Propriétés différentielles des fonctions puissances

Céline Blondeau, Anne Canteaut, Pascale Charpin

Equipe projet SECRET, INRIA, France

21 janvier 2010

Outline

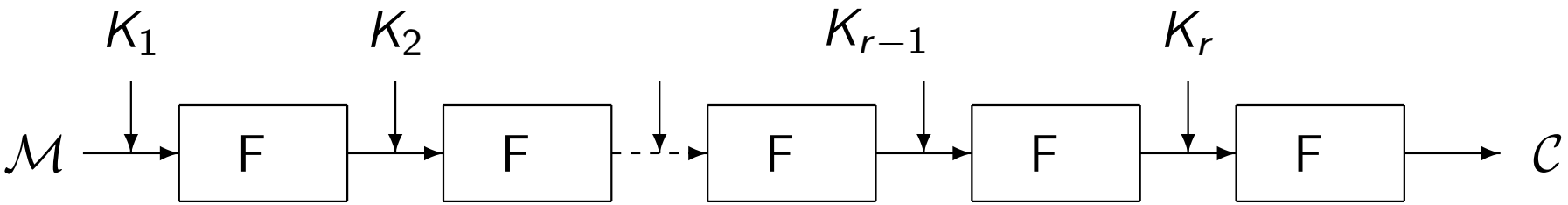
Outline

Le chiffrement par blocs

Systèmes de chiffrement par blocs : on chiffre des messages de N bits.

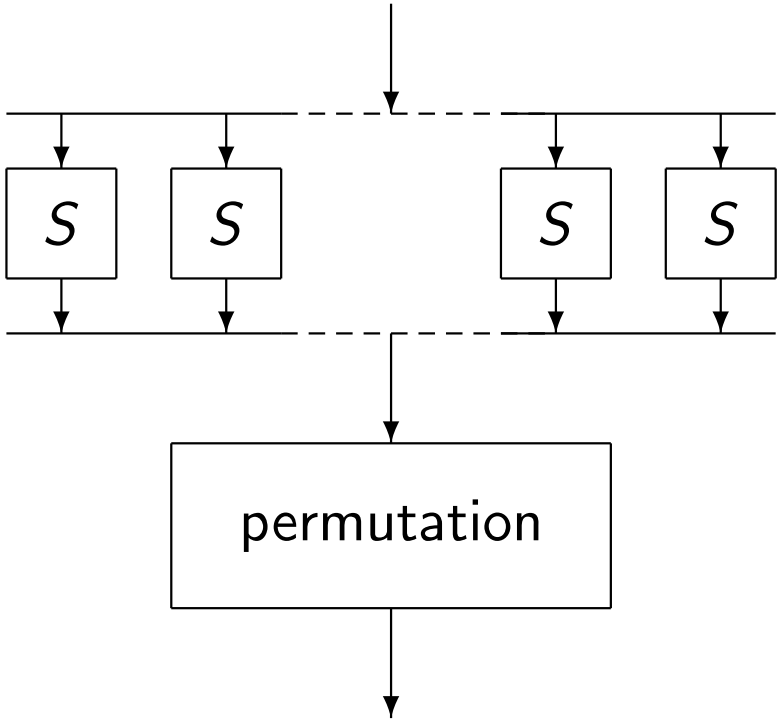
DES :Data Encryption Standard (1977)
AES :Advanced Encryption Standard (2000)
...

Chiffrement itératif

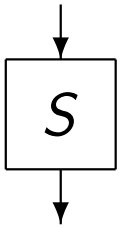


- F est appellé **fonction de tour**.
- Les clés K_i sont des **clés de tours** dérivées d'une **clé maître** K.

La fonction de tour



Les boites-S



$$S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$$

Ici $n = m$.

Plusieurs façons de définir les boites-S :

- par une table.
  $S(0) = 1, S(1) = 4, ...$
- par une permutation du corps $\mathbb{F}_{2^n}$
  $S(x) = x^d$

Les types d'attaques

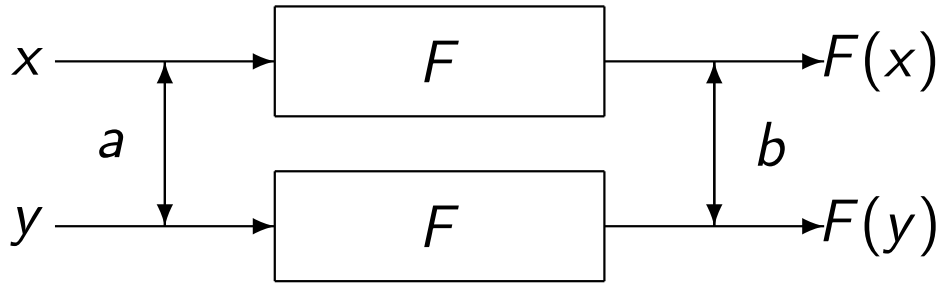
- Les attaques algébriques
  Courtois 2002

- Les attaques statistiques
  - Cryptanalyse linéaire
    Matsui 1991
  - Cryptanalyse différentielle
    Biham Shamir 1991

Une différentielle

Une **différentielle d'un système de chiffrement par bloc** est un couple $(a, b) \in (\mathbb{F}_2^n \backslash \{0\}, \mathbb{F}_2^n)$. On définit le cardinal d'une différentielle par

$$\delta(a, b) = \#\{x \in \mathbb{F}_2^n, \ \ F(x) + F(x + a) = b\}$$



La cryptanalyse différentielle

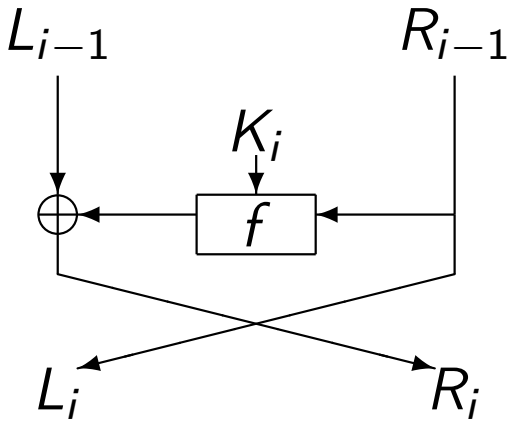
$F : \mathbb{F}_2^N \mapsto \mathbb{F}_2^N$

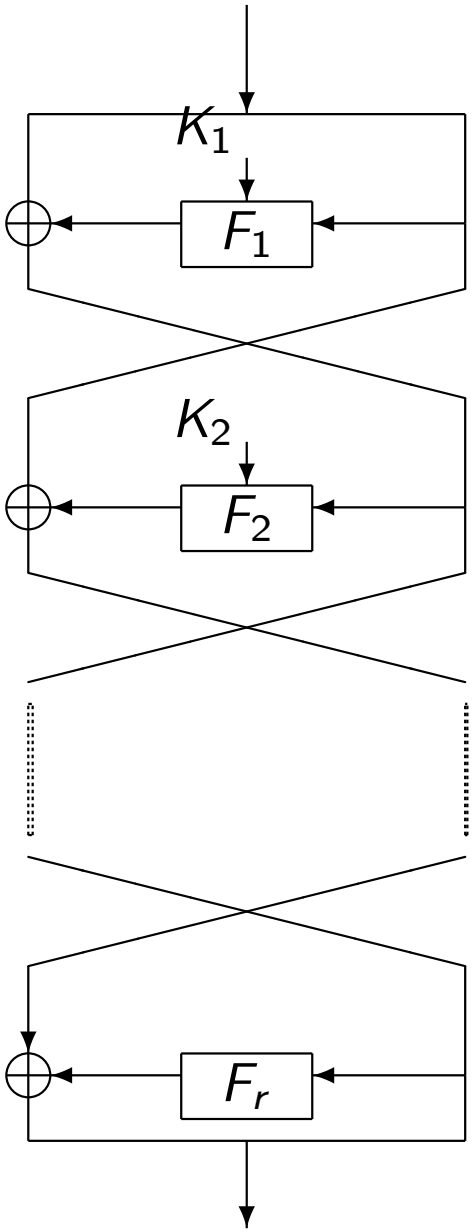
$$\delta(F) = \max_{a \neq 0, b} \delta(a, b)$$

- Probabilité uniforme d'une différentielle : $p = \frac{1}{2^N}$.
- Probabilité d'une différentielle $p* = \frac{\delta(a,b)}{2^N}$.
- Probabilité maximale d'une différentielle $p_{max} = \frac{\delta(F)}{2^N}$.

But :Trouver une différentielle avec probabilité $p* > p$
Probabilité définie par les boites S.

Chiffrement de Feistel





Critère de résistance

- f fonction de tour.
- $p_{max} = \dfrac{\delta(f)}{2^N}$

Théorème (Nyberg Knudsen 1992)

Supposons que la fonction de tour f du schéma de Feistel est une permutation et que les entrées de chaque tour sont indépendantes et uniformément aléatoires. Alors la probabilité d'une différentielle sur $r \geq 3$ tours est inférieure ou égale à p_{max}^2.

Les fonctions APN

Critère de résistance $\delta(F)$ petit.

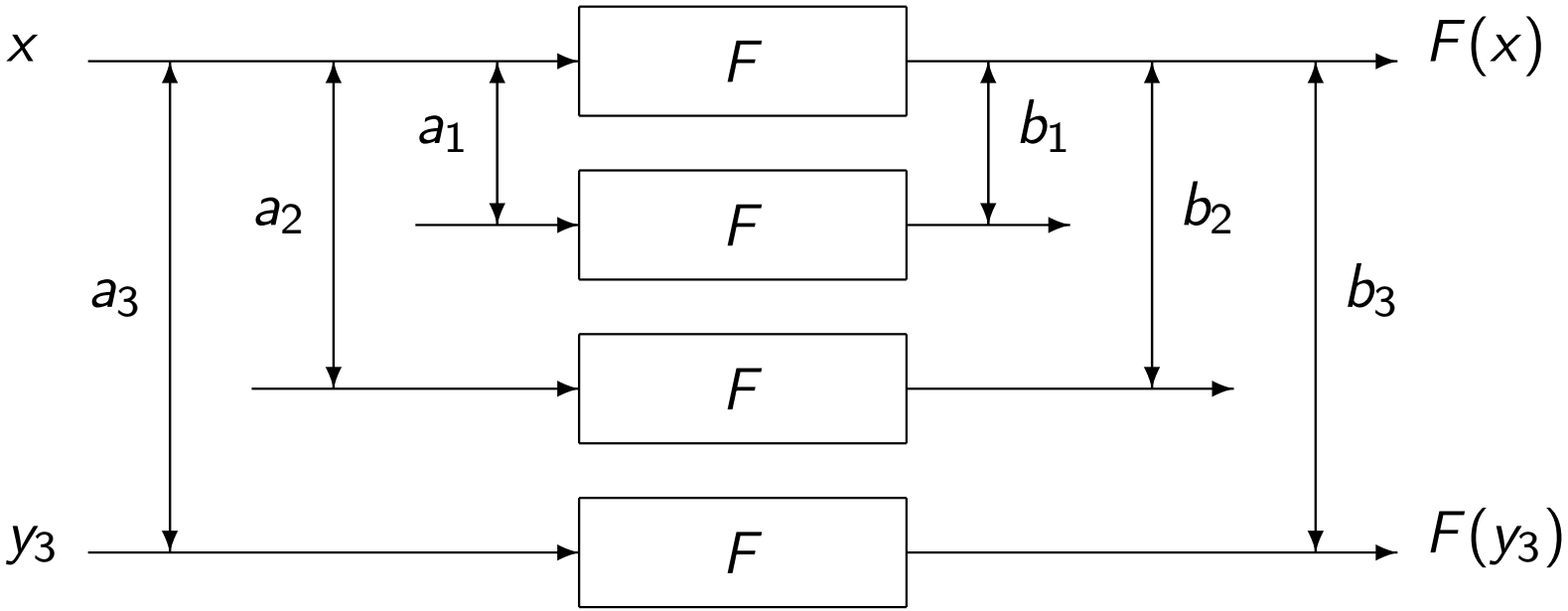
$$F(x) + F(x + a) = b$$

$\delta(a, b)$ pair.

Définition

Soit $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$. *Si* $\delta(F) = 2$ *alors on dit que* F *est* **APN (almost perfect non linear)**.

la cryptanalyse différentielle tronquée



Outline

Fonctions puissances

- Soit $\mathbb{F}_{2^n}$ le corps fini à 2^n.
- Soit $F_d(x) = x^d$ une fonction puissance.

- $\delta(a,b) = \delta(1, b/a^d)$ $\qquad\qquad$ $\delta(b) = \delta(1,b)$

$$x^d + (x+a)^d = b \Leftrightarrow a^d \left((\frac{x}{a})^d + (\frac{x}{a} + 1)^d \right) = b$$

- F_d est une permutation ssi $pgcd(d, 2^n - 1) = 1$.

$$\delta(0) = pgcd(d, 2^n - 1) - 1$$

Spectre Différentiel

$$\omega_i = \#\{b|\delta(b) = i\}$$

Spectre différentielle d'une fonction puissance :

$$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\}$$

$$\begin{cases} \omega_0 + \omega_2 + \cdots + \omega_{\delta(F)} = 2^n \\ 2 \cdot \omega_2 + 4 \cdot \omega_4 + \cdots \delta(F) \cdot \omega_{\delta(F_d)} = 2^n \end{cases}$$

F_d est APN ssi $\omega_0 = 2^{n-1}$ et $\omega_2 = 2^{n-1}$

Table des différences

$a \backslash b$	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	2	0	2	0	2	0	2
010	0	0	2	2	2	2	0	0
011	0	2	2	0	2	0	0	2
100	0	0	0	0	2	2	2	2
101	0	2	0	2	2	0	2	0
110	0	0	2	2	0	0	2	2
111	0	2	2	0	0	2	2	0

Tab.: $\delta(a, b)$ pour la fonction $F(x) = x^3$ et $n = 3$.

La fonction inverse

$$F_{2^n-2}(x) = x^{2^n-2} = \begin{cases} x^{-1} & \text{si} \quad x \neq 0 \\ 0 & \text{si} \quad x = 0 \end{cases}$$

Théorème

- *Si n est pair alors $\delta(F_{2^n-2}) = 4$ et*

$$\omega_0 = 2^{n-1} + 1 \quad \omega_2 = 2^{n-1} - 2 \quad \omega_4 = 1$$

- *Si n est impair alors $\delta(F_{2^n-2}) = 2$ et*

$$\omega_0 = 2^{n-1} \quad \omega_2 = 2^{n-1}$$

Preuve

Et on cherche les solutions de l'équation :

$$x^{-1} + (x+1)^{-1} = b \tag{1}$$

- Si $b = 1$ alors 0 et 1 sont solutions de (1).
- Si $x \neq \{0, 1\}$,(1) peut se réécrire

$$b = \frac{1}{x+1} + \frac{1}{x} \Leftrightarrow bx^2 + bx + 1 = 0$$

  qui a au plus deux solutions dans $\mathbb{F}_{2^n}$.(solutions si $Tr(1/b) = 0$)
- Donc si $b = 1$: 4 solutions dans le cas ou n est pair
  2 solutions dans le cas où n est impair.

Exemple de cryptanalyse différentielle tronquée

$a \backslash b$	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	2	0	2	0	2	0	2
010	0	0	2	2	2	2	0	0
011	0	2	2	0	2	0	0	2
100	0	0	0	0	2	2	2	2
101	0	2	0	2	2	0	2	0
110	0	0	2	2	0	0	2	2
111	0	2	2	0	0	2	2	0

Tab.: $\delta(a, b)$ pour la fonction $F(x) = x^3$ et $n = 3$.

Exemple de cryptanalyse différentielle tronquée

$a \backslash b$	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	2	0	2	0	2	0	2
010	0	0	2	2	2	2	0	0
011	0	2	2	0	**2**	0	0	**2**
100	0	0	0	0	**2**	2	2	**2**
101	0	2	0	2	2	0	2	0
110	0	0	2	2	0	0	2	2
111	0	2	2	0	0	2	2	0

Tab.: $\delta(a, b)$ pour la fonction $F(x) = x^3$ et $n = 3$.

Comparaison de spectre différentiel

$$\delta(F) = 4 \qquad \delta(G) = 4$$

$$\begin{array}{lll} \text{F} : & \omega_0 = 2^{n-1} + 1 & \omega_2 = 2^{n-1} - 2 \quad \omega_4 = 1 \\ \text{G} : & \omega_0 = 2^n - 2^{n-2} & \omega_2 = 0 \qquad\quad \omega_4 = 2^{n-2} \end{array}$$

$a \backslash b$	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	0	0	2	0	4	2	0
010	0	2	2	0	4	0	0	0
011	0	2	4	0	0	0	0	2
100	0	0	0	0	2	2	0	4
101	0	0	0	2	0	2	4	0
110	0	0	0	4	2	0	0	2
111	0	4	2	0	0	0	2	0

Comparaison de spectre différentiel

$a \backslash b$	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	4	0	0	0	4	0	0
010	0	0	4	0	4	0	0	0
011	0	4	0	0	0	0	0	4
100	0	0	0	0	0	4	4	0
101	0	0	0	0	4	0	4	0
110	0	0	0	4	0	0	0	4
111	0	0	4	4	0	0	0	0

2 fonctions qui ont la même différentiabilité n'ont pas le même spectre différentiel.

Outline

2-valués

- F_d est **différentiellement 2-valué** si $\forall b \;\; \delta(b) \in \{0, \kappa\}$.
- $\omega_0 + \omega_\kappa = 2^n$ et $\kappa\omega_\kappa = 2^n$
- Dans ce cas $\exists s$ tel que $\kappa = 2^s$.

Fonction plateau

Spectre de Walsh d'une fonction booléenne : $\{\mathcal{F}(f+\phi_a)\}$
Fonction plateau : 3 valeurs pour le spectre de Walsh.

Théorème

Soit d tel que $pgcd(d, 2^n-1)=1$. Soit $F_d(x)=x^d$ et $f(x)=Tr(x^d)$.
Supposons que f est une fonction plateau avec spectre de Walsh $\{0, \pm 2^{(n+k)/2}\}$.
Alors $\delta(F_d) \geq 2^k$ avec égalité ssi $\delta(b) \in \{0, 2^k\}$ pour tout b.
Si tout $\delta(b) \neq 0$ tel que $\delta(b) \geq 2^k$ alors $\delta(b) \in \{0, 2^k\}$

Quadratique

$$Q_t : x \mapsto x^{2^t+1} \text{ sur } \mathbb{F}_{2^n}$$

Théorème

Soit $s = pgcd(n, t)$.

$$\delta(Q_t) = 2^s \ et \ \forall b \ \delta(b) \in \{0, 2^s\}$$

$$Q_t(x) + Q_t(x+1) = b \Leftrightarrow x^{2^t} + x + b + 1 = 0$$

Si il existe une solution x de cette équation alors l'ensemble des solutions est $x + \mathbb{F}_{2^s}$.

Kasami

$$K_t : x \mapsto x^{2^{2t}-2^t+1} \text{ sur } \mathbb{F}_{2^n}$$

Théorème

Soit $s = pgcd(n, t)$. Supposons que $n \neq 3t$ et que n/s est impair. Alors

$$\delta(K_t) = 2^s \ et \ \delta(b) \in \{0, 2^s\}.$$

Si l'équation $x^d + (x+1)^d = b$ a une solution x alors l'ensemble des solutions est $(y + a\mathbb{F}_{2^s})^{2^t+1}$ où $x = y^{2^t+1}$ et $x + 1 = (y + a)^{2^t+1}$.

Preuve

On a $2^{3t}+1=(2^t+1)(2^{2t}-2^t+1)$.

$$x^{2^{2t}-2^t+1}+(x+1)^{2^{2t}-2^t+1}=b \tag{2}$$

Changement de variable : $x=y^{2^t+1}$ et $(x+1)=(y+a)^{2^t+1}$

$$y^{2^{3t}+1}+(y+a)^{2^{3t}+1}=b$$

Soit $k=pgcd(3t,n)$ si y est solution alors $y+a\mathbb{F}_{2^k}$ est solution.
Vérifier que $\forall\beta\in\mathbb{F}_{2^s}$ on a $(y+\beta a)^{2^t+1}$ est solution de (2).

Conjecture

Conjecture

Toute les permutations puissances $F_d(x) = x^d$ qui ont un spectre différentiel 2 valué sont telles que d est à équivalence près un exposant Quadratique ou un exposent Kasami.

n	$\delta(F) = 4$	$\delta(F) = 8$	$\delta(F) = 16$	$\delta(F) = 32$	$\delta(F) = 64$
$n = 2^m$	X	X	X	X	X
$n = p^m$	X	$p \neq 3$	$p \neq 7$	$p \neq 3, 5$	$p \neq 31$
$n = 2p^m$	X	$p \neq 5$	$p \neq 3, 11$	$p \neq 7, 23$	$p \neq 3, 5, 47$

Tab.: Liste d'exposants pour lesquels il n'existe pas de permutations différentiellement 2-valués

Outline

Permutations différentiellement 4 et 6 uniforme

Soit F_d tel que $\delta(F_d) \leq 6$.

- Si n est impair. F_d est une permutation si
  - $\delta(F_d) \leq 4$
  - $\delta(F_d) = 6$ avec $pgcd(3, n) = 1$

  Quand $pgcd(3, n) = 3$ et $\delta(F_d) = 6$ soit 7 divise d soit F_d est une permutation.
- Si $n = 2m$ avec m impair. Si $pgcd(3, d) = 1$ alors $\delta(F_d) \in \{4, 6\}$, $\delta(1) = 4$ et
  - Si $\delta(F_d) = 4$ alors F_d est une permutation.
  - Si $\delta(F_d) = 6$ et $pgcd(3, n) = 1$ alors F_d est une permutation.

  Quand $pgcd(3, n) = 3$ et $\delta(F_d) = 6$ soit 7 divise d soit F_d est une permutation.

$d = 7$

Theorem

Soit $F_7 : x \mapsto x^7$ *sur* $\mathbb{F}_{2^n}$. *On a* $\delta(F_7) = 6$.

- *Si n est impair,*

$$\omega_6 = \frac{2^n+1}{24} - \frac{1}{8}\left(\frac{1-i\sqrt{7}}{2}\right)^n - \frac{1}{8}\left(\frac{1+i\sqrt{7}}{2}\right)^n$$

$$\omega_4 = 0 \qquad \omega_2 = 2^{n-1} - 3\omega_6 \qquad \omega_0 = 2^{n-1} + 2\omega_6$$

- *Si n est pair :*

$$\omega_6 = \frac{2^n-13}{24} - \frac{1}{8}\left(\frac{1-i\sqrt{7}}{2}\right)^n - \frac{1}{8}\left(\frac{1+i\sqrt{7}}{2}\right)^n$$

$$\omega_4 = 1 \qquad \omega_2 = 2^{n-1} - 3\omega_6 - 2 \qquad \omega_0 = 2^{n-1} + 2\omega_6 + 1.$$

Permutations différentiellement 4-uniforme (1)

n	exposant/inverse	ω_0	ω_2	ω_4	
6	5/13	48	0	16	Quadratic/Kasami
	31/31	33	30	1	Inverse
7	19/47	85	22	21	
8	127/127	129	126	1	Inverse
9	45/125	292	184	36	
10	5/205	768	0	256	Quadratic
	13/79	768	0	256	Kasami
	17/181	768	0	256	Quadratic
	29/247	573	390	61	
	103/149	588	360	76	
	223/367	603	330	91	
	511/511	513	510	1	Inverse
11	79/183	1156	760	132	
	109/695	1189	694	165	
	251/367	1255	562	231	
	463/703	1222	628	198	

Permutation différentiellement 4-uniforme (2)

n	exposant/inverse	ω_0	ω_2	ω_4	
12	73/731	2496	1152	448	Bracken and Leander
	2047/2047	2049	2046	1	Inverse
13	303/947	4603	3082	507	
14	5/3277	12288	0	4096	Quadratic
	13/1339	12288	0	4096	Kasami
	17/2893	12288	0	4096	Quadratic
	65/2773	12288	0	4096	Quadratic
	205/241	12288	0	4096	Kasami
	319/979	12288	0	4046	Kasami (4033)
	8191/8191	8193	8190	1	Inverse
16	32767/32767	32769	32766	1	Inverse
18	5/52429	196608	0	65536	Quadratic
	13/20165	196608	0	65536	Kasami
	17/46261	196608	0	65536	Quadratic
	241/12101	196608	0	65536	Kasami
	257/43861	196608	0	65536	Quadratic

Permutation différentiellement 4-uniforme (3)

n	exposant/inverse	ω_0	ω_2	ω_4	
18	1279/12605	196608	0	65536	Kasami (65281)
	131071/131071	131073	131070	1	Inverse
20	1057/306539	651264	270336	126976	Bracken and Leander
	524287/524287	524289	524286	1	Inverse
22	5/838861	3145728	0	1048576	Quadratic
	13/322639	3145728	0	1048576	Kasami
	17/740173	3145728	0	1048576	Quadratic
	65/709813	3145728	0	1048576	Quadratic
	241/87019	3145728	0	1048576	Kasami
	257/734419	3145728	0	1048576	Quadratic
	1025/699733	3145728	0	1048576	Quadratic
	3277/16639	3145728	0	1048576	Kasami (65281)
	4033/246739	3145728	0	1048576	Kasami
	5119/49981	3145728	0	1048576	Kasami (1047553)
	2097151/2097151	2097153	2097150	1	Inverse
24	8388607/8388607	8388609	8388606	1	Inverse

Questions ouvertes

- Existe t'il des permutations puissances differentiellement 4 uniforme pour n impair $n > 13$.
- Existe t'il des fonctions différentiellement 2-valués différentes des Quadratique et des Kasami ?
- Quelles sont les meilleures fonctions pour les boites S ?