Une nouvelle étape vers la classification des fonctions APN

Florian Caullery

Institut Mathématiques de Luminy
Aix-Marseille Université

Journées C2, 2012

Outline

Institut de Mathématiques de Luminy

Fonctions booléennes vectorielles

- Une **fonction booléenne vectorielle** est une fonction $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$
- f admet une **représentation en polynôme d'une seule variable unique**.

Institut de Mathématiques de Luminy

Fonctions booléennes vectorielles

- Une **fonction booléenne vectorielle** est une fonction $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$
- f admet une **représentation en polynôme d'une seule variable unique**.

Institut de Mathématiques de Luminy

Fonctions APN (K. Nyberg)

- Les fonctions vectorielles booléennes sont les **S-Boxes** dans les systèmes de **chiffrement par blocs**.
- On étudie leur résistance à la **cryptanalyse différentielle**.
- Les fonctions **Almost Perfectly Nonlinear (APN)** ont la meilleure résistance à cette attaque. (K. Nyberg).

Institut de Mathématiques de Luminy

Fonctions APN (K. Nyberg)

- Les fonctions vectorielles booléennes sont les **S-Boxes** dans les systèmes de **chiffrement par blocs**.
- On étudie leur résistance à la **cryptanalyse différentielle**.
- Les fonctions **Almost Perfectly Nonlinear (APN)** ont la meilleure résistance à cette attaque. (K. Nyberg).

Institut de Mathématiques de Luminy

Fonctions APN (K. Nyberg)

- Les fonctions vectorielles booléennes sont les **S-Boxes** dans les systèmes de **chiffrement par blocs**.
- On étudie leur résistance à la **cryptanalyse différentielle**.
- Les fonctions **Almost Perfectly Nonlinear (APN)** ont la meilleure résistance à cette attaque. (K. Nyberg).

Institut de Mathématiques de Luminy

Fonctions APN (K. Nyberg)

- Soit $q = 2^m$ et $f : \mathbb{F}_q \to \mathbb{F}_q$:
  La résistance de f à la cryptanalyse différentielle est mesurée par le nombre de solutions dans $\mathbb{F}_q$ de

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

  $\forall a, b \in \mathbb{F}_q, a \neq 0$.
- Plus ce nombre est petit, plus la résistance de f est grande. Il est évidemment non nul et pair donc sa plus petite valeur est 2.

Institut de Mathématiques de Luminy

Fonctions APN (K. Nyberg)

- Soit $q = 2^m$ et $f : \mathbb{F}_q \to \mathbb{F}_q$:
  La résistance de f à la cryptanalyse différentielle est mesurée par le nombre de solutions dans $\mathbb{F}_q$ de

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

  $\forall a, b \in \mathbb{F}_q, a \neq 0$.
- Plus ce nombre est petit, plus la résistance de f est grande. Il est évidemment non nul et pair donc sa plus petite valeur est 2.

Institut de Mathématiques de Luminy

Fonctions APN (K. Nyberg)

Definition

Une fonction f est dite **Presque Parfaitement Non-linéaire (APN)** si pour tout $a \neq 0 \in \mathbb{F}_q$ et $b \in \mathbb{F}_q$, il existe au plus 2 éléments de $\mathbb{F}_q$ tels que

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

Institut de Mathématiques de Luminy

Outline

Institut de Mathématiques de Luminy

Fonctions puissances APN

- On considère les fonctions qui s'écrivent $f(x) = x^d$.
  f est APN si :
  - $d = 2^i + 1$ et pgcd$(i, m) = 1$ - **Fonctions Gold** .
  - $d = 2^{2i} - 2^i + 1$ et pgcd$(i, m) = 1$ - **Fonctions Kasami**.
  - Il y a d'autres exemples où d dépend de m.
- F. Hernando and G. McGuire ont donné le premier théorème de classification :

Théorème (F. Hernando, G. McGuire, 2009)

Les fonctions Gold et Kasami sont les seuls fonctions **monômiales** avec d impair qui sont APN sur une infinité d'extension de $\mathbb{F}_q$.

Mathématiques de Luminy

Fonctions puissances APN

- On considère les fonctions qui s'écrivent $f(x) = x^d$.
  f est APN si :
  - $d = 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Gold** .
  - $d = 2^{2i} - 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Kasami**.
  - Il y a d'autres exemples où d dépend de m.
- F. Hernando and G. McGuire ont donné le premier théorème de classification :

Théorème (F. Hernando, G. McGuire, 2009)

Les fonctions Gold et Kasami sont les seuls fonctions **monômiales** avec d impair qui sont APN sur une infinité d'extension de $\mathbb{F}_q$.

Mathématiques de Luminy

Fonctions puissances APN

- On considère les fonctions qui s'écrivent $f(x) = x^d$.
  f est APN si :
  - $d = 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Gold** .
  - $d = 2^{2i} - 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Kasami**.
  - Il y a d'autres exemples où d dépend de m.
- F. Hernando and G. McGuire ont donné le premier théorème de classification :

Théorème (F. Hernando, G. McGuire, 2009)

Les fonctions Gold et Kasami sont les seuls fonctions **monômiales** avec d impair qui sont APN sur une infinité d'extension de $\mathbb{F}_q$.

Mathématiques de Luminy

Fonctions puissances APN

- On considère les fonctions qui s'écrivent $f(x) = x^d$.
  f est APN si :
  - $d = 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Gold** .
  - $d = 2^{2i} - 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Kasami**.
  - Il y a d'autres exemples où d dépend de m.
- F. Hernando and G. McGuire ont donné le premier théorème de classification :

Théorème (F. Hernando, G. McGuire, 2009)

Les fonctions Gold et Kasami sont les seuls fonctions **monômiales** avec d impair qui sont APN sur une infinité d'extension de $\mathbb{F}_q$.

Mathématiques de Luminy

Fonctions puissances APN

- On considère les fonctions qui s'écrivent $f(x) = x^d$.
  f est APN si :
  - $d = 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Gold** .
  - $d = 2^{2i} - 2^i + 1$ et pgcd(i, m) = 1 - **Fonctions Kasami**.
  - Il y a d'autres exemples où d dépend de m.
- F. Hernando and G. McGuire ont donné le premier théorème de classification :

Théorème (F. Hernando, G. McGuire, 2009)

Les fonctions Gold et Kasami sont les seuls fonctions **monômiales** avec d impair qui sont APN sur une infinité d'extension de $\mathbb{F}_q$.

Mathématiques de Luminy

Conjecture sur les polynômes APN

Notre but est de montrer la conjecture suivante :

Conjecture (Y. Aubry, G. McGuire, F. Rodier)

Les fonctions Gold et Kasami sont (à équivalence près) les seules fonctions APN sur une infinité d'extension de $\mathbb{F}_q$.

Institut de Mathématiques de Luminy

Equivalence de Carlet Charpin Zinoviev

On considère f et $g : \mathbb{F}_q \to \mathbb{F}_q$.

Définition

On dit que f et g sont CCZ-équivalentes si il existe une permutation q-affine $L : \mathbb{F}_q \to \mathbb{F}_q$ telle que $L(G_g) = G_f$ où G_f et G_g sont respectivement les graphes de f et g.

f est APN si et seulement si g est APN.

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

- Soit $f(x) \in \mathbb{F}_q[x]$.
- On considère le polynôme suivant :

$$\phi(x,y,z) = \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}$$

- Et la surface X d'équation $\phi(x,y,z) = 0$

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

- Soit $f(x) \in \mathbb{F}_q[x]$.
- On considère le polynôme suivant :

$$\phi(x,y,z) = \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}$$

- Et la surface X d'équation $\phi(x,y,z) = 0$

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

- Soit $f(x) \in \mathbb{F}_q[x]$.
- On considère le polynôme suivant :

$$\phi(x,y,z) = \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}$$

- Et la surface X d'équation $\phi(x,y,z) = 0$

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

Résultat principal (F. Rodier, 2009)

Si la surface X associée à f possède une composante irréductible définie sur $\mathbb{F}_q$ alors f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$.

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

Théorème 1 (Y. Aubry, G. McGuire, F. Rodier, 2010)

Si le degré d'une fonction polynômiale f est impair et pas un exposant de **Gold** ou de **Kasami** alors f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$.

Theorem 2 (Y. Aubry, G. McGuire, F. Rodier, 2010)

Si le degré d'une fonction polynômiale f est égale à $2e$ avec e impair et si f contient un terme de degré impair, alors f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$.

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

Théorème 1 (Y. Aubry, G. McGuire, F. Rodier, 2010)

Si le degré d'une fonction polynômiale f est impair et pas un exposant de **Gold** ou de **Kasami** alors f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$.

Theorem 2 (Y. Aubry, G. McGuire, F. Rodier, 2010)

Si le degré d'une fonction polynômiale f est égale à $2e$ avec e impair et si f contient un terme de degré impair, alors f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$.

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

Théorème 3 (F. Rodier, 2011)

Si le degré d d'une fonction polynômiale f est pair et tel que $d = 4e$ avec $e \equiv 3(mod 4)$, et si un polynôme de la forme

$$(x+y)(x+z)(y+z)+c_1(x^2+y^2+z^2)+c_2(xy+xz+yz)+b(x+y+z)+d$$

$c_1, c_2, b \in \mathbb{F}_{q^3}$, ne divise pas ϕ, alors f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$.

Institut de Mathématiques de Luminy

Résultats sur les fonctions polynômiales APN

Théorème 4 (F. Rodier, 2011)

Si le degré d'une fonction polynômiale f est égale à 12 alors :
soit f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$,
soit f est CCZ-équivalente à la fonction Gold x^3.

Institut de Mathématiques de Luminy

Résumé

d = 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, . . .

Institut de Mathématiques de Luminy

Résumé

d = ~~3~~, 4, ~~5~~, 6, ~~7~~, 8, ~~9~~, 10, ~~11~~, 12, ~~13~~, 14, ~~15~~, 16, ~~17~~, 18, ~~19~~, 20, ~~21~~ . . .
Le théorème 1 traite les cas où d est impair.

Institut de Mathématiques de Luminy

Résumé

d = ~~3~~, 4, ~~5~~, ~~6~~, ~~7~~, 8, ~~9~~, ~~10~~, ~~11~~, 12, ~~13~~, ~~14~~, ~~15~~, 16, ~~17~~, ~~18~~, ~~19~~, 20, ~~21~~ . . .
Le théorème 2 traite les cas où $d = 2e$ avec e impair.

Institut de Mathématiques de Luminy

Résumé

d = ~~3~~, 4, ~~5~~, ~~6~~, ~~7~~, 8, ~~9~~, ~~10~~, ~~11~~, ~~12~~, ~~13~~, ~~14~~, ~~15~~, 16, ~~17~~, ~~18~~, ~~19~~, 20, ~~21~~ ...
Le théorème 3 traite les cas où $d = 4e$ avec $\equiv 3(mod 4)$.

Institut de Mathématiques de Luminy

Outline

Institut de Mathématiques de Luminy

Première étape - Introduction

- Dans notre cas $d = 4e$ avec $e \equiv 1 mod(4)$.
- L'adaptation de la preuve du cas où $e \equiv 3 mod(4)$ est impossible. ϕ_e (le polynôme ϕ associé à x^e) **n'est pas irréductible**.
- Utilisation des diviseurs sur la surface X et de la symétrie en x, y, z.

Institut de Mathématiques de Luminy

Première étape - Introduction

- Dans notre cas $d = 4e$ avec $e \equiv 1 mod(4)$.
- L'adaptation de la preuve du cas où $e \equiv 3 mod(4)$ est impossible. ϕ_e (le polynôme ϕ associé à x^e) **n'est pas irréductible**.
- Utilisation des diviseurs sur la surface X et de la symétrie en x, y, z.

Institut de Mathématiques de Luminy

Première étape - Introduction

- Dans notre cas $d = 4e$ avec $e \equiv 1 mod(4)$.
- L'adaptation de la preuve du cas où $e \equiv 3 mod(4)$ est impossible. ϕ_e (le polynôme ϕ associé à x^e) **n'est pas irréductible**.
- Utilisation des diviseurs sur la surface X et de la symétrie en x, y, z.

Institut de Mathématiques de Luminy

Première étape - Théorème

Théorème 5. (F.C. , F. Rodier)

Si le degré d'une fonction polynômiale de $\mathbb{F}_q$ est égale à 20 et si l'un des deux polynômes suivant ne divise pas ϕ, alors f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$:

$$\phi_5 + a(x+y+z) + b$$

ou

$$(x+y)(x+z)(y+z)+c_1(x^2+y^2+z^2)+c_2(xy+xz+yz)+b(x+y+z)+d$$

avec $a, b, c_1, c_2, d \in \mathbb{F}_{q^3}$.

Première étape - Conditions nécessaires

2 formes possibles pour f :

- $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
- $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + q_2(c_1)a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.

Institut de Mathématiques de Luminy

Première étape - Conditions nécessaires

2 formes possibles pour f :

- $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
- $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + q_2(c_1)a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.

Institut de Mathématiques de Luminy

Première étape - Conditions nécessaires

2 formes possibles pour f :

- $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
- $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + q_2(c_1)a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.

Institut de Mathématiques de Luminy

Seconde étape - Prouver la CCZ équivalence à x^5

- Premier cas : $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
  $f_1 = L(x^5)$ où $L(x) = x^4 + a_{10}x^2 + a_5x$ est une permutation affine sur $\mathbb{F}_q$.
- Second cas :
  $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + a_{17}a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.
  - Prouver que $f_2 = L(x)^5$.
  - On utilise le fait que "f n'a pas de composante irréductible défini $\mathbb{F}_q$" pour obtenir $a_{12} = q_1(c_1)^4$.
  - Conclusion $f_2 = L(x)^5$.

Institut de Mathématiques de Luminy

Seconde étape - Prouver la CCZ équivalence à x^5

- Premier cas : $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
  $f_1 = L(x^5)$ où $L(x) = x^4 + a_{10}x^2 + a_5x$ est une permutation affine sur $\mathbb{F}_q$.
- Second cas :
  $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + a_{17}a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.
  - Prouver que $f_2 = L(x)^5$.
  - On utilise le fait que "f n'a pas de composante irréductible défini $\mathbb{F}_q$" pour obtenir $a_{12} = q_1(c_1)^4$.
  - Conclusion $f_2 = L(x)^5$.

Institut de Mathématiques de Luminy

Seconde étape - Prouver la CCZ équivalence à x^5

- Premier cas : $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
  $f_1 = L(x^5)$ où $L(x) = x^4 + a_{10}x^2 + a_5x$ est une permutation affine sur $\mathbb{F}_q$.
- Second cas :
  $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + a_{17}a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.
  - Prouver que $f_2 = L(x)^5$.
  - On utilise le fait que "f n'a pas de composante irréductible défini $\mathbb{F}_q$" pour obtenir $a_{12} = q_1(c_1)^4$.
  - Conclusion $f_2 = L(x)^5$.

Institut de Mathématiques de Luminy

Seconde étape - Prouver la CCZ équivalence à x^5

- Premier cas : $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
  $f_1 = L(x^5)$ où $L(x) = x^4 + a_{10}x^2 + a_5x$ est une permutation affine sur $\mathbb{F}_q$.
- Second cas :
  $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + a_{17}a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.
  - Prouver que $f_2 = L(x)^5$.
  - On utilise le fait que "f n'a pas de composante irréductible défini $\mathbb{F}_q$" pour obtenir $a_{12} = q_1(c_1)^4$.
  - Conclusion $f_2 = L(x)^5$.

Institut de Mathématiques de Luminy

Seconde étape - Prouver la CCZ équivalence à x^5

- Premier cas : $f_1 = x^{20} + a_{10}x^{10} + a_5x^5$.
  $f_1 = L(x^5)$ où $L(x) = x^4 + a_{10}x^2 + a_5x$ est une permutation affine sur $\mathbb{F}_q$.
- Second cas :
  $f_2 = x^{20} + q_1(c_1)x^{18} + q_2(c_1)x^{17} + a_{12}x^{12} + q_1(c_1)^4a_{12}x^{10} + a_{17}a_{12}x^9 + a_8x^8 + q_1(c_1)q_2(c_1)^4x^6 + q_1(c_1)^5x^5 + a_{12} + q_1(c_1)^4$.
  - Prouver que $f_2 = L(x)^5$.
  - On utilise le fait que "f n'a pas de composante irréductible défini $\mathbb{F}_q$" pour obtenir $a_{12} = q_1(c_1)^4$.
  - Conclusion $f_2 = L(x)^5$.

Institut de Mathématiques de Luminy

Seconde étape - Théorème

Théorème (F.C, F. Rodier)

Si le degré d'une fonction polynômiale f est égale à 20 alors :
soit f n'est pas APN sur une infinité d'extension de $\mathbb{F}_q$,
soit f est CCZ-équivalente à la fonction Gold x^5.

Institut de Mathématiques de Luminy

Outline

Institut de Mathématiques de Luminy

Résumé

- La classification des fonctions puissance APN est terminée.
- la classification des functions polynômiales APN est récente et incomplète.
- On ne dispose pas de méthode simple pour la classification.

Institut de Mathématiques de Luminy

Résumé

- La classification des fonctions puissance APN est terminée.
- la classification des functions polynômiales APN est récente et incomplète.
- On ne dispose pas de méthode simple pour la classification.

Institut de Mathématiques de Luminy

Résumé

- La classification des fonctions puissance APN est terminée.
- la classification des functions polynômiales APN est récente et incomplète.
- On ne dispose pas de méthode simple pour la classification.

Institut de Mathématiques de Luminy

Travaux en cours

- Généraliser le théorème 5. aux degrés supérieurs ($d \equiv 1 (mod 4)$).
- Trouver une méthode plus simple pour dresser la liste de toute les fonctions APN d'un degré donné et prouver leur CCZ-équivalence aux fonctions Gold et Kasami.
- Prouver la conjecture

Institut de Mathématiques de Luminy

Travaux en cours

- Généraliser le théorème 5. aux degrés supérieurs ($d \equiv 1 (mod 4)$).
- Trouver une méthode plus simple pour dresser la liste de toute les fonctions APN d'un degré donné et prouver leur CCZ-équivalence aux fonctions Gold et Kasami.
- Prouver la conjecture

Institut de Mathématiques de Luminy

Travaux en cours

- Généraliser le théorème 5. aux degrés supérieurs ($d \equiv 1 (mod 4)$).
- Trouver une méthode plus simple pour dresser la liste de toute les fonctions APN d'un degré donné et prouver leur CCZ-équivalence aux fonctions Gold et Kasami.
- Prouver la conjecture

Institut de Mathématiques de Luminy

Informations

Florian Caullery
Fonctions booléennes cryptographiquement robustes
sous la direction de F. Rodier.
Financement de la région Provence-Alpes-Côte d'Azur.

Institut Mathématiques de Luminy
Aix Marseille Université
www.iml.univ-mrs.fr

Contact : florian.caullery@etu.univ-amu.fr