Fonctions Parfaitement Non Linéaires & Actions de Groupe

Laurent Poinsot

Laboratoire Systèmes Navals Complexes
Université du Sud Toulon-Var (France)

15 janvier 2007

Introduction

Soient G et H deux groupes finis. Une application $f : G \to H$ est dite parfaitement non linéaire (PN en abrégé) (ou *planaire*) si pour chaque α non nul dans G et chaque $\beta \in H$,

$$|\{x \in G | f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Définissons l'application $\sigma_\alpha : G \to G$ par $x \mapsto \alpha + x$. L'équation précédente peut naturellement être ré-écrite sous la forme suivante :

$$|\{x \in G | f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Introduction

Soient G et H deux groupes finis. Une application $f : G \to H$ est dite parfaitement non linéaire (PN en abrégé) (ou *planaire*) si pour chaque α non nul dans G et chaque $\beta \in H$,

$$|\{x \in G | f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Définissons l'application $\sigma_\alpha : G \to G$ par $x \mapsto \alpha + x$. L'équation précédente peut naturellement être ré-écrite sous la forme suivante :

$$|\{x \in G | f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Introduction

Soient G et H deux groupes finis. Une application $f : G \to H$ est dite parfaitement non linéaire (PN en abrégé) (ou *planaire*) si pour chaque α non nul dans G et chaque $\beta \in H$,

$$|\{x \in G | f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|} \ .$$

Définissons l'application $\sigma_\alpha : G \to G$ par $x \mapsto \alpha + x$. L'équation précédente peut naturellement être ré-écrite sous la forme suivante :

$$|\{x \in G | f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|} \ .$$

Introduction

Soient maintenant G et H deux groupes finis et X un ensemble fini non vide sur lequel G agit. Une application $f : X \to H$ est G-parfaitement non linéaire si pour chaque g non nul dans G et pour chaque $\beta \in H$,

$$|\{x \in X | f(g.x) - f(x) = \beta\}| = \frac{|X|}{|H|} .$$

Plan

Plan

1. Attaques Différentielle & Linéaire
   - Principes de la cryptographie
   - Principes de cryptanalyse
2. Approche traditionnelle
   - Non linéarité parfaite
   - Fonctions courbes
   - Ensembles à différences
3. Non linéarité parfaite au sens des actions de groupe
   - Actions de groupe
   - G-non linéarité parfaite
4. Constructions de fonctions booléennes courbes impossibles
   - Longueur impaire
   - Cas planaire

Plan

1. Attaques Différentielle & Linéaire
   - Principes de la cryptographie
   - Principes de cryptanalyse
2. Approche traditionnelle
   - Non linéarité parfaite
   - Fonctions courbes
   - Ensembles à différences
3. Non linéarité parfaite au sens des actions de groupe
   - Actions de groupe
   - G-non linéarité parfaite
4. Constructions de fonctions booléennes courbes impossibles
   - Longueur impaire
   - Cas planaire

Plan

Plan

Principe du chiffrement

Alice souhaite envoyer un message confidentiel m à *Bob* sur un canal public (ex. voie postale, les ondes hertziennes, Internet, *etc.*).

Dans cette situation ils doivent utiliser un cryptosystème (ou *procédé de chiffrement*) qui consiste en :

- Un algorithme de chiffrement E ;
- Un algorithme de déchiffrement D ;
- Un ensemble de clefs de chiffrement et un ensemble de clefs de déchiffrement (possiblement différents) ;
- Pour chaque clef de chiffrement k il y a une clef de déchiffrement notée k^{-1} (non nécessairement unique) telle que pour chaque message clair m

$$\texttt{Si } c{:=}E(m,k) \texttt{ alors } m{=}D(c,k^{-1}) \texttt{ .}$$

Principe du chiffrement

Alice souhaite envoyer un message confidentiel m à *Bob* sur un canal public (ex. voie postale, les ondes hertziennes, Internet, *etc.*).
Dans cette situation ils doivent utiliser un cryptosystème (ou *procédé de chiffrement*) qui consiste en :

- Un algorithme de chiffrement E ;
- Un algorithme de déchiffrement D ;
- Un ensemble de clefs de chiffrement et un ensemble de clefs de déchiffrement (possiblement différents) ;
- Pour chaque clef de chiffrement k il y a une clef de déchiffrement notée k^{-1} (non nécessairement unique) telle que pour chaque message clair m

$$\texttt{Si } c := E(m, k) \texttt{ alors } m = D(c, k^{-1}) \texttt{ .}$$

Principe du chiffrement

Alice souhaite envoyer un message confidentiel m à *Bob* sur un canal public (ex. voie postale, les ondes hertziennes, Internet, *etc.*).
Dans cette situation ils doivent utiliser un cryptosystème (ou *procédé de chiffrement*) qui consiste en :

- Un algorithme de chiffrement E ;
- Un algorithme de déchiffrement D ;
- Un ensemble de clefs de chiffrement et un ensemble de clefs de déchiffrement (possiblement différents) ;
- Pour chaque clef de chiffrement k il y a une clef de déchiffrement notée k^{-1} (non nécessairement unique) telle que pour chaque message clair m

$$\texttt{Si } c := E(m,k) \texttt{ alors } m = D(c,k^{-1}) \; .$$

Principe du chiffrement

Alice souhaite envoyer un message confidentiel m à *Bob* sur un canal public (ex. voie postale, les ondes hertziennes, Internet, *etc.*).

Dans cette situation ils doivent utiliser un cryptosystème (ou *procédé de chiffrement*) qui consiste en :

- Un algorithme de chiffrement E ;
- Un algorithme de déchiffrement D ;
- Un ensemble de clefs de chiffrement et un ensemble de clefs de déchiffrement (possiblement différents) ;
- Pour chaque clef de chiffrement k il y a une clef de déchiffrement notée k^{-1} (non nécessairement unique) telle que pour chaque message clair m

$$\texttt{Si } c := E(m, k) \texttt{ alors } m = D(c, k^{-1}) \ .$$

Principe du chiffrement

Alice souhaite envoyer un message confidentiel m à *Bob* sur un canal public (ex. voie postale, les ondes hertziennes, Internet, *etc.*).
Dans cette situation ils doivent utiliser un cryptosystème (ou *procédé de chiffrement*) qui consiste en :

- Un algorithme de chiffrement E ;
- Un algorithme de déchiffrement D ;
- Un ensemble de clefs de chiffrement et un ensemble de clefs de déchiffrement (possiblement différents) ;
- Pour chaque clef de chiffrement k il y a une clef de déchiffrement notée k^{-1} (non nécessairement unique) telle que pour chaque message clair m

$$\texttt{Si } c := E(m,k) \texttt{ alors } m = D(c, k^{-1}) .$$

Principe du chiffrement

Alice souhaite envoyer un message confidentiel m à *Bob* sur un canal public (ex. voie postale, les ondes hertziennes, Internet, *etc.*).
Dans cette situation ils doivent utiliser un cryptosystème (ou *procédé de chiffrement*) qui consiste en :

- Un algorithme de chiffrement E ;
- Un algorithme de déchiffrement D ;
- Un ensemble de clefs de chiffrement et un ensemble de clefs de déchiffrement (possiblement différents) ;
- Pour chaque clef de chiffrement k il y a une clef de déchiffrement notée k^{-1} (non nécessairement unique) telle que pour chaque message clair m

$$\texttt{Si } c{:=}E(m,k) \texttt{ alors } m{=}D(c,k^{-1})\ .$$

Principe du chiffrement (suite)

- Alice produit le (texte) chiffré c correspondant au (texte) clair m et à la clef de chiffrement k par

$$c := E(m, k) \ .$$

- Alice envoie c à Bob sur le canal public ;
- Bob retrouve le clair m puisque

$$m = D(c, k^{-1}) \ .$$

Notons que Bob doit connaître la clef de déchiffrement qui correspond à k (par contre il n'est pas obligé de connaître k elle-même).

Principe du chiffrement (suite)

- Alice produit le (texte) chiffré c correspondant au (texte) clair m et à la clef de chiffrement k par

$$c := E(m, k) \ .$$

- Alice envoie c à Bob sur le canal public ;
- Bob retrouve le clair m puisque

$$m = D(c, k^{-1}) \ .$$

Notons que Bob doit connaître la clef de déchiffrement qui correspond à k (par contre il n'est pas obligé de connaître k elle-même).

Principe du chiffrement (suite)

- Alice produit le (texte) chiffré c correspondant au (texte) clair m et à la clef de chiffrement k par

$$c := E(m, k) \ .$$

- Alice envoie c à Bob sur le canal public ;
- Bob retrouve le clair m puisque

$$m = D(c, k^{-1}) \ .$$

Notons que Bob doit connaître la clef de déchiffrement qui correspond à k (par contre il n'est pas obligé de connaître k elle-même).

Principe du chiffrement (suite)

- Alice produit le (texte) chiffré c correspondant au (texte) clair m et à la clef de chiffrement k par

$$c := E(m, k) \; .$$

- Alice envoie c à Bob sur le canal public ;
- Bob retrouve le clair m puisque

$$m = D(c, k^{-1}) \; .$$

Notons que Bob doit connaître la clef de déchiffrement qui correspond à k (par contre il n'est pas obligé de connaître k elle-même).

Principe du chiffrement (suite)

- Alice produit le (texte) chiffré c correspondant au (texte) clair m et à la clef de chiffrement k par

$$c := E(m, k) \ .$$

- Alice envoie c à Bob sur le canal public ;
- Bob retrouve le clair m puisque

$$m = D(c, k^{-1}) \ .$$

Notons que Bob doit connaître la clef de déchiffrement qui correspond à k (par contre il n'est pas obligé de connaître k elle-même).

Deux principaux types de cryptosystèmes

- Les schémas à clef secrète (ou symétriques) : k et k^{-1} sont identiques et (*a priori*) seulement connues par Alice et Bob ;
- Les schémas à clef publique (ou asymétrique) : la clef de chiffrement k est publique (connue par tout le monde), la clef de déchiffrement k^{-1} est une quantité secrète détenue par le seul Bob.

Deux principaux types de cryptosystèmes

- Les schémas à clef secrète (ou symétriques) : k et k^{-1} sont identiques et (*a priori*) seulement connues par Alice et Bob ;
- Les schémas à clef publique (ou asymétrique) : la clef de chiffrement k est publique (connue par tout le monde), la clef de déchiffrement k^{-1} est une quantité secrète détenue par le seul Bob.

Deux principaux types de cryptosystèmes

- Les schémas à clef secrète (ou symétriques) : k et k^{-1} sont identiques et (*a priori*) seulement connues par Alice et Bob ;
- Les schémas à clef publique (ou asymétrique) : la clef de chiffrement k est publique (connue par tout le monde), la clef de déchiffrement k^{-1} est une quantité secrète détenue par le seul Bob.

Procédé par blocs itéré

Un procédé de chiffrement par blocs est un cryptosystème (à clef secrète) dans lequel les messages clairs sont divisés en plusieurs blocs de bits de même taille.

Un procédé de chiffrement par blocs itéré consiste en l'application itérative d'une fonction de tour (paramétrée par une clef) f sur le clair.

Dans un procédé de chiffrement par blocs itéré à r tours nous avons

$$x_i := f(k_i, x_{i-1}) \text{ pour } 1 \leq i \leq r \ ,$$

où x_0 est le clair, x_r est le chiffré et $k_1, \ldots, k_r$ sont les sous-clefs de chacun des tours (obtenues à partir d'une clef secrète principale).

Dans de tels cryptosystèmes, pour chaque (sous-)clef k la fonction $f_k : x \mapsto f(x, k)$ est une permutation.

Exemples : DES, IDEA, AES, ...

Procédé par blocs itéré

Un procédé de chiffrement par blocs est un cryptosystème (à clef secrète) dans lequel les messages clairs sont divisés en plusieurs blocs de bits de même taille.

Un procédé de chiffrement par blocs itéré consiste en l'application itérative d'une fonction de tour (paramétrée par une clef) f sur le clair.

Dans un procédé de chiffrement par blocs itéré à r tours nous avons

$$x_i := f(k_i, x_{i-1}) \text{ pour } 1 \leq i \leq r \ ,$$

où x_0 est le clair, x_r est le chiffré et $k_1, \ldots, k_r$ sont les sous-clefs de chacun des tours (obtenues à partir d'une clef secrète principale).

Dans de tels cryptosystèmes, pour chaque (sous-)clef k la fonction $f_k : x \mapsto f(x, k)$ est une permutation.

Exemples : DES, IDEA, AES, ...

Procédé par blocs itéré

Un procédé de chiffrement par blocs est un cryptosystème (à clef secrète) dans lequel les messages clairs sont divisés en plusieurs blocs de bits de même taille.
Un procédé de chiffrement par blocs itéré consiste en l'application itérative d'une fonction de tour (paramétrée par une clef) f sur le clair.
Dans un procédé de chiffrement par blocs itéré à r tours nous avons

$$x_i := f(k_i, x_{i-1}) \text{ pour } 1 \leq i \leq r \ ,$$

où x_0 est le clair, x_r est le chiffré et $k_1, \ldots, k_r$ sont les sous-clefs de chacun des tours (obtenues à partir d'une clef secrète principale).
Dans de tels cryptosystèmes, pour chaque (sous-)clef k la fonction $f_k : x \mapsto f(x, k)$ est une permutation.
Exemples : DES, IDEA, AES, ...

Procédé par blocs itéré

Un procédé de chiffrement par blocs est un cryptosystème (à clef secrète) dans lequel les messages clairs sont divisés en plusieurs blocs de bits de même taille.
Un procédé de chiffrement par blocs itéré consiste en l'application itérative d'une fonction de tour (paramétrée par une clef) f sur le clair.
Dans un procédé de chiffrement par blocs itéré à r tours nous avons

$$x_i := f(k_i, x_{i-1}) \text{ pour } 1 \leq i \leq r ,$$

où x_0 est le clair, x_r est le chiffré et $k_1, \ldots, k_r$ sont les sous-clefs de chacun des tours (obtenues à partir d'une clef secrète principale).
Dans de tels cryptosystèmes, pour chaque (sous-)clef k la fonction $f_k : x \mapsto f(x, k)$ est une permutation.
Exemples : DES, IDEA, AES, ...

Procédé par blocs itéré

Un procédé de chiffrement par blocs est un cryptosystème (à clef secrète) dans lequel les messages clairs sont divisés en plusieurs blocs de bits de même taille.
Un procédé de chiffrement par blocs itéré consiste en l'application itérative d'une fonction de tour (paramétrée par une clef) f sur le clair.
Dans un procédé de chiffrement par blocs itéré à r tours nous avons

$$x_i := f(k_i, x_{i-1}) \text{ pour } 1 \leq i \leq r \ ,$$

où x_0 est le clair, x_r est le chiffré et $k_1, \ldots, k_r$ sont les sous-clefs de chacun des tours (obtenues à partir d'une clef secrète principale).
Dans de tels cryptosystèmes, pour chaque (sous-)clef k la fonction $f_k : x \mapsto f(x, k)$ est une permutation.
Exemples : DES, IDEA, AES, ...

Procédé par blocs itéré

Un procédé de chiffrement par blocs est un cryptosystème (à clef secrète) dans lequel les messages clairs sont divisés en plusieurs blocs de bits de même taille.
Un procédé de chiffrement par blocs itéré consiste en l'application itérative d'une fonction de tour (paramétrée par une clef) f sur le clair.
Dans un procédé de chiffrement par blocs itéré à r tours nous avons

$$x_i := f(k_i, x_{i-1}) \text{ pour } 1 \leq i \leq r \ ,$$

où x_0 est le clair, x_r est le chiffré et $k_1, \ldots, k_r$ sont les sous-clefs de chacun des tours (obtenues à partir d'une clef secrète principale).
Dans de tels cryptosystèmes, pour chaque (sous-)clef k la fonction $f_k : x \mapsto f(x, k)$ est une permutation.
Exemples : DES, IDEA, AES, ...

Plan

Attaque par force brute (ou recherche exhaustive)

Algorithme

Étant donné un chiffré c, chercher toutes les clefs possibles k telles que $D(c, k)$ produise un clair "correct".

Un cryptosystème est *sûr* s'il n'est vulnérable à aucune attaque plus efficace que la recherche exhaustive.

Attaque par force brute (ou recherche exhaustive)

Algorithme

Étant donné un chiffré c, chercher toutes les clefs possibles k telles que $D(c, k)$ produise un clair "correct".

Un cryptosystème est *sûr* s'il n'est vulnérable à aucune attaque plus efficace que la recherche exhaustive.

Attaques sur le dernier tour d'un procédé par blocs itéré

Objectif

Retrouver la clef k_r utilisée au dernier tour à partir de la connaissance de certains couples de textes clairs/chiffrés.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Principe

- Il faut être capable de distinguer de manière statistique le procédé de chiffrement réduit, $R = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$, d'une variable uniformément distribuée.
- Si une telle propriété statistique, appelée un distingueur, peut être trouvée, on peut déduire de l'information sur k_r en vérifiant si, pour une valeur donnée k_r, la fonction

$$x_0 \mapsto f_{k_r}^{-1}(x_r)$$

satisfait le distingueur ou non.
Les valeurs de k_r pour lesquelles le biais statistique est observé sont des candidates pour être la clef réellement utilisée au dernier tour.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Principe

- Il faut être capable de distinguer de manière statistique le procédé de chiffrement réduit, $R = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$, d'une variable uniformément distribuée.
- Si une telle propriété statistique, appelée un distingueur, peut être trouvée, on peut déduire de l'information sur k_r en vérifiant si, pour une valeur donnée k_r, la fonction

$$x_0 \mapsto f_{k_r}^{-1}(x_r)$$

satisfait le distingueur ou non.
Les valeurs de k_r pour lesquelles le biais statistique est observé sont des candidates pour être la clef réellement utilisée au dernier tour.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Principe

- Il faut être capable de distinguer de manière statistique le procédé de chiffrement réduit, $R = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$, d'une variable uniformément distribuée.
- Si une telle propriété statistique, appelée un distingueur, peut être trouvée, on peut déduire de l'information sur k_r en vérifiant si, pour une valeur donnée k_r, la fonction

$$x_0 \mapsto f_{k_r}^{-1}(x_r)$$

satisfait le distingueur ou non.

Les valeurs de k_r pour lesquelles le biais statistique est observé sont des candidates pour être la clef réellement utilisée au dernier tour.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Principe

- Il faut être capable de distinguer de manière statistique le procédé de chiffrement réduit, $R = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$, d'une variable uniformément distribuée.
- Si une telle propriété statistique, appelée un distingueur, peut être trouvée, on peut déduire de l'information sur k_r en vérifiant si, pour une valeur donnée k_r, la fonction

  $$x_0 \mapsto f_{k_r}^{-1}(x_r)$$

  satisfait le distingueur ou non.
  Les valeurs de k_r pour lesquelles le biais statistique est observé sont des candidates pour être la clef réellement utilisée au dernier tour.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Différents distingueurs

Différents distingueurs peuvent être exploités :

- Le chiffrement réduit R possède une dérivée, $d_\alpha R : x \mapsto R(x \oplus \alpha) \oplus R(x)$, dont les valeurs en sortie ne sont pas uniformément distribuées. Ce distingueur mène à l'attaque différentielle ;
- Il existe un combinaison linéaire de bits en entrée et en sortie du chiffrement réduit qui constitue une approximation affine du procédé. Cela conduit à l'attaque linéaire ;
- Le chiffrement réduit, vu comme un polynôme de $GF(2^m)[X]$, est de petit degré. Cela conduit à l'attaque par interpolation.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Différents distingueurs

Différents distingueurs peuvent être exploités :

- Le chiffrement réduit R possède une dérivée, $d_\alpha R : x \mapsto R(x \oplus \alpha) \oplus R(x)$, dont les valeurs en sortie ne sont pas uniformément distribuées. Ce distingueur mène à l'attaque différentielle ;
- Il existe un combinaison linéaire de bits en entrée et en sortie du chiffrement réduit qui constitue une approximation affine du procédé. Cela conduit à l'attaque linéaire ;
- Le chiffrement réduit, vu comme un polynôme de $GF(2^m)[X]$, est de petit degré. Cela conduit à l'attaque par interpolation.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Différents distingueurs

Différents distingueurs peuvent être exploités :

- Le chiffrement réduit R possède une dérivée, $d_\alpha R : x \mapsto R(x \oplus \alpha) \oplus R(x)$, dont les valeurs en sortie ne sont pas uniformément distribuées. Ce distingueur mène à l'attaque différentielle ;
- Il existe un combinaison linéaire de bits en entrée et en sortie du chiffrement réduit qui constitue une approximation affine du procédé. Cela conduit à l'attaque linéaire ;
- Le chiffrement réduit, vu comme un polynôme de $GF(2^m)[X]$, est de petit degré. Cela conduit à l'attaque par interpolation.

Attaques sur le dernier tour d'un procédé par blocs itéré (suite)

Différents distingueurs

Différents distingueurs peuvent être exploités :

- Le chiffrement réduit R possède une dérivée, $d_\alpha R : x \mapsto R(x \oplus \alpha) \oplus R(x)$, dont les valeurs en sortie ne sont pas uniformément distribuées. Ce distingueur mène à l'attaque différentielle ;
- Il existe un combinaison linéaire de bits en entrée et en sortie du chiffrement réduit qui constitue une approximation affine du procédé. Cela conduit à l'attaque linéaire ;
- Le chiffrement réduit, vu comme un polynôme de $GF(2^m)[X]$, est de petit degré. Cela conduit à l'attaque par interpolation.

Cryptanalyse différentielle (Biham & Shamir)

- Trouver une différence (α, β) telle que

$$\Pr(R(x) \oplus R(x \oplus \alpha) = \beta)$$

soit la plus éloignée possible de la distribution uniforme ;

- Choisir un clair x_0 et chiffrer à la fois x_0 et $x_0 \oplus \alpha$. Deux couples clairs/chiffrés sont ainsi obtenus (x_0, x_r) et $(x_0 \oplus \alpha, x'_r)$;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ pour la clef du dernier tour telles que

$$f^{-1}_{\widehat{k_r}}(x_r) \oplus f^{-1}_{\widehat{k_r}}(x'_r) = \beta \,;$$

- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse différentielle (Biham & Shamir)

- Trouver une différence (α, β) telle que
$$\mathrm{Pr}(R(x) \oplus R(x \oplus \alpha) = \beta)$$
soit la plus éloignée possible de la distribution uniforme ;
- Choisir un clair x_0 et chiffrer à la fois x_0 et $x_0 \oplus \alpha$. Deux couples clairs/chiffrés sont ainsi obtenus (x_0, x_r) et $(x_0 \oplus \alpha, x'_r)$;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ pour la clef du dernier tour telles que
$$f^{-1}_{\widehat{k_r}}(x_r) \oplus f^{-1}_{\widehat{k_r}}(x'_r) = \beta \ ;$$
- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse différentielle (Biham & Shamir)

- Trouver une différence (α, β) telle que
$$\Pr(R(x) \oplus R(x \oplus \alpha) = \beta)$$
soit la plus éloignée possible de la distribution uniforme ;
- Choisir un clair x_0 et chiffrer à la fois x_0 et $x_0 \oplus \alpha$. Deux couples clairs/chiffrés sont ainsi obtenus (x_0, x_r) et $(x_0 \oplus \alpha, x'_r)$;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ pour la clef du dernier tour telles que
$$f^{-1}_{\widehat{k_r}}(x_r) \oplus f^{-1}_{\widehat{k_r}}(x'_r) = \beta \; ;$$
- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse différentielle (Biham & Shamir)

- Trouver une différence (α, β) telle que
$$\Pr(R(x) \oplus R(x \oplus \alpha) = \beta)$$
soit la plus éloignée possible de la distribution uniforme ;
- Choisir un clair x_0 et chiffrer à la fois x_0 et $x_0 \oplus \alpha$. Deux couples clairs/chiffrés sont ainsi obtenus (x_0, x_r) et $(x_0 \oplus \alpha, x_r')$;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ pour la clef du dernier tour telles que
$$f_{\widehat{k_r}}^{-1}(x_r) \oplus f_{\widehat{k_r}}^{-1}(x_r') = \beta \;;$$
- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse différentielle (Biham & Shamir)

- Trouver une différence (α, β) telle que
$$\Pr(R(x) \oplus R(x \oplus \alpha) = \beta)$$
soit la plus éloignée possible de la distribution uniforme ;
- Choisir un clair x_0 et chiffrer à la fois x_0 et $x_0 \oplus \alpha$. Deux couples clairs/chiffrés sont ainsi obtenus (x_0, x_r) et $(x_0 \oplus \alpha, x'_r)$;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ pour la clef du dernier tour telles que
$$f^{-1}_{\widehat{k_r}}(x_r) \oplus f^{-1}_{\widehat{k_r}}(x'_r) = \beta \;;$$
- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse linéaire (Matsui)

- Trouver un masque (α, β) pour lequel l'équation

$$\alpha.x_0 \oplus \beta.R(x_0) = 0$$

  est satisfaite pour la plupart des clairs x_0 et clefs de tour $k_1, \ldots, k_{r-1}$;
- Choisir au hasard un clair x_0 et calculer le chiffré correspondant x_r ;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ de la clef du dernier tour telles que

$$\alpha.x_0 \oplus \beta.f_{\widehat{k_r}}^{-1}(x_r) = 0 ;$$

- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse linéaire (Matsui)

- Trouver un masque (α, β) pour lequel l'équation

$$\alpha.x_0 \oplus \beta.R(x_0) = 0$$

  est satisfaite pour la plupart des clairs x_0 et clefs de tour $k_1, \ldots, k_{r-1}$;
- Choisir au hasard un clair x_0 et calculer le chiffré correspondant x_r ;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ de la clef du dernier tour telles que

$$\alpha.x_0 \oplus \beta.f_{\widehat{k_r}}^{-1}(x_r) = 0 ;$$

- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse linéaire (Matsui)

- Trouver un masque (α, β) pour lequel l'équation

$$\alpha . x_0 \oplus \beta . R(x_0) = 0$$

  est satisfaite pour la plupart des clairs x_0 et clefs de tour $k_1, \ldots, k_{r-1}$;
- Choisir au hasard un clair x_0 et calculer le chiffré correspondant x_r ;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ de la clef du dernier tour telles que

$$\alpha . x_0 \oplus \beta . f^{-1}_{\widehat{k_r}}(x_r) = 0 \; ;$$

- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse linéaire (Matsui)

- Trouver un masque (α, β) pour lequel l'équation

$$\alpha.x_0 \oplus \beta.R(x_0) = 0$$

  est satisfaite pour la plupart des clairs x_0 et clefs de tour $k_1, \ldots, k_{r-1}$;
- Choisir au hasard un clair x_0 et calculer le chiffré correspondant x_r ;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ de la clef du dernier tour telles que

$$\alpha.x_0 \oplus \beta.f^{-1}_{\widehat{k_r}}(x_r) = 0 \ ;$$

- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Cryptanalyse linéaire (Matsui)

- Trouver un masque (α, β) pour lequel l'équation

$$\alpha.x_0 \oplus \beta.R(x_0) = 0$$

  est satisfaite pour la plupart des clairs x_0 et clefs de tour $k_1, \ldots, k_{r-1}$;
- Choisir au hasard un clair x_0 et calculer le chiffré correspondant x_r ;
- Trouver toutes les valeurs possibles $\widehat{k_r}$ de la clef du dernier tour telles que

$$\alpha.x_0 \oplus \beta.f_{\widehat{k_r}}^{-1}(x_r) = 0 \ ;$$

- Itérer les deuxième et troisième étapes jusqu'à ce qu'une des valeurs $\widehat{k_r}$ apparaisse plus fréquemment que les autres.

Résistances contre les attaques différentielle et linéaire

Dans la plupart des cas, les faiblesses différentielle et/ou linéaire d'un chiffrement réduit peuvent être décelées si certains composants internes de la fonction de tour f, les boîtes-S, présentent un défaut similaire. Aussi pour qu'un cryptosystème soit résistant il faut que quelle que soit S une boîtes-S on ait :

- Pour chaque bloc non nul α, la distribution des différences $S(x \oplus \alpha) \oplus S(x)$ doit être la plus proche possible de l'équiprobabilité (fonctions booléennes parfaitement non linéaires) ;
- Pour chaque bloc non nul β, la fonction booléenne $x \mapsto \beta.S(x)$ doit être suffisament loin de toutes fonctions affines (fonctions booléennes courbes).

Résistances contre les attaques différentielle et linéaire

Dans la plupart des cas, les faiblesses différentielle et/ou linéaire d'un chiffrement réduit peuvent être décelées si certains composants internes de la fonction de tour f, les boîtes-S, présentent un défaut similaire. Aussi pour qu'un cryptosystème soit résistant il faut que quelle que soit S une boîtes-S on ait :

- Pour chaque bloc non nul α, la distribution des différences $S(x \oplus \alpha) \oplus S(x)$ doit être la plus proche possible de l'équiprobabilité (fonctions booléennes parfaitement non linéaires) ;
- Pour chaque bloc non nul β, la fonction booléenne $x \mapsto \beta.S(x)$ doit être suffisament loin de toutes fonctions affines (fonctions booléennes courbes).

Résistances contre les attaques différentielle et linéaire

Dans la plupart des cas, les faiblesses différentielle et/ou linéaire d'un chiffrement réduit peuvent être décelées si certains composants internes de la fonction de tour f, les boîtes-S, présentent un défaut similaire. Aussi pour qu'un cryptosystème soit résistant il faut que quelle que soit S une boîtes-S on ait :

- Pour chaque bloc non nul α, la distribution des différences $S(x \oplus \alpha) \oplus S(x)$ doit être la plus proche possible de l'équiprobabilité (fonctions booléennes parfaitement non linéaires) ;
- Pour chaque bloc non nul β, la fonction booléenne $x \mapsto \beta.S(x)$ doit être suffisament loin de toutes fonctions affines (fonctions booléennes courbes).

Résistances contre les attaques différentielle et linéaire

Dans la plupart des cas, les faiblesses différentielle et/ou linéaire d'un chiffrement réduit peuvent être décelées si certains composants internes de la fonction de tour f, les boîtes-S, présentent un défaut similaire. Aussi pour qu'un cryptosystème soit résistant il faut que quelle que soit S une boîtes-S on ait :

- Pour chaque bloc non nul α, la distribution des différences $S(x \oplus \alpha) \oplus S(x)$ doit être la plus proche possible de l'équiprobabilité (fonctions booléennes parfaitement non linéaires) ;
- Pour chaque bloc non nul β, la fonction booléenne $x \mapsto \beta.S(x)$ doit être suffisament loin de toutes fonctions affines (fonctions booléennes courbes).

Résistances contre les attaques différentielle et linéaire

Dans la plupart des cas, les faiblesses différentielle et/ou linéaire d'un chiffrement réduit peuvent être décelées si certains composants internes de la fonction de tour f, les boîtes-S, présentent un défaut similaire. Aussi pour qu'un cryptosystème soit résistant il faut que quelle que soit S une boîtes-S on ait :

- Pour chaque bloc non nul α, la distribution des différences $S(x \oplus \alpha) \oplus S(x)$ doit être la plus proche possible de l'équiprobabilité (fonctions booléennes parfaitement non linéaires) ;
- Pour chaque bloc non nul β, la fonction booléenne $x \mapsto \beta.S(x)$ doit être suffisament loin de toutes fonctions affines (fonctions booléennes courbes).

Résistances contre les attaques différentielle et linéaire

Dans la plupart des cas, les faiblesses différentielle et/ou linéaire d'un chiffrement réduit peuvent être décelées si certains composants internes de la fonction de tour f, les boîtes-S, présentent un défaut similaire. Aussi pour qu'un cryptosystème soit résistant il faut que quelle que soit S une boîtes-S on ait :

- Pour chaque bloc non nul α, la distribution des différences $S(x \oplus \alpha) \oplus S(x)$ doit être la plus proche possible de l'équiprobabilité (fonctions booléennes parfaitement non linéaires) ;
- Pour chaque bloc non nul β, la fonction booléenne $x \mapsto \beta.S(x)$ doit être suffisament loin de toutes fonctions affines (fonctions booléennes courbes).

Plan

Historique

Définition (Nyberg, 1991)

Une application $f : \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^n$ est parfaitement non linéaire si pour chaque α non nul de $\mathbb{Z}_2^m$ et chaque $\beta \in \mathbb{Z}_2^n$,

$$|\{x \in \mathbb{Z}_2^m | f(\alpha \oplus x) \oplus f(x) = \beta\}| = 2^{m-n} .$$

Garantit la résistance maximale contre l'attaque différentielle.

Dans le cadre des groupes finis commutatifs (1)

Pour un groupe G, 0_G représente son élément neutre et $G^* = G \setminus \{0_G\}$.

Définition

- Soient X et Y deux ensembles finis non vides. Une application $f : X \to Y$ est équilibrée si pour chaque $y \in Y$, $|\{x \in X | f(x) = y\}| = \frac{|X|}{|Y|}$;
- Soient G et H deux groupes finis commutatifs et $f : G \to H$. La dérivée de f en $\alpha \in G$ est définie par

$$\begin{array}{rccc} d_\alpha f : & G & \to & H \\ & x & \mapsto & f(\alpha + x) - f(x) \,. \end{array}$$

Dans le cadre des groupes finis commutatifs (2)

Définition

Une application $f : G \to H$ est (classiquement) parfaitement non linéaire (ou PN) si $\forall \alpha \in G^*$, $d_\alpha f$ est équilibrée, *i.e.* $\forall \alpha \in G^*$ and $\forall \beta \in H$,

$$|\{x \in G | f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Dans le cadre des groupes finis commutatifs (2)

Définition

Une application $f : G \to H$ est (classiquement) parfaitement non linéaire (ou PN) si $\forall \alpha \in G^*$, $d_\alpha f$ est équilibrée, *i.e.* $\forall \alpha \in G^*$ and $\forall \beta \in H$,

$$|\{x \in G | f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Caractérisations équivalentes

La non linéarité parfaite (traditionnelle) $\Leftrightarrow$

- Par la transformée de Fourier : notion de fonctions courbes ;
- Caractérisation combinatoire par les ensembles à différences.

Caractérisations équivalentes

La non linéarité parfaite (traditionnelle) $\Leftrightarrow$

- Par la transformée de Fourier : notion de fonctions courbes ;
- Caractérisation combinatoire par les ensembles à différences.

Caractérisations équivalentes

La non linéarité parfaite (traditionnelle) $\Leftrightarrow$

- Par la transformée de Fourier : notion de fonctions courbes ;
- Caractérisation combinatoire par les ensembles à différences.

Plan

Historique

Définition (Dillon 1974, Rothaus 1976)

Une application $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ est courbe si pour chaque $\alpha \in \mathbb{Z}_2^m$,

$$\sum_{x \in \mathbb{Z}_2^m} (-1)^{f(x) \oplus \alpha . x} = \pm 2^{\frac{m}{2}} .$$

Assure la résistance maximale contre l'attaque linéaire.

Exemple

L'application suivante

$$\begin{array}{rccc} f: & \mathbb{Z}_2^m \times \mathbb{Z}_2^m & \longrightarrow & \mathbb{Z}_2 \\ & (x, y) & \mapsto & x.y = \bigoplus_{i=1}^{m} x_i y_i \ . \end{array}$$

est une fonction courbe.

Dans le cadre des groupes finis commutatifs (1)

Le groupe dual de G, noté $\widehat{G}$, est l'ensemble de tous homomorphismes de groupes de G dans $\mathbb{U}$ équippé de la multiplication point-à-point.

Il est isomorphe à G lui-même. Ses éléments sont appelés des caractères : pour $\alpha \in G$, le caractère correspondant à α (via l'isomorphisme de G sur $\widehat{G}$) est noté χ_G^{α}.

Par exemple si G est $\mathbb{Z}_2^m$ et $\alpha \in \mathbb{Z}_2^m$, alors $\chi_G^{\alpha}(x) = (-1)^{\alpha.x}$.

Dans le cadre des groupes finis commutatifs (1)

Le groupe dual de G, noté $\widehat{G}$, est l'ensemble de tous homomorphismes de groupes de G dans $\mathbb{U}$ équippé de la multiplication point-à-point.
Il est isomorphe à G lui-même. Ses éléments sont appelés des caractères : pour $\alpha \in G$, le caractère correspondant à α (via l'isomorphisme de G sur $\widehat{G}$) est noté χ_G^α.
Par exemple si G est $\mathbb{Z}_2^m$ et $\alpha \in \mathbb{Z}_2^m$, alors $\chi_G^\alpha(x) = (-1)^{\alpha.x}$.

Dans le cadre des groupes finis commutatifs (1)

Le groupe dual de G, noté $\widehat{G}$, est l'ensemble de tous homomorphismes de groupes de G dans $\mathbb{U}$ équippé de la multiplication point-à-point.
Il est isomorphe à G lui-même. Ses éléments sont appelés des caractères : pour $\alpha \in G$, le caractère correspondant à α (via l'isomorphisme de G sur $\widehat{G}$) est noté χ_G^α.
Par exemple si G est $\mathbb{Z}_2^m$ et $\alpha \in \mathbb{Z}_2^m$, alors $\chi_G^\alpha(x) = (-1)^{\alpha.x}$.

Dans le cadre des groupes finis commutatifs (2)

Définition

Soit G un groupe abélien fini et $\varphi : G \longrightarrow \mathbb{C}$. La transformée de Fourier (discrète) de φ est l'application $\widehat{\varphi}$ definie comme suit

$$\begin{array}{rccl} \widehat{\varphi} : & G & \rightarrow & \mathbb{C} \\ & \alpha & \mapsto & \displaystyle\sum_{x \in G} \varphi(x)\chi_G^{\alpha}(x) \ . \end{array}$$

Caractérisation "duale"

Théorème (Carlet & Ding and Pott, 2004)

Soient G et H deux groupes finis commutatifs. Soit $f : G \to H$. L'application f est parfaitement non linéaire si et seulement si $\forall \alpha \in G$, $\forall \beta \in H^*$,

$$|\widehat{\chi_H^\beta \circ f}(\alpha)|^2 = |G| \ .$$

Lorsque $G = \mathbb{Z}_2^m$ et $H = \mathbb{Z}_2$, il s'agit de la notion classique de fonctions courbes introduite par Dillon.
En 2006, ce résultat a été généralisé aux cas des groupes finis **non commutatifs** (la notion de caractères est alors remplacée par celle plus générale de représentations linéaires).

Caractérisation "duale"

Théorème (Carlet & Ding and Pott, 2004)

Soient G et H deux groupes finis commutatifs. Soit $f : G \rightarrow H$. L'application f est parfaitement non linéaire si et seulement si $\forall \alpha \in G$, $\forall \beta \in H^*$,

$$|\widehat{\chi_H^\beta \circ f}(\alpha)|^2 = |G| \ .$$

Lorsque $G = \mathbb{Z}_2^m$ et $H = \mathbb{Z}_2$, il s'agit de la notion classique de fonctions courbes introduite par Dillon.

En 2006, ce résultat a été généralisé aux cas des groupes finis **non commutatifs** (la notion de caractères est alors remplacée par celle plus générale de représentations linéaires).

Caractérisation "duale"

Théorème (Carlet & Ding and Pott, 2004)

Soient G et H deux groupes finis commutatifs. Soit $f : G \to H$. L'application f est parfaitement non linéaire si et seulement si $\forall \alpha \in G$, $\forall \beta \in H^*$,

$$|\widehat{\chi_H^\beta \circ f}(\alpha)|^2 = |G| \ .$$

Lorsque $G = \mathbb{Z}_2^m$ et $H = \mathbb{Z}_2$, il s'agit de la notion classique de fonctions courbes introduite par Dillon.
En 2006, ce résultat a été généralisé aux cas des groupes finis **non commutatifs** (la notion de caractères est alors remplacée par celle plus générale de représentations linéaires).

Plan

Définition

Soit G un groupe fini. Soit $D \subset G$. D est un (v, k, λ) ensemble à différences de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet λ solutions (x, y) dans D^2.

Définition

Soit G un groupe fini. Soit $D \subset G$. D est un (v, k, λ) ensemble à différences de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet λ solutions (x, y) dans D^2.

Définition

Soit G un groupe fini. Soit $D \subset G$. D est un (v, k, λ) ensemble à différences de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet λ solutions (x, y) dans D^2.

Définition

Soit G un groupe fini. Soit $D \subset G$. D est un (v, k, λ) ensemble à différences de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet λ solutions (x, y) dans D^2.

Ensembles à différences de Hadamard

Définition

Un (v, k, λ) ensemble à différences D de G est dit de Hadamard si

$$(v, k, \lambda) = (4n^2, 2n^2 \pm n, n(n \pm 1)) \ .$$

pour un certain entier n.

Caractérisation combinatoire

Théorème (Carlet & Ding, 2004)

Soit G un groupe fini commutatif tel que $|G| = 4n^2$. Une fonction $f : G \longrightarrow \mathbb{Z}_2$ est parfaitement non linéaire si et seulement si son support $S_f = \{x \in G | f(x) = 1\}$ est un ensemble à différences de Hadamard de G.

Il s'agit d'une généralisation d'un résultat de Dillon (1974) concernant les fonctions booléennes.

Les cas impossibles

En vue d'une implantation logicielle ou matérielle, les cryptographes s'intéressent aux fonctions booléennes $f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ mais les fonctions booléennes courbes n'existent que si m est un entier pair et $m \geq 2n$.

Cas impossibles : Longueur impaire (m est un entier impair) et le cas planaire ($m = n$).

Les cas impossibles

En vue d'une implantation logicielle ou matérielle, les cryptographes s'intéressent aux fonctions booléennes $f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ mais les fonctions booléennes courbes n'existent que si m est un entier pair et $m \geq 2n$.
Cas impossibles : Longueur impaire (m est un entier impair) et le cas planaire ($m = n$).

Plan

Actions de groupe (1)

Soit un groupe $(G, *)$ et X un ensemble non vide. Une action de groupe (à gauche) de G sur X est un homomorphisme de groupes ϕ de G vers le groupe $S(X)$ des permutations sur X (appelé *groupe symétrique* lorsque X est fini). En particulier,

- $\phi(0_G) = Id_X$;
- $\forall (g_1, g_2) \in G^2, \phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$.

Actions de groupe (1)

Soit un groupe $(G, *)$ et X un ensemble non vide.
Une action de groupe (à gauche) de G sur X est un homomorphisme de groupes ϕ de G vers le groupe $S(X)$ des permutations sur X (appelé *groupe symétrique* lorsque X est fini). En particulier,

- $\phi(0_G) = Id_X$;
- $\forall (g_1, g_2) \in G^2$, $\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$.

Actions de groupe (2)

Notation

Pour $x \in X$ et $g \in G$, on note

$$g.x = \phi(g)(x)\ .$$

Intuitivement une action de groupe s'interprète comme un loi de composition externe de G sur X.

Actions de groupe (2)

Notation

Pour $x \in X$ et $g \in G$, on note

$$g.x = \phi(g)(x) \; .$$

Intuitivement une action de groupe s'interprète comme un loi de composition externe de G sur X.

Actions de groupe (3)

Définition

L'action ϕ de G sur X est dite

- fidèle si ϕ est injective ;
- régulière si quels que soient x et y dans X, il existe un et un seul g de G tel que $g.x_1 = x_2$.

Actions de groupe (3)

Définition

L'action ϕ de G sur X est dite

- fidèle si ϕ est injective ;
- régulière si quels que soient x et y dans X, il existe un et un seul g de G tel que $g.x_1 = x_2$.

Actions de groupe (3)

Définition

L'action ϕ de G sur X est dite

- fidèle si ϕ est injective ;
- régulière si quels que soient x et y dans X, il existe un et un seul g de G tel que $g.x_1 = x_2$.

Exemples

- L'action de G sur lui-même par translation à gauche est régulière. Pour α et x dans G, $\alpha.x := \alpha * x$;
- Si H est un sous-groupe de G alors l'action de H sur G par translation à gauche est fidèle ;
- L'action du groupe multiplicatif $\mathbb{K}^*$ d'un corps $\mathbb{K}$ sur un $\mathbb{K}$-espace vectoriel V par multiplication scalaire est fidèle. Pour $\lambda \in \mathbb{K}^*$ et $v \in V$, on a $\lambda.v := \lambda v$.

Exemples

- L'action de G sur lui-même par translation à gauche est régulière. Pour α et x dans G, $\alpha.x := \alpha * x$;
- Si H est un sous-groupe de G alors l'action de H sur G par translation à gauche est fidèle ;
- L'action du groupe multiplicatif $\mathbb{K}^*$ d'un corps $\mathbb{K}$ sur un $\mathbb{K}$-espace vectoriel V par multiplication scalaire est fidèle. Pour $\lambda \in \mathbb{K}^*$ et $v \in V$, on a $\lambda.v := \lambda v$.

Exemples

- L'action de G sur lui-même par translation à gauche est régulière. Pour α et x dans G, $\alpha.x := \alpha * x$;
- Si H est un sous-groupe de G alors l'action de H sur G par translation à gauche est fidèle ;
- L'action du groupe multiplicatif $\mathbb{K}^*$ d'un corps $\mathbb{K}$ sur un $\mathbb{K}$-espace vectoriel V par multiplication scalaire est fidèle. Pour $\lambda \in \mathbb{K}^*$ et $v \in V$, on a $\lambda.v := \lambda v$.

Exemples

- L'action de G sur lui-même par translation à gauche est régulière. Pour α et x dans G, $\alpha.x := \alpha * x$;
- Si H est un sous-groupe de G alors l'action de H sur G par translation à gauche est fidèle ;
- L'action du groupe multiplicatif $\mathbb{K}^*$ d'un corps $\mathbb{K}$ sur un $\mathbb{K}$-espace vectoriel V par multiplication scalaire est fidèle. Pour $\lambda \in \mathbb{K}^*$ et $v \in V$, on a $\lambda.v := \lambda v$.

Plan

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = S(k_i.x_{i-1})$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$;

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = S(k_i.x_{i-1})$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$;

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = S(k_i.x_{i-1})$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$;

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = S(k_i.x_{i-1})$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$;

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = S(k_i.x_{i-1})$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$;

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité

$$Pr(R(\alpha.x) - R(x) = \beta)$$

est la plus éloignée possible de la distribution uniforme ;

- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que

$$f^{-1}_{\hat{k}_r}(x'_r) - f^{-1}_{\hat{k}_r}(x_r) = \beta \ .$$

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité

$$Pr(R(\alpha.x) - R(x) = \beta)$$

est la plus éloignée possible de la distribution uniforme ;

- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que

$$f_{\hat{k}_r}^{-1}(x'_r) - f_{\hat{k}_r}^{-1}(x_r) = \beta\ .$$

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité

$$Pr(R(\alpha.x) - R(x) = \beta)$$

est la plus éloignée possible de la distribution uniforme ;

- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que

$$f_{\hat{k}_r}^{-1}(x'_r) - f_{\hat{k}_r}^{-1}(x_r) = \beta\ .$$

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité
$$Pr(R(\alpha.x) - R(x) = \beta)$$
est la plus éloignée possible de la distribution uniforme ;
- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que
$$f_{\hat{k}_r}^{-1}(x'_r) - f_{\hat{k}_r}^{-1}(x_r) = \beta \ .$$

Objectif

Construction de boîtes-S maximalement résistantes à l'attaque différentielle modifiée.

Cela conduit à la notion de fonctions G-parfaitement non linéaires.

Objectif

Construction de boîtes-S maximalement résistantes à l'attaque différentielle modifiée.
Cela conduit à la notion de fonctions G-parfaitement non linéaires.

Définition

Soit G un groupe fini commutatif agissant sur un ensemble fini non vide X. Soit H un (éventuellement autre) groupe fini commutatif. Une application $f : X \rightarrow H$ est dite *G-parfaitement non linéaire* si pour chaque $\alpha \in G$ et chaque $\beta \in H$,

$$|\{x \in X | f(\alpha.x) - f(x) = \beta\}| = \frac{|X|}{|H|} .$$

Caractérisation "duale"

Soit G un groupe fini commutatif agissant sur un ensemble fini non vide X. Soit H un (éventuellement autre) groupe fini commutatif. Pour chaque application $f : X \to H$ et chaque $x \in X$, on définit l'application

$$\begin{array}{rccl} f_x : & G & \to & H \\ & g & \mapsto & f_x(g) := f(g.x) \ . \end{array}$$

Théorème

L'application f est G-parfaitement non linéaire si et seulement si pour chaque $\alpha \in G$ et chaque $\beta \in H^*$, on a

$$\frac{1}{|X|} \sum_{x \in X} |\widehat{(\chi_H^\beta \circ f_x)}(\alpha)|^2 = |G| \ .$$

Caractérisation "duale"

Soit G un groupe fini commutatif agissant sur un ensemble fini non vide X. Soit H un (éventuellement autre) groupe fini commutatif. Pour chaque application $f : X \to H$ et chaque $x \in X$, on définit l'application

$$\begin{array}{rccl} f_x : & G & \to & H \\ & g & \mapsto & f_x(g) := f(g.x)\ . \end{array}$$

Théorème

L'application f est G-parfaitement non linéaire si et seulement si pour chaque $\alpha \in G$ et chaque $\beta \in H^*$, on a

$$\frac{1}{|X|} \sum_{x \in X} |\widehat{(\chi_H^\beta \circ f_x)}(\alpha)|^2 = |G|\ .$$

Caractérisation combinatoire

Définition

Soit G un groupe fini agissant sur un ensemble fini non vide X et D un sous-ensemble de X. D est un G-(v, k, λ)-ensemble à différences de X si

- $|X| = v$;
- $|D| = k$;
- Pour chaque $\alpha \in G^*$, l'équation $x = \alpha.y$ admet exactement λ solutions $(x, y) \in D^2$.

Caractérisation combinatoire

Définition

Soit G un groupe fini agissant sur un ensemble fini non vide X et D un sous-ensemble de X. D est un G-(v, k, λ)-ensemble à différences de X si

- $|X| = v$;
- $|D| = k$;
- Pour chaque $\alpha \in G^*$, l'équation $x = \alpha.y$ admet exactement λ solutions $(x, y) \in D^2$.

Caractérisation combinatoire

Définition

Soit G un groupe fini agissant sur un ensemble fini non vide X et D un sous-ensemble de X. D est un G-(v, k, λ)-ensemble à différences de X si

- $|X| = v$;
- $|D| = k$;
- Pour chaque $\alpha \in G^*$, l'équation $x = \alpha.y$ admet exactement λ solutions $(x, y) \in D^2$.

Caractérisation combinatoire

Définition

Soit G un groupe fini agissant sur un ensemble fini non vide X et D un sous-ensemble de X. D est un G-(v, k, λ)-ensemble à différences de X si

- $|X| = v$;
- $|D| = k$;
- Pour chaque $\alpha \in G^*$, l'équation $x = \alpha.y$ admet exactement λ solutions $(x, y) \in D^2$.

Caractérisation combinatoire

Théorème

Soit G un groupe fini agissant sur un ensemble fini non vide X. Une fonction booléenne $f : X \to \mathbb{Z}_2$ est G-PN si et seulement si son support S_f est un G-ensemble à différences de X dont les paramètres (v, k, λ) satisfont l'égalité

$$v = 4(k - \lambda) .$$

Caractérisation combinatoire

Théorème

Soit G un groupe fini agissant sur un ensemble fini non vide X. Une fonction booléenne $f : X \to \mathbb{Z}_2$ est G-PN si et seulement si son support S_f est un G-ensemble à différences de X dont les paramètres (v, k, λ) satisfont l'égalité

$$v = 4(k - \lambda)\ .$$

Plan

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.

On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$. Notons qu'une action libre est fidèle.

Soit V_m un espace vectoriel de dimension m sur le corps fini à deux éléments. Soit G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).

Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{rccl} \phi_x : & G & \to & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.
On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$. Notons qu'une action libre est fidèle.
Soit V_m un espace vectoriel de dimension m sur le corps fini à deux éléments. Soit G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).
Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{cccc} \phi_x : & G & \to & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.
On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$. Notons qu'une action libre est fidèle.
Soit V_m un espace vectoriel de dimension m sur le corps fini à deux éléments. Soit G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).
Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{cccc} \phi_x : & G & \rightarrow & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.
On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$. Notons qu'une action libre est fidèle.
Soit V_m un espace vectoriel de dimension m sur le corps fini à deux éléments. Soit G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).
Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{rccc} \phi_x : & G & \rightarrow & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

À chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.

On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.

Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.

On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

À chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.

On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.

Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.

On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

À chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.

On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.

Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.

On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

À chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.

On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.

Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.

On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

À chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.
On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.
Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.
On définit alors $D := \displaystyle\bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

L'ensemble D ainsi défini est un G-$(2^m, (2N^2 - N)j + (2N^2 + N)(\frac{2^m}{4N^2} - j), (N^2 - N)j + (N^2 + N)(\frac{2^m}{4N^2} - j))$- ensemble à différences de V_m où j est un entier entre 0 et $\frac{2^m}{4N^2}$ désignant le nombre d'ensembles à différences D_x choisis dont les paramètres sont de la forme $(4N^2, 2N^2 - N, N^2 - N)$. Les paramètres de D satisfont en particulier l'équation $v = 4(k - \lambda)$.

Concaténation d'ensembles à différences de Hadamard

L'ensemble D ainsi défini est un G-$(2^m, (2N^2-N)j+(2N^2+N)(\frac{2^m}{4N^2}-j), (N^2-N)j+(N^2+N)(\frac{2^m}{4N^2}-j))$- ensemble à différences de V_m où j est un entier entre 0 et $\frac{2^m}{4N^2}$ désignant le nombre d'ensembles à différences D_x choisis dont les paramètres sont de la forme $(4N^2, 2N^2-N, N^2-N)$.

Les paramètres de D satisfont en particulier l'équation $v = 4(k-\lambda)$.

Concaténation d'ensembles à différences de Hadamard

L'ensemble D ainsi défini est un G-$(2^m, (2N^2 - N)j + (2N^2 + N)(\frac{2^m}{4N^2} - j), (N^2 - N)j + (N^2 + N)(\frac{2^m}{4N^2} - j))$- ensemble à différences de V_m où j est un entier entre 0 et $\frac{2^m}{4N^2}$ désignant le nombre d'ensembles à différences D_x choisis dont les paramètres sont de la forme $(4N^2, 2N^2 - N, N^2 - N)$.
Les paramètres de D satisfont en particulier l'équation $v = 4(k - \lambda)$.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en longueur impaire.

Soient m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.

D'après le résultat précédent, on peut construire une fonction $f : V_m \to \mathbb{Z}_2$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en longueur impaire.

Soient m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.

D'après le résultat précédent, on peut construire une fonction $f : V_m \to \mathbb{Z}_2$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en longueur impaire.
Soient m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.
D'après le résultat précédent, on peut construire une fonction $f : V_m \to \mathbb{Z}_2$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en longueur impaire.
Soient m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.
D'après le résultat précédent, on peut construire une fonction $f : V_m \to \mathbb{Z}_2$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Plan

On a déjà vu qu'il n'existe pas de fonction courbe $f : V_m \to V_m$.

Dès que l'on a une solution x_0 à l'équation $f(\alpha \oplus x) \oplus f(x) = \beta$, on en trouve immédiatement une autre $\alpha \oplus x_0$.

Le mieux que l'on puisse espérer pour f est qu'elle soit presque parfaitement non linéaire *i.e.* pour chaque $(\alpha, \beta) \in V_m^* \times V_m$, $|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| \in \{0, 2\}$.

On a déjà vu qu'il n'existe pas de fonction courbe $f : V_m \to V_m$.

Dès que l'on a une solution x_0 à l'équation $f(\alpha \oplus x) \oplus f(x) = \beta$, on en trouve immédiatement une autre $\alpha \oplus x_0$.

Le mieux que l'on puisse espérer pour f est qu'elle soit presque parfaitement non linéaire *i.e.* pour chaque $(\alpha, \beta) \in V_m^* \times V_m$, $|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| \in \{0, 2\}$.

On a déjà vu qu'il n'existe pas de fonction courbe $f : V_m \to V_m$.
Dès que l'on a une solution x_0 à l'équation $f(\alpha \oplus x) \oplus f(x) = \beta$, on en trouve immédiatement une autre $\alpha \oplus x_0$.
Le mieux que l'on puisse espérer pour f est qu'elle soit presque parfaitement non linéaire *i.e.* pour chaque $(\alpha, \beta) \in V_m^* \times V_m$, $|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| \in \{0, 2\}$.

Conjecture

Il n'existe pas de bijection presque parfaitement non linéaire pour m pair.

Théorème

Soit m un entier strictement positif quelconque. Soit $f : GF(2^m) \rightarrow GF(2^m)$ un automorphisme additif. Alors f est une bijection $GF(2^m)^*$-PN.

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

$$
\begin{array}{rrcl}
 & f(\alpha.x) \oplus f(x) & = & \beta \\
\Leftrightarrow & f(\alpha x) \oplus f(x) & = & \beta \\
\Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\
\Leftrightarrow & f((\alpha \oplus 1)x) & = & \beta \\
\Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\
\Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{\alpha \oplus 1} .
\end{array}
$$

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

$$\begin{array}{rrcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & f((\alpha \oplus 1)x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{\alpha \oplus 1} . \end{array}$$

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

$$
\begin{array}{rlcl}
 & f(\alpha.x) \oplus f(x) & = & \beta \\
\Leftrightarrow & f(\alpha x) \oplus f(x) & = & \beta \\
\Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\
\Leftrightarrow & f((\alpha \oplus 1)x) & = & \beta \\
\Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\
\Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{\alpha \oplus 1} .
\end{array}
$$

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

$$
\begin{array}{rlcl}
 & f(\alpha.x) \oplus f(x) & = & \beta \\
\Leftrightarrow & f(\alpha x) \oplus f(x) & = & \beta \\
\Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\
\Leftrightarrow & f((\alpha \oplus 1)x) & = & \beta \\
\Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\
\Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{\alpha \oplus 1} .
\end{array}
$$

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

$$\begin{array}{rrcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & f((\alpha \oplus 1)x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{\alpha \oplus 1}. \end{array}$$

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha,\beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

$$\begin{array}{rrcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & f((\alpha \oplus 1)x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{\alpha \oplus 1}\,. \end{array}$$

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

$$\begin{array}{rrcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & f((\alpha \oplus 1)x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{\alpha \oplus 1}\ . \end{array}$$