Quelques aspects de la cryptographie et du codage - Partie 1

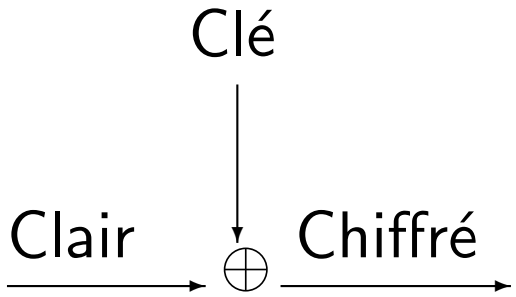
Claude Carlet (Université Paris 8-MAATICAH et INRIA)

Sommaire

- Utilisation des fonctions booléennes dans les schémas par flots.
- Représentations des fonctions booléennes.
- Critères cryptographiques (degré, nonlinéarité, résilience) et bornes sur ces critères.
- Les constructions classiques et récentes.
- Immunité algébrique des fonctions booléennes.

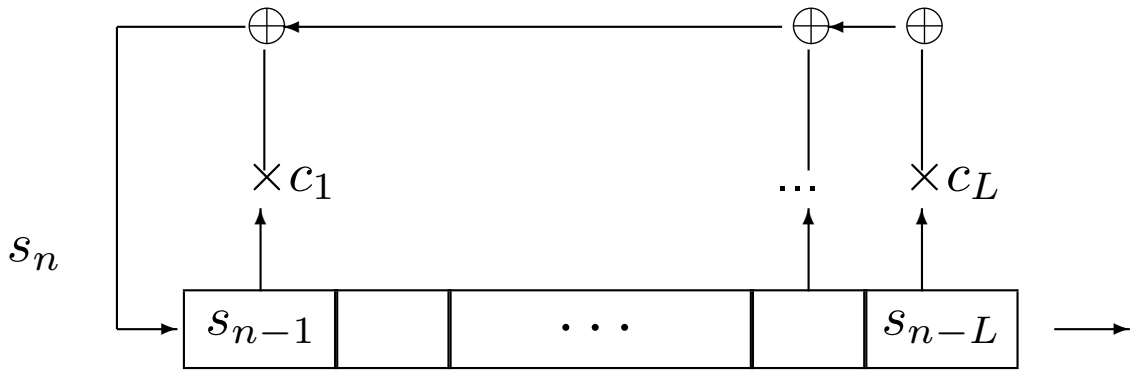
Utilisation des fonctions booléennes dans les schémas par flots

Chiffrement de Vernam



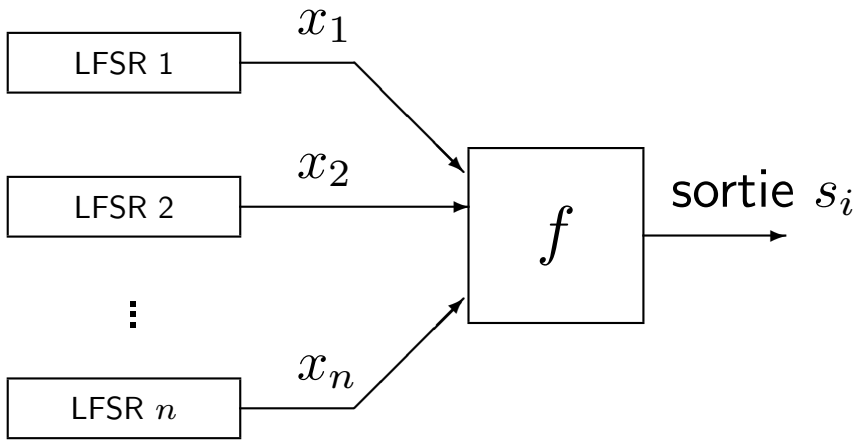
En pratique, il est nécessaire d'utiliser des générateurs de pseudo-aléas.

Registre à décalage (Linear feedback shift register) :



$$s_n = \sum_{i=1}^{L} c_i s_{n-i}.$$

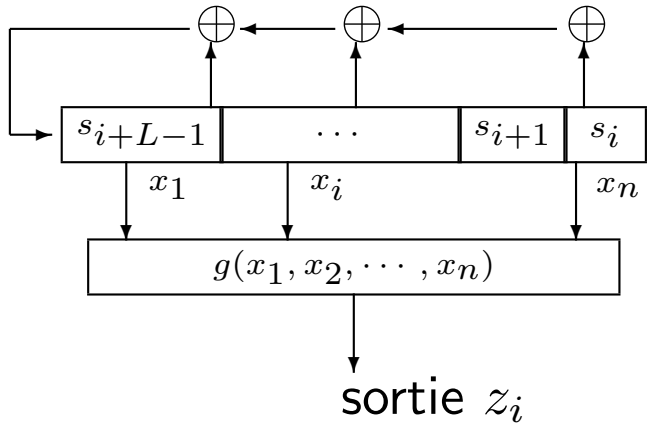
Fonction de combinaison



Les c_i peuvent être publiques.

La clé : l'initialisation des LFSRs.

Fonction de filtrage



Ce générateur “équivaut” au précédent.

Etude des fonctions booléennes

Le nombre des fonctions booléennes $f : {F_2}^n \mapsto F_2$:

n :	4	5	6	7	8
$\lvert\mathcal{B}_n\rvert$:	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}

TAB. 1: NOMBRE DES FONCTIONS BOOLÉENNES

Même pour n petit, les critères cryptographiques ne peuvent pas être étudiés par simple investigation sur machine ; des preuves mathématiques sont nécessaires.
On ne peut pas non plus obtenir, par tirage, des fonctions satisfaisant les critères cryptographiques à de bons niveaux ; des constructions sont nécessaires.

Représentations usuelles des fonctions booléennes

La forme algébrique normale A.N.F. (elle existe et est unique) :

$$x = (x_1, \cdots, x_n);\ f(x) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \sum_{u \in F_2^n} a_u\, x^u,$$

où $x^u = \prod_{i=1}^{n} x_i^{u_i}$.

Le degré de l'A.N.F. est un invariant affine, de même que le *poids de Hamming* $w_H(f) = \#\{x \in F_2^n / \ f(x) \neq 0\}$.

La fonction $u \longrightarrow a_u$ est la *transformée de Möbius* de f.

On définit sur F_2^n l'ordre partiel suivant :

$$(v_1, \ldots, v_n) \leq (u_1, \ldots, u_n) \Longleftrightarrow \forall i = 1, \ldots, n,\ v_i \leq u_i.$$

Alors, la transformée de Möbius de f est définie par :

$$g(u) = \sum_{v \in F_2^n \mid v \leq u} f(v).$$

Le *code de Reed-Muller* d'ordre k $(0 \leq k \leq n)$:

l'ensemble $R(k, n)$ des fonctions de degrés $\leq k$.

$R(1,n)$: l'ensemble des fonctions affines $l(x) = a \cdot x + a_0$ où $a \cdot x = a_1x_1 + \cdots + a_nx_n$ $(a_0, a_1, \ldots, a_n \in F_2)$.

La représentation trace

- toute application F de $F_2^n \sim F_{2^n}$ dans lui-même admet une unique représentation polynomiale (d'une seule variable) de degré au plus $2^n - 1$: $F(x) = \sum_{i=0}^{2^n-1} \beta_i x^i$.

- toute fonction booléenne $f(x)$ peut donc s'écrire $f(x) = tr(P(x))$ où P est un polynôme de degré au plus $2^n - 1$ puisque $f(x) = tr(\beta f(x))$ où $tr(\beta) = 1$. Comme $tr(\beta x^i) = tr(\beta^2 x^{2i})$, on peut restreindre les exposants à un seul exposant par classe cyclotomique de 2 modulo $2^n - 1$.

Le degré est alors égal au poids maximal des expressions binaires des exposants des monômes ayant des coefficients non nuls.

Critères cryptographiques sur les fonctions booléennes

1. toute fonction cryptographique f doit avoir un *degré élevé*.

2. toute fonction cryptographique f doit être *équilibrée* (i.e. équidistribuée sur $\{0,1\}$).

3. toute fonction cryptographique doit être *à grande distance de Hamming*

$$d_H(f,l) = \#\{x \in F_2^n;\ f(x) \neq l(x)\} = w_H(f+l)$$

des fonctions affines.

La *nonlinéarité* $\mathcal{NL}(f)$ de f est sa distance minimale aux fonctions affines.

Elle peut être caractérisée à l'aide de la *transformation de Fourier discrète*.

Définition

Soit φ une fonction numérique (i.e. à valeurs dans **R**) sur F_2^n. La transformée de Fourier de φ est la fonction

$$\widehat{\varphi}(a) = \sum_{x \in F_2^n} \varphi(x)\,(-1)^{a \cdot x}.$$

Propriétés

Etant donné un sous-espace vectoriel E de F_2^n, on note $E^\perp$ son *orthogonal* $E^\perp = \{x \in F_2^n / \forall y \in E;\ x \cdot y = 0\}$.

On note 1_E l'indicatrice de E. Alors, on a :

$$\widehat{1_E} = |E|\, 1_{E^\perp}.$$

On en déduit que, pour tout sous-espace vectoriel E de F_2^n, on a :

$$\sum_{s \in E} \widehat{\varphi}(s) = |E| \sum_{x \in E^\perp} \varphi(x).$$

Preuve :

$$\sum_{s\in E}\widehat{\varphi}(s)=\sum_{x\in F_2^n}\varphi(x)\,\widehat{1_E}(x)=|E|\sum_{x\in E^\perp}\varphi(x).$$

On peut appliquer la transformée de Fourier à f ou à sa fonction signe $f_\chi(x)=(-1)^{f(x)}$;

On obtient alors la *transformée de Walsh* de f :

$$\widehat{f_\chi}(a)=\sum_{x\in {F_2}^n}(-1)^{f(x)+a\cdot x},$$

dont le support $\{a\in F_2^n \mid \widehat{f_\chi}(a)\neq 0\}$ s'appelle le *support de Walsh*.

La caractérisation des structures algébriques possibles des supports de Walsh des fonctions booléennes est un problème ouvert difficile (C.C., S. Mesnager).

En posant : $\mathcal{F}(f) = \widehat{f_\chi}(0) = \sum_{x \in F_2^n} (-1)^{f(x)}$ on a :

$$w_H(f) = 2^{n-1} - \frac{1}{2}\mathcal{F}(f).$$

D'où $\mathcal{NL}(f)$ est égal à

$$2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} \left| \widehat{f_\chi}(a) \right|.$$

Le rayon de recouvrement de $R(1,n)$ est $\rho(n) = \max_{f \in \mathcal{B}_n} \mathcal{NL}(f)$. On a : $\rho(n) \leq 2^{n-1} - 2^{n/2-1}$.

C'est une conséquence de la relation de *Parseval*

$$\sum_{a \in F_2^n} \widehat{f_\chi}^2(a) = \sum_{x,y \in F_2^n} (-1)^{f(x)+f(y)} \left(\sum_{a \in F_2^n} (-1)^{a \cdot (x+y)} \right) = 2^{2n}.$$

$$\begin{aligned} \rho(n) &= 2^{n-1} - 2^{n/2-1} \text{ si } n \text{ pair} \\ &< 2^{n-1} - 2^{n/2-1} \text{ si } n \text{ impair.} \end{aligned}$$

On appelle *courbes* les fonctions de nonlinéarité $2^{n-1} - 2^{n/2-1}$ (n pair).

Alors $\widehat{f_\chi}(a) = \pm 2^{n/2}$ pour tout a (condition indépendante du choix du produit scalaire), et la fonction définie par $\widetilde{f}(a) = 0$ si $\widehat{f_\chi}(a) = 2^{n/2}$ et $\widetilde{f}(a) = 1$ sinon est elle-même courbe.

Une fonction est courbe si et seulement si toutes ses dérivées $f(x) + f(x + a)$ sont équilibrées : provient du fait que la transformée de Fourier de la *fonction d'autocorrélation* de f : $a \mapsto \sum_{x \in F_2^n} (-1)^{f(x)+f(x+a)}$ est égale au carré de la transformée de Walsh de f.

Beacoup de travail a été fait sur les constructions de fonctions

courbes (Maiorana, McFarland, Rothaus, Dillon, C.C., Dobbertin, Leander).

Une sous-classe, les fonctions *hyper-courbes* (Youssef-Gong ; C.C.-Gaborit) : pour tout $a \in F_2^n \equiv F_{2^n}$, pour tout i premier avec $2^n - 1$

$$\sum_{x \in F_{2^n}} (-1)^{f(x)+tr(ax^i)} = \pm 2^{n/2}$$

i.e. $f(x^i)$ courbe pour tout i premier avec $2^n - 1$.

4. toute fonction de combinaison $f(x)$ doit rester équilibrée si on fixe certaines des coordonnées x_i de x (au plus m d'entre elles). On dit alors que f est m-*résiliente*. Si f n'est pas résiliente d'ordre élevé, alors il existe une corrélation entre la sortie de f et les sorties d'un petit nombre de LFSRs. Cette corrélation permet une attaque efficace.

Caractérisation à l'aide de la transformée de Walsh :

$\widehat{f_\chi}(a) = 0$ pour tout $a \in F_2^n$ tel que $w_H(a) \leq m$.

Preuve On applique la relation $\sum_{s\in E}\widehat{\varphi}(s) = |E|\sum_{x\in E^\perp}\varphi(x)$ à la fonction numérique $\varphi(x) = f_\chi(x+b)$ et à l'espace $E = \{x \in F_2^n/\ x_i = 0,\ \forall i \notin I\}$ (dont l'orthogonal est $E^\perp = \{x \in F_2^n/\ x_i = 0,\ \forall i \in I\}$) où I est un sous-ensemble de $\{1,\ldots,n\}$ de cardinal m.

Borne sur le degré des fonctions m-résilientes (Siegenthaler) : $d \leq n - m - 1$.

Preuve : Soit g la transformée de Möbius de f :

$$g(u) = \sum_{v\leq u} f(v) \mod 2.$$

On applique la relation $\sum_{s\in E}\widehat{\varphi}(s) = |E|\sum_{x\in E^\perp}\varphi(x)$ à $\varphi = f$

et $E^{\perp} = \{v \in F_2^n \,|\, v \leq u\}$, c'est à dire : $E = \{v \in F_2^n \,|\, v \leq (u_1 + 1, \ldots, u_n + 1)\}$, on obtient :

$$g(u) = \left(2^{w_H(u)-n} \sum_{w \in E} \widehat{f}(w) \right) \mod 2. \qquad (1)$$

Si u est de poids supérieur ou égal à $n-m$, alors $(u_1+1, \ldots, u_n+1)$ est de poids inférieur ou égal à m et, f étant m-résiliente, $g(u)$ est donc égal à $2^{w_H(u)-n}\ \widehat{f}(0) \mod 2$.

Or, $\widehat{f}(0) = 2^{n-1}$. ◇

Les fonctions quadratiques $(n-3)$-résilientes ont été caractérisées et dénombrées (Camion, C.C., Charpin, Sendrier).

Une classification partielle des fonctions cubiques $(n-4)$-résilientes existe (C.C., Charoin).

Borne sur la nonlinéarité des fonctions m-résilientes (Sarkar et al.) : $\widehat{f_\chi}(u)$ est divisible par 2^{m+2} pour tout u. [*Cela implique que* $\mathcal{NL}(f)$ *est divisible par* 2^{m+1} *et donc que*

$$\mathcal{NL}(f) \leq 2^{n-1} - 2^{m+1}].$$

Preuve : soit u un vecteur de F_2^n ; d'après la relation $\sum_{s\in E}\widehat{\varphi}(s) = |E|\sum_{x\in E^\perp}\varphi(x)$ appliquée à la fonction $\varphi = f_\chi$ et à l'espace $E = \{v \in F_2^n / \ v \leq u\}$, on obtient

$$\sum_{v\in E}\widehat{f_\chi}(v) = 2^{w_H(u)}\sum_{x\in E^\perp} f_\chi(x). \tag{2}$$

On démontre la propriété de divisibilité par récurrence sur le poids de u : elle est claire pour $w_H(u) \leq m$; pour $w_H(u) = m+1$, on la déduit directement de la propriété (2), puisque la somme $\sum_{v\in E}\widehat{f_\chi}(v)$ ne contient que $\widehat{f_\chi}(u)$ et que la somme $\sum_{x\in E^\perp} f_\chi(x)$ est paire, et on continue jusqu'à $w_H(u) = n$ en appliquant toujours (2).

Si la borne $\mathcal{NL}(f) \leq 2^{n-1} - 2^{m+1}$ est atteinte par f alors la borne sur le degré l'est aussi car $\widehat{f_\chi}(a)$ est divisible par $2^{m+2+\left\lfloor \frac{n-m-2}{d} \right\rfloor}$ (C.C.).

Si n est pair et si $m \leq \frac{n}{2} - 2$ alors $\mathcal{NL}(f) \leq 2^{n-1} - 2^{n/2-1} - 2^{m+1}$.

Un exemple de fonction optimale : $f(x) = x_1x_2x_3 + x_1x_4 + x_2$

x_1	x_2	x_3	x_4	$x_1x_2x_3$	x_1x_4	$f(x)$	$(-1)^{f(x)}$				$\widehat{\chi_f}(x)$
0	0	0	0	0	0	0	1	2	4	0	0
1	0	0	0	0	0	0	1	0	0	0	0
0	1	0	0	0	0	1	-1	-2	-4	8	8
1	1	0	0	0	0	1	-1	0	0	0	8
0	0	1	0	0	0	0	1	2	0	0	0
1	0	1	0	0	0	0	1	0	0	0	0
0	1	1	0	0	0	1	-1	-2	0	0	0
1	1	1	0	1	0	0	1	0	0	0	0
0	0	0	1	0	0	0	1	0	0	0	4
1	0	0	1	0	1	1	-1	2	4	4	-4
0	1	0	1	0	0	1	-1	0	0	0	4
1	1	0	1	0	1	0	1	-2	0	4	-4
0	0	1	1	0	0	0	1	0	0	0	-4
1	0	1	1	0	1	1	-1	2	0	-4	4
0	1	1	1	0	0	1	-1	0	0	0	4
1	1	1	1	1	1	1	-1	2	-4	4	-4

TAB. 2: table de vérité et de Walsh de f

5. Un dernier critère très récent : ni f, ni $f+1$ ne doit admettre un annihilateur de bas degré (i.e. une fonction g non nulle telle que $f \star g = 0$).

Construction de Maiorana-McFarland

Pour obtenir des fonctions courbes $f_{\pi,g}(x,y) = x \cdot \pi(y) + g(y)$, (où $\pi : F_2^{n/2} \mapsto F_2^{n/2}$, $g : F_2^{n/2} \mapsto F_2$) est courbe ssi π est une permutation.

Pour obtenir des fonctions résilientes

$n = r + s$.

Soit $g : F_2^s \mapsto F_2$ et $\phi : F_2^s \mapsto F_2^r$.

Si $w_H(\phi(y)) > k, \forall y \in F_2^s$ alors la fonction :

$$f_{\phi,g}(x,y) = x \cdot \phi(y) + g(y),\ x \in F_2^r,\ y \in F_2^s$$

est m-résiliente avec $m \geq k$, car :

$$\begin{aligned}
\widehat{f_{\phi,g_\chi}}(s\,,t) &= \sum_{x\in F_2^r}\sum_{y\in F_2^{n-r}} (-1)^{x\cdot\phi(y)+g(y)+s\cdot x+t\cdot y} \\
&= \sum_{y\in F_2^{n-r}} (-1)^{g(y)+t\cdot y}\left(\sum_{x\in F_2^r}(-1)^{x\cdot(\phi(y)+s)}\right) \\
&= 2^r \sum_{y\in\phi^{-1}(s)} (-1)^{g(y)+t\cdot y}.
\end{aligned}$$

Nonlinéarité de $f_{\phi,g}$:

$A = \max_{a \in F_2^r} \#\phi^{-1}(a)$.

$$2^{n-1} - 2^{r-1}A \leq \mathcal{NL}(f_{\phi,g}) \leq 2^{n-1} - 2^{r-1}\left\lceil \sqrt{A} \right\rceil.$$

Conséquence si $f_{\phi,g}$ atteint la meilleure nonlinéarité possible $2^{n-1} - 2^{k+1}$, alors $n \leq k + 2 + \log_2(k+3)$.

Première généralisation

(C.C., CRYPTO 2002) Concaténation de fonctions quadratiques sous formes de Dickson :

Soit $n = r + s$ et $r = 2t$ ou $r = 2t + 1$.

Soit $g : F_2^s \mapsto F_2$, $\phi : F_2^s \mapsto F_2^r$ et $\psi : F_2^s \mapsto F_2^t$.

Pour $x \in F_2^r,\ y \in F_2^s$, posons

$$f_{\psi,\phi,g}(x,y) = \sum_{i=1}^{t} x_{2i-1}x_{2i}\,\psi_i(y) + x \cdot \phi(y) + g(y).$$

Deuxième généralisation

(C.C. DCC)

$f(x,y) = \prod_{i=1}^{h(y)} (x \cdot \phi_i(y) + g_i(y)) + x \cdot \phi(y) + g(y)$, où

- $\phi_1, \ldots$ et ϕ sont des fonctions de F_2^s dans F_2^r telles que, pour tout $y \in F_2^s$, les vecteurs $\phi_1(y), \ldots$ sont linéairement indépendants,
- $g_1, \ldots$ et g sont des fonctions booléennes sur F_2^s.

Ces constructions (primaires) permettent d'obtenir des fonctions en des petits nombres de variables, qui atteignent les bornes.
Des constructions secondaires existent, qui permettent d'obtenir des fonctions en des plus grands nombres de variables

T. Johansson, S. Maitra, E. Pasalic, P. Sarkar, C.C.,
Y. Tarannikov.

Immunité algébrique des fonctions booléennes

Un critère récent important : il n'existe pas g et h de bas degrés telles que $g \neq 0$ et $f \star g = h$.

Critère équivalent : il n'existe pas g de bas degré telle que $g \neq 0$ et $f \star g = 0$ (i.e. g annihilateur de f) ou $f \star g = g$ (i.e. g annihilateur de $f + 1$). L'*immunité algébrique de* f est par définition le degré minimal des fonctions $g \neq 0$ telles que $f \star g = 0$ ou $f \star g = g$.

L'immunité algébrique de f doit être suffisante pour une résistance aux attaques algébriques. Il existe une algorithme rapide pour calculer l'immunité algébrique.

L'immunité algébrique de toute fonction booléenne de n variables est majorée par $\lceil \frac{n}{2} \rceil$ (Courtois-Meier). La probabilité qu'une fonction équilibrée aléatoire admette un annihilateur de degré au plus d étant au plus :

$$\frac{(2^{n+\cdots+\binom{n}{d}}-1)\binom{2^n-2^{n-d}}{2^{n-1}-2^{n-d}}}{\binom{2^n}{2^{n-1}}}, \tag{3}$$

on a le théorème (Meier, Pasalic, C.C.) :

Soit d_n une suite d'entiers positifs tels que $d_n \leq \mu n$ où $\mu = \frac{1}{2}(1+\frac{\ln 2}{2}-\sqrt{(1+\frac{\ln 2}{2})^2-1}) \approx 0.22$. Alors

$$Pb\{\exists g \in An(f) | deg(g) \leq d_n\} \to 0,\ n \to \infty. \tag{4}$$

Améliorable avec $\mu' = \approx 0.27$

	$d = 5$	$d = 6$	$d = 7$	$d = 8$
$n; P_b$	$18; 10^{-1134}$	$22; 10^{-6326}$	$26; 10^{-23138}$	$31; 10^{-10^7}$

TAB. 3: Borne sup sur la probabilité de l'existence d'un annihilateur de degré au plus d

En fait, des arguments heuristiques (C.C., Gaborit) montrent que les fonctions équilibrées aléatoires sont d'immunités algébriques optimales ou sous-optimales. Le problème est de trouver des constructions de fonctions dont l'immunité algébrique peut être garantie.

n	d	poids	degré	nonlinearité	immunité algébrique
6	-1	32	5	24	3
7	-1	64	6	54	4
8	-1	128	7	112	4
9	-1	256	8	234	4
10	-1	512	9	480	5
11	-1	1024	10	980	5
12	-1	2048	11	1984	5
13	-1	4096	12	4006	6
14	-1	8192	13	8064	6

TAB. 4: La fonction $tr(x^{-1})$ pour $6 \leq n \leq 14$

n	d	poids	degré	nonlinearité	immunité algébrique
8	31	128	5	112	4
8	39 (Kasami)	128^*	6	114	4
9	57 (Kasami)	256	4	224	4
9	59	256	5	240	5
9	115	256	5	240	5
10	241 (Kasami)	512	5	480	5
10	362	512	5	480	5
10	31 (Dillon)	512^*	9	486	5
10	339 (Dobbertin)	512^*	9	480	5
11	315	1024	6	992	6
12	993 (Kasami)	2048^*	11	2000	6
12	63 (Dillon)	2048^*	11	2000	6
12	636	2048^*	11	2000	6
13	993 (Kasami)	4096	6	4032	6
13	939	4096^{**}	12	4030	7
14	4033 (Kasami)	8192	7	8064	7
14	127 (Dillon)	8192^{**}	13	8088	7

TAB. 5: Certaines fonctions puissances

n	r	s	d	Const.	w	m	nl	ai
8	4	4	5	b	2	2	112	3
9	5	4	5	b	3	3	224	3
9	5	4	5	a	3	2	240	4
10	5	5	6	b	3	3	480	4
10	6	4	5	a	4	3	480	4
11	6	5	6	b	4	4	960	4
11	6	5	6	a	3	2	992	5
12	6	6	7	b	4	4	$2^{11} - 2^6$	5
12	7	5	6	a	4	3	$2^{11} - 2^6$	5
13	7	6	7	a	4	3	$2^{11} - 2^6$	5
13	7	6	7	b	4	4	$2^{12} - 2^7$	5
13	8	5	6	a	5	4	$2^{12} - 2^7$	5
14	7	7	8	b	4	4	$2^{13} - 2^7$	5
14	8	6	7	b	6	6	$2^{13} - 2^8$	5
14	8	6	7	a	5	4	$2^{13} - 2^7$	5
14	8	6	7	a	5	4	$2^{13} - 2^7$	5
14	9	5	6	a	7	6	$2^{13} - 2^8$	5

TAB. 6: Certaines fonctions de Maiorana-McFarland

Une nouvelle construction (C.C., D. Dalai, Gupta, S. Maitra)

Soit : $g_0 = 0$ et pour tout $k \geq 1$:

$$g_k = (x_{2k-1}x_{2k} + 1)g_{k-1} + x_{2k-1}x_{2k}h^1_{k-1}$$

où

$$h^i_j = (x_{2j-1} + 1)(x_{2j} + 1)h^{i-1}_{j-1} + (x_{2j-1} + x_{2j})h^i_{j-1} + x_{2j-1}x_{2j}h^{i+1}_{j-1}$$

pour tout $j \geq 1$ et tout $i \geq 1$,

$h^i_0 = i$ [mod 2], pour tout $s > 0$,

$h^0_j = g_j$ pour tout $j \geq 0$.

Alors g_k est d'immunité algébrique au moins k.