 \times N$ variables intermédiaires.
- Nombre d'équations du système :
  - une équation de corps pour chaque variable.
  - deux équations de cadencement de clef à chaque tour (pour $N > 40$).
  - 2 équations quadratiques à chaque tour.

Katan_32 avec 254 tours

- 1048 variables.
- 1984 équations.

Pour aller plus loin : attaques sur Katan_32

Scénario de l'attaque

1. Choisir un texte clair P (une séquence de 32 bits).
2. Fixer les variables correspondant au texte clair dans le système.
3. Choisir une clef K (une séquence de 80 bits).
4. Calculer C le chiffré de P par K.
5. Fixer les variables qui correspondent au résultat dans le système.
6. Lancer la résolution avec l'algorithme $F4$.

Limites de l'approche

- Impossible de dépasser les 23 tours.

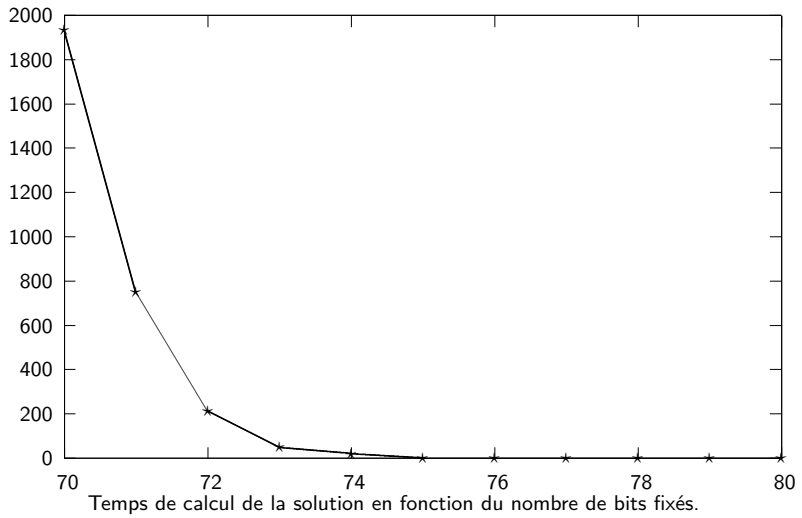
Nombre de tours	Temps de calcul de la solution (en secondes)
10	0.040
15	0.050
20	0.250
21	0.960
22	5.190
23	55.700

Pour aller plus loin : attaques sur Katan_32 et Ktantan_32

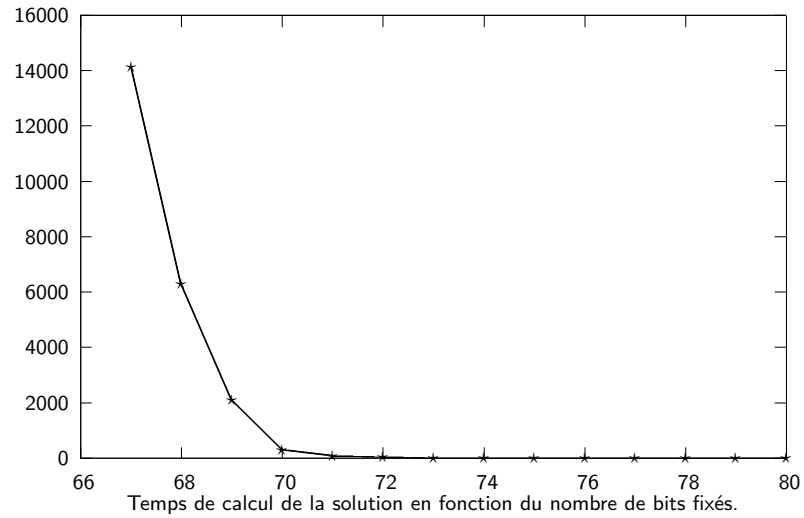
Scénario d'attaque plus souple

1. On fixera le nombre de tours à 100.
2. On supposera connus certains bits de la clef.

Nouveaux résultats : *Katan_32*



Nouveaux résultats : *Ktantan_32*

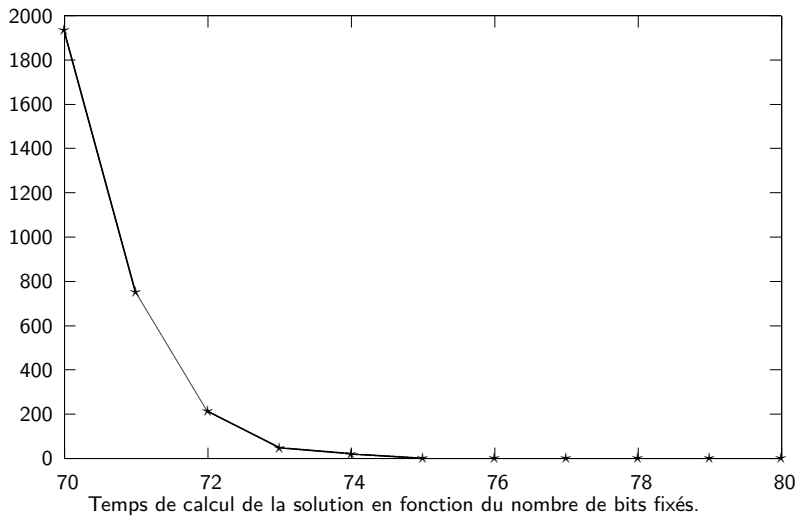


Pour aller plus loin : attaques sur Katan_32 et Ktantan_32

Scénario d'attaque plus souple

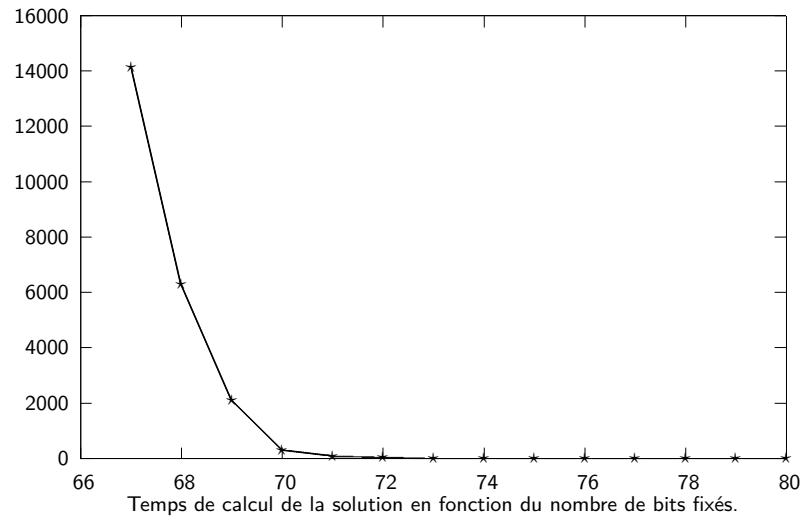
1. On fixera le nombre de tours à 100.
2. On supposera connus certains bits de la clef.

Nouveaux résultats : *Katan_32*



Temps de calcul de la solution en fonction du nombre de bits fixés.

Nouveaux résultats : *Ktantan_32*



Temps de calcul de la solution en fonction du nombre de bits fixés.

Bilan de *Katan_32* réduit à 100 tours

Une attaque théorique de complexité 2^{70} est possible.

Bilan de *Ktantan_32* réduit à 100 tours

Une attaque théorique de complexité 2^{67} est possible.

Sommaire

1. Introduction
2. Rappels sur les chiffrements par bloc
3. La famille Katan/Ktantan
   - Algorithmes de cadencement de clef
   - Fonction de chiffrement
4. Cryptanalyse algébrique de Katan/Ktantan
5. Conclusion

Conclusion

Objectifs de départs atteints

- Nous avons présenté une nouvelle famille de chiffrement.
- Nous avons proposé une modélisation de *Katan*/*Ktantan*.

Conclusion

Objectifs de départs atteints

- Nous avons présenté une nouvelle famille de chiffrement.
- Nous avons proposé une modélisation de *Katan*/*Ktantan*.

Objectifs de départs dépassés

- Nous avons exposé quelques scénarios d'attaques ainsi que leurs résultats.

Conclusion

Objectifs de départs atteints

- Nous avons présenté une nouvelle famille de chiffrement.
- Nous avons proposé une modélisation de *Katan*/*Ktantan*.

Objectifs de départs dépassés

- Nous avons exposé quelques scénarios d'attaques ainsi que leurs résultats.

Pour finir

Katan et Ktantan :

- Des chiffrements modernes.
- Sobres et orientés hardware.
- Assez résistants aux attaques algébriques.

Conclusion

Merci à tous ! ! !