G-perfect nonlinearity

Laurent Poinsot

Université du Sud Toulon-Var (France)

Organized by Professor J. Davis
University of Richmond

Introduction

Cryptographic properties of Boolean functions :

- Balance ;
- Non correlation ;
- High algebraic degree ;
- Perfect nonlinearity (bentness).

Introduction

Cryptographic properties of Boolean functions :

- Balance ;
- Non correlation ;
- High algebraic degree ;
- Perfect nonlinearity (bentness).

Introduction

Cryptographic properties of Boolean functions :

- Balance ;
- Non correlation ;
- High algebraic degree ;
- Perfect nonlinearity (bentness).

Introduction

Cryptographic properties of Boolean functions :

- Balance ;
- Non correlation ;
- High algebraic degree ;
- Perfect nonlinearity (bentness).

Introduction

Cryptographic properties of Boolean functions :

- Balance ;
- Non correlation ;
- High algebraic degree ;
- Perfect nonlinearity (bentness).

Introduction

Let G and H be two finite groups. A mapping $f : G \to H$ is called perfect nonlinear (or *planar*) if for each nonzero α in G and each $\beta \in H$,

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

Let define $\sigma_\alpha : G \to G$ as $x \mapsto \alpha + x$. The previous equation can naturally be re-written as :

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

Introduction

Let G and H be two finite groups. A mapping $f : G \to H$ is called perfect nonlinear (or *planar*) if for each nonzero α in G and each $\beta \in H$,

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

Let define $\sigma_\alpha : G \to G$ as $x \mapsto \alpha + x$. The previous equation can naturally be re-written as :

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

Introduction

Let G and H be two finite groups. A mapping $f : G \rightarrow H$ is called perfect nonlinear (or *planar*) if for each nonzero α in G and each $\beta \in H$,

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

Let define $\sigma_\alpha : G \rightarrow G$ as $x \mapsto \alpha + x$. The previous equation can naturally be re-written as :

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

Introduction

Now let G and H be two finite groups and X be a finite nonempty set on which G acts. A function $f : X \to H$ is *G*-perfect nonlinear if for each nonzero g in G and for each $\beta \in H$,

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

Outline

Outline

Outline

Outline

Outline

Outline

Principle of an encryption

Alice wants to send a confidential message m to *Bob* over a public channel.

In this situation they need a cryptosystem that consists in :

- An encryption algorithm E ;
- A decryption algorithm D ;
- A set of encryption keys and a set of decryption keys (they can be different) ;
- For each encryption key k there is a decryption key k^{-1} (not necessary unique) such that for each plaintext m

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

Principle of an encryption

Alice wants to send a confidential message m to *Bob* over a public channel.
In this situation they need a cryptosystem that consists in :

- An encryption algorithm E ;
- A decryption algorithm D ;
- A set of encryption keys and a set of decryption keys (they can be different) ;
- For each encryption key k there is a decryption key k^{-1} (not necessary unique) such that for each plaintext m

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

Principle of an encryption

Alice wants to send a confidential message m to *Bob* over a public channel.

In this situation they need a cryptosystem that consists in :

- An encryption algorithm E ;
- A decryption algorithm D ;
- A set of encryption keys and a set of decryption keys (they can be different) ;
- For each encryption key k there is a decryption key k^{-1} (not necessary unique) such that for each plaintext m

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

Principle of an encryption

Alice wants to send a confidential message m to *Bob* over a public channel.
In this situation they need a cryptosystem that consists in :

- An encryption algorithm E ;
- A decryption algorithm D ;
- A set of encryption keys and a set of decryption keys (they can be different) ;
- For each encryption key k there is a decryption key k^{-1} (not necessary unique) such that for each plaintext m

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

Principle of an encryption

Alice wants to send a confidential message m to *Bob* over a public channel.

In this situation they need a cryptosystem that consists in :

- An encryption algorithm E ;
- A decryption algorithm D ;
- A set of encryption keys and a set of decryption keys (they can be different) ;
- For each encryption key k there is a decryption key k^{-1} (not necessary unique) such that for each plaintext m

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

Principle of an encryption

Alice wants to send a confidential message m to *Bob* over a public channel.
In this situation they need a cryptosystem that consists in :

- An encryption algorithm E ;
- A decryption algorithm D ;
- A set of encryption keys and a set of decryption keys (they can be different) ;
- For each encryption key k there is a decryption key k^{-1} (not necessary unique) such that for each plaintext m

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

Principle of an encryption (cont'd)

- Alice computes the ciphertext c corresponding to the plaintext m and the encryption key k by

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

- Alice sends c to Bob on the public channel ;
- Bob recovers the plaintext m by

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

Note that Bob must know the decryption key corresponding to k.

Principle of an encryption (cont'd)

- Alice computes the ciphertext c corresponding to the plaintext m and the encryption key k by

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

- Alice sends c to Bob on the public channel ;
- Bob recovers the plaintext m by

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

Note that Bob must know the decryption key corresponding to k.

Principle of an encryption (cont'd)

- Alice computes the ciphertext c corresponding to the plaintext m and the encryption key k by

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

- Alice sends c to Bob on the public channel ;
- Bob recovers the plaintext m by

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

Note that Bob must know the decryption key corresponding to k.

Principle of an encryption (cont'd)

- Alice computes the ciphertext c corresponding to the plaintext m and the encryption key k by

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

- Alice sends c to Bob on the public channel ;
- Bob recovers the plaintext m by

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

Note that Bob must know the decryption key corresponding to k.

Principle of an encryption (cont'd)

- Alice computes the ciphertext c corresponding to the plaintext m and the encryption key k by

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

- Alice sends c to Bob on the public channel ;
- Bob recovers the plaintext m by

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

Note that Bob must know the decryption key corresponding to k.

Two main kinds of cryptosystems

- Secret-key (or symmetric) schemes : k and k^{-1} are identical and only known by Alice and Bob ;
- Public-key (or asymmetric) schemes : the encryption key k is public (known by everybody), the decryption key k^{-1} is a secret quantity only known by Bob.

Two main kinds of cryptosystems

- Secret-key (or symmetric) schemes : k and k^{-1} are identical and only known by Alice and Bob ;
- Public-key (or asymmetric) schemes : the encryption key k is public (known by everybody), the decryption key k^{-1} is a secret quantity only known by Bob.

Two main kinds of cryptosystems

- Secret-key (or symmetric) schemes : k and k^{-1} are identical and only known by Alice and Bob ;
- Public-key (or asymmetric) schemes : the encryption key k is public (known by everybody), the decryption key k^{-1} is a secret quantity only known by Bob.

Iterated Block Ciphers

A block cipher is a (secret-key) cryptosystem in which the plaintexts are divided into several blocks of bits of same length.
An iterated block cipher consists in an iterative application of a (keyed) round function f to a plaintext.
In an r-round iterated cipher we have

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

where x_0 is the plaintext, x_r is the ciphertext and $k_1, \ldots, k_r$ are the subkeys of each round (obtained from a main secret-key).
In such cryptosystems for any round key k the function $f_k : x \mapsto f(x, k)$ is a permutation.
Examples : DES, AES, ...

Iterated Block Ciphers

A block cipher is a (secret-key) cryptosystem in which the plaintexts are divided into several blocks of bits of same length.

An iterated block cipher consists in an iterative application of a (keyed) round function f to a plaintext.

In an r-round iterated cipher we have

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

where x_0 is the plaintext, x_r is the ciphertext and $k_1, \ldots, k_r$ are the subkeys of each round (obtained from a main secret-key).

In such cryptosystems for any round key k the function $f_k : x \mapsto f(x, k)$ is a permutation.

Examples : DES, AES, ...

Iterated Block Ciphers

A block cipher is a (secret-key) cryptosystem in which the plaintexts are divided into several blocks of bits of same length.

An iterated block cipher consists in an iterative application of a (keyed) round function f to a plaintext.

In an r-round iterated cipher we have

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

where x_0 is the plaintext, x_r is the ciphertext and $k_1, \ldots, k_r$ are the subkeys of each round (obtained from a main secret-key).

In such cryptosystems for any round key k the function $f_k : x \mapsto f(x, k)$ is a permutation.

Examples : DES, AES, ...

Iterated Block Ciphers

A block cipher is a (secret-key) cryptosystem in which the plaintexts are divided into several blocks of bits of same length.

An iterated block cipher consists in an iterative application of a (keyed) round function f to a plaintext.

In an r-round iterated cipher we have

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

where x_0 is the plaintext, x_r is the ciphertext and $k_1, \ldots, k_r$ are the subkeys of each round (obtained from a main secret-key).

In such cryptosystems for any round key k the function $f_k : x \mapsto f(x, k)$ is a permutation.

Examples : DES, AES, . . .

Iterated Block Ciphers

A block cipher is a (secret-key) cryptosystem in which the plaintexts are divided into several blocks of bits of same length.
An iterated block cipher consists in an iterative application of a (keyed) round function f to a plaintext.
In an r-round iterated cipher we have

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

where x_0 is the plaintext, x_r is the ciphertext and $k_1, \ldots, k_r$ are the subkeys of each round (obtained from a main secret-key).
In such cryptosystems for any round key k the function $f_k : x \mapsto f(x, k)$ is a permutation.
Examples : DES, AES, $\ldots$

Iterated Block Ciphers

A block cipher is a (secret-key) cryptosystem in which the plaintexts are divided into several blocks of bits of same length.
An iterated block cipher consists in an iterative application of a (keyed) round function f to a plaintext.
In an r-round iterated cipher we have

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

where x_0 is the plaintext, x_r is the ciphertext and $k_1, \ldots, k_r$ are the subkeys of each round (obtained from a main secret-key).
In such cryptosystems for any round key k the function $f_k : x \mapsto f(x, k)$ is a permutation.
Examples : DES, AES, ...

Outline

Brute force attack (or exhaustive search)

Algorithm

Given a ciphertext c, try all the possible secret-keys k such that $D(c, k)$ gives a "correct" plaintext.

If the key length is l then this attack needs an average of 2^{l-1} tries. (If $l = 128$ bits a cryptosystem is supposed to be secure against such an attack.)

A cryptosystem is secure if it is not vulnerable to a cryptanalysis which is more efficient than the exhaustive search.

Brute force attack (or exhaustive search)

Algorithm

Given a ciphertext c, try all the possible secret-keys k such that $D(c, k)$ gives a "correct" plaintext.

If the key length is l then this attack needs an average of 2^{l-1} tries. (If $l = 128$ bits a cryptosystem is supposed to be secure against such an attack.)

A cryptosystem is secure if it is not vulnerable to a cryptanalysis which is more efficient than the exhaustive search.

Brute force attack (or exhaustive search)

Algorithm

Given a ciphertext c, try all the possible secret-keys k such that $D(c, k)$ gives a "correct" plaintext.

If the key length is l then this attack needs an average of 2^{l-1} tries. (If $l = 128$ bits a cryptosystem is supposed to be secure against such an attack.)
A cryptosystem is secure if it is not vulnerable to a cryptanalysis which is more efficient than the exhaustive search.

Last-round attacks on iterated block ciphers

Objective

Recover the last round key k_r from the knowledge of some pairs of plaintexts and corresponding ciphertexts.

Last-round attacks on iterated block ciphers (cont'd)

Principle

- Distinguish the reduced cipher, $G = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$, from a random permutation for all round keys $k_1, \ldots, k_r$.
- If such a discriminator can be found, some information on k_r can be recovered by checking wheter, for a given value k_r, the function

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

satisfies this property or not, where x_0 (resp. x_r) denotes the plaintext (resp. the ciphertext).
The values of k_r for which the expected statistical bias is observed are candidates for the correct last-round key.

Last-round attacks on iterated block ciphers (cont'd)

Principle

- Distinguish the reduced cipher, $G = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$, from a random permutation for all round keys $k_1, \ldots, k_r$.
- If such a discriminator can be found, some information on k_r can be recovered by checking wheter, for a given value k_r, the function

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

satisfies this property or not, where x_0 (resp. x_r) denotes the plaintext (resp. the ciphertext).
The values of k_r for which the expected statistical bias is observed are candidates for the correct last-round key.

Last-round attacks on iterated block ciphers (cont'd)

Principle

- Distinguish the reduced cipher, $G = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$, from a random permutation for all round keys $k_1, \ldots, k_r$.
- If such a discriminator can be found, some information on k_r can be recovered by checking wheter, for a given value k_r, the function

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

satisfies this property or not, where x_0 (resp. x_r) denotes the plaintext (resp. the ciphertext).
The values of k_r for which the expected statistical bias is observed are candidates for the correct last-round key.

Last-round attacks on iterated block ciphers (cont'd)

Different discriminators

Different discriminators can be exploited :

- The reduced cipher G has a derivative, $d_\alpha G : x \mapsto G(x \oplus \alpha) \oplus G(x)$, which is not uniformly distributed. This discriminator leads to a differential attack ;
- There exists a linear combination of the n output bits of the reduced cipher which is close to an affine function. This leads to a linear attack ;
- The reduced cipher, seen as a univariate polynomial in $GF(2^m)[X]$, is close to a low-degree polynomial. This leads to an interpolation attack.

Last-round attacks on iterated block ciphers (cont'd)

Different discriminators

Different discriminators can be exploited :

- The reduced cipher G has a derivative, $d_\alpha G : x \mapsto G(x \oplus \alpha) \oplus G(x)$, which is not uniformly distributed. This discriminator leads to a differential attack ;
- There exists a linear combination of the n output bits of the reduced cipher which is close to an affine function. This leads to a linear attack ;
- The reduced cipher, seen as a univariate polynomial in $GF(2^m)[X]$, is close to a low-degree polynomial. This leads to an interpolation attack.

Last-round attacks on iterated block ciphers (cont'd)

Different discriminators

Different discriminators can be exploited :

- The reduced cipher G has a derivative, $d_\alpha G : x \mapsto G(x \oplus \alpha) \oplus G(x)$, which is not uniformly distributed. This discriminator leads to a differential attack ;
- There exists a linear combination of the n output bits of the reduced cipher which is close to an affine function. This leads to a linear attack ;
- The reduced cipher, seen as a univariate polynomial in $GF(2^m)[X]$, is close to a low-degree polynomial. This leads to an interpolation attack.

Last-round attacks on iterated block ciphers (cont'd)

Different discriminators

Different discriminators can be exploited :

- The reduced cipher G has a derivative, $d_\alpha G : x \mapsto G(x \oplus \alpha) \oplus G(x)$, which is not uniformly distributed. This discriminator leads to a differential attack ;
- There exists a linear combination of the n output bits of the reduced cipher which is close to an affine function. This leads to a linear attack ;
- The reduced cipher, seen as a univariate polynomial in $GF(2^m)[X]$, is close to a low-degree polynomial. This leads to an interpolation attack.

Differential cryptanalysis (Biham & Shamir)

- Find a differential (α, β) so that

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

is far from the uniform distribution ;
- Choose at random a plaintext x_0 and encrypt both x_0 and $x_0 \oplus \alpha$. We obtain two pairs of plaintexts and ciphertexts (x_0, x_r) and $(x_0 \oplus \alpha, x'_r)$;
- Find all possible values of the last round key $\widehat{k_r}$ such that

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

- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occurs more than the others. It will be considered as the last round subkey.

Differential cryptanalysis (Biham & Shamir)

- Find a differential (α, β) so that

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

  is far from the uniform distribution ;
- Choose at random a plaintext x_0 and encrypt both x_0 and $x_0 \oplus \alpha$. We obtain two pairs of plaintexts and ciphertexts (x_0, x_r) and $(x_0 \oplus \alpha, x_r')$;
- Find all possible values of the last round key $\widehat{k_r}$ such that

$$f_{\widehat{k_r}}^{-1}(x_r) \oplus f_{\widehat{k_r}}^{-1}(x_r') = \beta \text{ ;}$$

- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occurs more than the others. It will be considered as the last round subkey.

Differential cryptanalysis (Biham & Shamir)

- Find a differential (α, β) so that

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

  is far from the uniform distribution ;
- Choose at random a plaintext x_0 and encrypt both x_0 and $x_0 \oplus \alpha$. We obtain two pairs of plaintexts and ciphertexts (x_0, x_r) and $(x_0 \oplus \alpha, x_r')$;
- Find all possible values of the last round key $\widehat{k}_r$ such that

$$f_{\widehat{k}_r}^{-1}(x_r) \oplus f_{\widehat{k}_r}^{-1}(x_r') = \beta \ ;$$

- Iterate the third and fourth steps until one of the values of $\widehat{k}_r$ occurs more than the others. It will be considered as the last round subkey.

Differential cryptanalysis (Biham & Shamir)

- Find a differential (α, β) so that
$$\Pr(G(x) \oplus G(x \oplus \alpha) = \beta)$$
is far from the uniform distribution ;
- Choose at random a plaintext x_0 and encrypt both x_0 and $x_0 \oplus \alpha$. We obtain two pairs of plaintexts and ciphertexts (x_0, x_r) and $(x_0 \oplus \alpha, x'_r)$;
- Find all possible values of the last round key $\widehat{k_r}$ such that
$$f^{-1}_{\widehat{k_r}}(x_r) \oplus f^{-1}_{\widehat{k_r}}(x'_r) = \beta \;;$$
- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occurs more than the others. It will be considered as the last round subkey.

Differential cryptanalysis (Biham & Shamir)

- Find a differential (α, β) so that

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

is far from the uniform distribution ;

- Choose at random a plaintext x_0 and encrypt both x_0 and $x_0 \oplus \alpha$. We obtain two pairs of plaintexts and ciphertexts (x_0, x_r) and $(x_0 \oplus \alpha, x'_r)$;
- Find all possible values of the last round key $\widehat{k_r}$ such that

$$f_{\widehat{k_r}}^{-1}(x_r) \oplus f_{\widehat{k_r}}^{-1}(x'_r) = \beta \text{ ;}$$

- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occurs more than the others. It will be considered as the last round subkey.

Linear cryptanalysis (Matsui)

- Find a mask (α, β) so that the equation
$$\alpha.x_0 \oplus \beta.G(x_0) = 0$$
is satisfied for most plaintexts x_0 and round keys $k_1, \ldots, k_{r-1}$;
- Choose at random a plaintext x_0 and compute its ciphertext x_r ;
- Find all possible values of the last round key $\widehat{k_r}$ such that
$$\alpha.x_0 \oplus \beta.f^{-1}_{\widehat{k_r}}(x_r) = 0 \ ;$$
- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occcurs more than the others. It will be considered as the last round subkey.

Linear cryptanalysis (Matsui)

- Find a mask (α, β) so that the equation

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

  is satisfied for most plaintexts x_0 and round keys $k_1, \ldots, k_{r-1}$;
- Choose at random a plaintext x_0 and compute its ciphertext x_r ;
- Find all possible values of the last round key $\widehat{k_r}$ such that

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

- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occcurs more than the others. It will be considered as the last round subkey.

Linear cryptanalysis (Matsui)

- Find a mask (α, β) so that the equation

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

  is satisfied for most plaintexts x_0 and round keys $k_1, \ldots, k_{r-1}$;
- Choose at random a plaintext x_0 and compute its ciphertext x_r ;
- Find all possible values of the last round key $\widehat{k_r}$ such that

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

- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occcurs more than the others. It will be considered as the last round subkey.

Linear cryptanalysis (Matsui)

- Find a mask (α, β) so that the equation

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

  is satisfied for most plaintexts x_0 and round keys $k_1, \ldots, k_{r-1}$;
- Choose at random a plaintext x_0 and compute its ciphertext x_r ;
- Find all possible values of the last round key $\widehat{k_r}$ such that

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

- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occcurs more than the others. It will be considered as the last round subkey.

Linear cryptanalysis (Matsui)

- Find a mask (α, β) so that the equation

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

  is satisfied for most plaintexts x_0 and round keys $k_1, \ldots, k_{r-1}$;
- Choose at random a plaintext x_0 and compute its ciphertext x_r ;
- Find all possible values of the last round key $\widehat{k_r}$ such that

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

- Iterate the third and fourth steps until one of the values of $\widehat{k_r}$ occcurs more than the others. It will be considered as the last round subkey.

Resistances against differential and linear attacks

In most cases, differential and/or linear weaknesses of the reduced cipher can be detected only if the round function f presents a similar default. Then the round function should satisfy the following property for any round key k :

- For any nonzero block α, the distribution of differences $f_k(x \oplus \alpha) \oplus f_k(x)$ should be close to the uniform distribution (Boolean perfect nonlinear functions) ;
- For any nonzero block β, the Boolean function $x \mapsto \beta.f_k(x)$ should be far away from all affine functions (Boolean bent functions).

Resistances against differential and linear attacks

In most cases, differential and/or linear weaknesses of the reduced cipher can be detected only if the round function f presents a similar default. Then the round function should satisfy the following property for any round key k :

- For any nonzero block α, the distribution of differences $f_k(x \oplus \alpha) \oplus f_k(x)$ should be close to the uniform distribution (Boolean perfect nonlinear functions) ;
- For any nonzero block β, the Boolean function $x \mapsto \beta.f_k(x)$ should be far away from all affine functions (Boolean bent functions).

Resistances against differential and linear attacks

In most cases, differential and/or linear weaknesses of the reduced cipher can be detected only if the round function f presents a similar default. Then the round function should satisfy the following property for any round key k :

- For any nonzero block α, the distribution of differences $f_k(x \oplus \alpha) \oplus f_k(x)$ should be close to the uniform distribution (Boolean perfect nonlinear functions) ;
- For any nonzero block β, the Boolean function $x \mapsto \beta.f_k(x)$ should be far away from all affine functions (Boolean bent functions).

Resistances against differential and linear attacks

In most cases, differential and/or linear weaknesses of the reduced cipher can be detected only if the round function f presents a similar default. Then the round function should satisfy the following property for any round key k :

- For any nonzero block α, the distribution of differences $f_k(x \oplus \alpha) \oplus f_k(x)$ should be close to the uniform distribution (Boolean perfect nonlinear functions) ;
- For any nonzero block β, the Boolean function $x \mapsto \beta.f_k(x)$ should be far away from all affine functions (Boolean bent functions).

Resistances against differential and linear attacks

In most cases, differential and/or linear weaknesses of the reduced cipher can be detected only if the round function f presents a similar default. Then the round function should satisfy the following property for any round key k :

- For any nonzero block α, the distribution of differences $f_k(x \oplus \alpha) \oplus f_k(x)$ should be close to the uniform distribution (Boolean perfect nonlinear functions) ;
- For any nonzero block β, the Boolean function $x \mapsto \beta.f_k(x)$ should be far away from all affine functions (Boolean bent functions).

Outline

History

Definition (Nyberg, 1991)

A function $f : \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^n$ is perfect nonlinear if for each nonzero α in $\mathbb{Z}_2^m$ and for each $\beta \in \mathbb{Z}_2^n$,

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

Ensure the maximal resistance against the differential attack.

In the finite abelian groups setting (1)

For a group G, 0_G is its identity element and $G^* = G \setminus \{0_G\}$.

Definition

Let G and H be two finite abelian groups and $f : G \to H$.

- f is balanced if for each $\beta \in H$,
$$|\{x \in G | f(x) = \beta\}| = \frac{|G|}{|H|}\ ;$$
- The derivative of f with respect to $\alpha \in G$ is defined by

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

In the finite abelian groups setting (2)

Definition

A function $f : G \to H$ is (classical) perfect nonlinear if $\forall \alpha \in G^*$, $d_\alpha f$ is balanced, *i.e.* $\forall \alpha \in G^*$ and $\forall \beta \in H$,

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

Remark

If G is a nonabelian group, such a function is called left-perfect nonlinear.

In the finite abelian groups setting (2)

Definition

A function $f : G \to H$ is (classical) perfect nonlinear if $\forall \alpha \in G^*$, $d_\alpha f$ is balanced, *i.e.* $\forall \alpha \in G^*$ and $\forall \beta \in H$,

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

Remark

If G is a nonabelian group, such a function is called left-perfect nonlinear.

In the finite abelian groups setting (2)

Definition

A function $f : G \to H$ is (classical) perfect nonlinear if $\forall \alpha \in G^*$, $d_\alpha f$ is balanced, *i.e.* $\forall \alpha \in G^*$ and $\forall \beta \in H$,

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

Remark

If G is a nonabelian group, such a function is called left-perfect nonlinear.

Equivalent characterizations

(Traditional) perfect nonlinearity $\Leftrightarrow$

- By the Fourier transform : notion of bentness ;
- Combinatorial characterization by difference sets.

Equivalent characterizations

(Traditional) perfect nonlinearity ⇔

- By the Fourier transform : notion of bentness ;
- Combinatorial characterization by difference sets.

Equivalent characterizations

(Traditional) perfect nonlinearity $\Leftrightarrow$

- By the Fourier transform : notion of bentness ;
- Combinatorial characterization by difference sets.

Outline

History

Definition (Dillon 1974, Rothaus 1976)

A function $f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$ is bent if for each $\alpha \in \mathbb{Z}_2^m$,

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

Ensure the maximal resistance against the linear attack.

Example

The following mapping

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

is a bent function.

In the finite abelian groups setting (1)

The dual group of G, denoted $\widehat{G}$, is the set of all group homomorphisms from G to $\mathbb{U}$ together with the pointwise multiplication.
It is isomorphic to G itself. Its elements are called characters : for $\alpha \in G$, the character corresponding to α (under the isomorphism) is denoted χ_G^α.
For instance if G is $\mathbb{Z}_2^m$ and $\alpha \in \mathbb{Z}_2^m$, then $\chi_G^\alpha(x) = (-1)^{\alpha.x}$.

In the finite abelian groups setting (1)

The dual group of G, denoted $\widehat{G}$, is the set of all group homomorphisms from G to $\mathbb{U}$ together with the pointwise multiplication.
It is isomorphic to G itself. Its elements are called characters : for $\alpha \in G$, the character corresponding to α (under the isomorphism) is denoted χ_G^{α}.
For instance if G is $\mathbb{Z}_2^m$ and $\alpha \in \mathbb{Z}_2^m$, then $\chi_G^{\alpha}(x) = (-1)^{\alpha.x}$.

In the finite abelian groups setting (2)

Definition

Let G be a finite abelian group and $\varphi : G \longrightarrow \mathbb{C}$. The (discrete) Fourier transform of φ is the function $\widehat{\varphi}$ defined as

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

Dual characterization

Theorem (Carlet & Ding and Pott, 2004)

Let G and H be two finite abelian groups. Let $f : G \rightarrow H$. The function f is perfect nonlinear if and only if $\forall \alpha \in G$, $\forall \beta \in H^*$,

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

When $G = \mathbb{Z}_2^m$ and $H = \mathbb{Z}_2$, this is the classical notion of bentness introduced by Dillon.

Dual characterization

Theorem (Carlet & Ding and Pott, 2004)

Let G and H be two finite abelian groups. Let $f : G \to H$. The function f is perfect nonlinear if and only if $\forall \alpha \in G$, $\forall \beta \in H^*$,

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

When $G = \mathbb{Z}_2^m$ and $H = \mathbb{Z}_2$, this is the classical notion of bentness introduced by Dillon.

Impossible cases

Due to implementation constraints we are interested in Boolean functions $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ but Boolean bent functions only exist when m is an even integer and $m \geq 2n$.

Impossible cases : odd dimension (m is an odd integer) and plane dimension ($m = n$).

Impossible cases

Due to implementation constraints we are interested in Boolean functions $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ but Boolean bent functions only exist when m is an even integer and $m \geq 2n$.
Impossible cases : odd dimension (m is an odd integer) and plane dimension ($m = n$).

Outline

Definition

Let G be a finite group. Let $D \subset G$. D is a (v, k, λ) difference set of G if

- $v = |G|$;
- $k = |D|$;
- For each $\alpha \in G^*$, the equation $x - y = \alpha$ has λ solutions (x, y) in D^2.

Definition

Let G be a finite group. Let $D \subset G$. D is a (v, k, λ) difference set of G if

- $v = |G|$;
- $k = |D|$;
- For each $\alpha \in G^*$, the equation $x - y = \alpha$ has λ solutions (x, y) in D^2.

Definition

Let G be a finite group. Let $D \subset G$. D is a (v, k, λ) difference set of G if

- $v = |G|$;
- $k = |D|$;
- For each $\alpha \in G^*$, the equation $x - y = \alpha$ has λ solutions (x, y) in D^2.

Definition

Let G be a finite group. Let $D \subset G$. D is a (v, k, λ) difference set of G if

- $v = |G|$;
- $k = |D|$;
- For each $\alpha \in G^*$, the equation $x - y = \alpha$ has λ solutions (x, y) in D^2.

Hadamard difference set

Definition

A (v, k, λ) difference set D of G is a Hadamard difference set if

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

Combinatorial characterization

Theorem (Carlet & Ding, 2004)

Let G be a finite abelian group such that $|G| = 4n^2$. A function $f : G \longrightarrow \mathbb{Z}_2$ is perfect nonlinear if and only if its support $S_f = \{x \in G | f(x) = 1\}$ is a Hadamard difference set of G.

This is a generalization of a result of Dillon (1974) concerning Boolean functions.

Combinatorial characterization (cont'd)

Theorem (Plott, 2004)

If G and H are two finite groups then a function $f : G \to H$ is (left-)perfect nonlinear if and only if $\{(x, f(x)) | x \in G\} \subset G \times H$ is a splitting semiregular $(|G|, |H|, |G|, \frac{|G|}{|H|})$ difference set of $G \times H$ relative to $\{0_G\} \times H$.

Outline

- Cryptography ;
- Mobile communications.

- Cryptography ;
- Mobile communications.

- Cryptography ;
- Mobile communications.

Mobile communications (1) : Code Division Multiple Access (CDMA)

Definition

Two vectors $u = (u_1, \ldots, u_m)$ and $v = (v_1, \ldots, v_m)$ are called orthogonal if

$$u.v = \sum_{i=1}^{m} u_i v_i = 0 \ .$$

For instance $u = (1, 1, 1, -1)$ and $v = (1, -1, 1, 1)$ are othogonal.

Mobile communications (2) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (2) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (2) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (2) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (3) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (3) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (3) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (3) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (3) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (4) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communication (5) : CDMA

Let $f : \mathbb{Z}_m \to \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha + 1), \ldots, f(\alpha + m - 1)) \ .$$

In particular $u_0 = (f(0), f(1), \ldots, f(m - 1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Mobile communication (5) : CDMA

Let $f : \mathbb{Z}_m \to \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha + 1), \ldots, f(\alpha + m - 1)) .$$

In particular $u_0 = (f(0), f(1), \ldots, f(m - 1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Mobile communication (5) : CDMA

Let $f : \mathbb{Z}_m \to \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha + 1), \dots, f(\alpha + m - 1)) \ .$$

In particular $u_0 = (f(0), f(1), \dots, f(m - 1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Mobile communication (5) : CDMA

Let $f : \mathbb{Z}_m \rightarrow \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha + 1), \ldots, f(\alpha + m - 1)) \ .$$

In particular $u_0 = (f(0), f(1), \ldots, f(m - 1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Outline

- Recall on group actions ;
- Group action based perfect nonlinearity.

Outline

Group actions (1)

Let $(G, *)$ be any group and X be a nonempty set.
A (left) group action of G on X is a group homomorphism ϕ from G to the symmetric group $S(X)$ of X (the group of permutations over X).
In particular,

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

Group actions (1)

Let $(G,*)$ be any group and X be a nonempty set.
A (left) group action of G on X is a group homomorphism ϕ from G to the symmetric group $S(X)$ of X (the group of permutations over X).
In particular,

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

Group actions (2)

Notation

For $x \in X$ and $g \in G$, we write

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

Group actions (3)

Let G be a group that acts on a nonempty set X.
For $x \in X$, the orbital function of x is defined as

$$\begin{array}{rccc} \phi_x : & G & \to & X \\ & g & \mapsto & g.x \end{array}$$

Group actions (4)

Definition

The action ϕ of G on X is

- faithful if ϕ is one-to-one ;
- regular if for each $x \in X$, ϕ_x is a bijective function.

Examples

- The natural action of $S(X)$ on X is faithful : for $\pi \in S(X)$ and $x \in X$, $\pi.x = \pi(x)$;
- The action of G on itself by (left) translation is regular : for α and x in G, $\alpha.x = \alpha + x$.

Group actions (4)

Definition

The action ϕ of G on X is

- faithful if ϕ is one-to-one ;
- regular if for each $x \in X$, ϕ_x is a bijective function.

Examples

- The natural action of $S(X)$ on X is faithful : for $\pi \in S(X)$ and $x \in X$, $\pi.x = \pi(x)$;
- The action of G on itself by (left) translation is regular : for α and x in G, $\alpha.x = \alpha + x$.

Group actions (4)

Definition

The action ϕ of G on X is

- faithful if ϕ is one-to-one ;
- regular if for each $x \in X$, ϕ_x is a bijective function.

Examples

- The natural action of $S(X)$ on X is faithful : for $\pi \in S(X)$ and $x \in X$, $\pi.x = \pi(x)$;
- The action of G on itself by (left) translation is regular : for α and x in G, $\alpha.x = \alpha + x$.

Group actions (4)

Definition

The action ϕ of G on X is

- faithful if ϕ is one-to-one ;
- regular if for each $x \in X$, ϕ_x is a bijective function.

Examples

- The natural action of $S(X)$ on X is faithful : for $\pi \in S(X)$ and $x \in X$, $\pi.x = \pi(x)$;
- The action of G on itself by (left) translation is regular : for α and x in G, $\alpha.x = \alpha + x$.

Outline

Definitions (1)

Let G be a finite group (not necessary abelian) that (left) acts at least **faithfully** on a finite nonempty set X and let H be a finite abelian group (in an additive representation). Let $f : X \to H$.

The (left) derivative of f with respect to $g \in G$ is defined as

$$\begin{array}{rccl} D_g f : & X & \to & H \\ & x & \mapsto & f(g.x) - f(x) \ . \end{array}$$

This is exactly the classical notion of derivative where the addition $\alpha + x$ is replaced by the group action $\alpha.x$.

Definitions (1)

Let G be a finite group (not necessary abelian) that (left) acts at least **faithfully** on a finite nonempty set X and let H be a finite abelian group (in an additive representation). Let $f : X \to H$.

The (left) derivative of f with respect to $g \in G$ is defined as

$$\begin{array}{rccl} D_g f : & X & \to & H \\ & x & \mapsto & f(g.x) - f(x) . \end{array}$$

This is exactly the classical notion of derivative where the addition $\alpha + x$ is replaced by the group action $\alpha . x$.

Definitions (1)

Let G be a finite group (not necessary abelian) that (left) acts at least **faithfully** on a finite nonempty set X and let H be a finite abelian group (in an additive representation). Let $f : X \to H$.

The (left) derivative of f with respect to $g \in G$ is defined as

$$\begin{array}{cccc} D_g f : & X & \to & H \\ & x & \mapsto & f(g.x) - f(x) \,. \end{array}$$

This is exactly the classical notion of derivative where the addition $\alpha + x$ is replaced by the group action $\alpha.x$.

Definitions (2)

Definition

The function $f : X \to H$ is called G-perfect nonlinear if $\forall g \in G^*$, $D_g f$ is balanced, i.e. $\forall g \in G^*$ et $\forall \beta \in H$,

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

Definitions (2)

Definition

The function $f : X \to H$ is called G-perfect nonlinear if $\forall g \in G^*$, $D_g f$ is balanced, *i.e.* $\forall g \in G^*$ et $\forall \beta \in H$,

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

Definitions (3)

Remark

Since the action of G on X is faithful, there is no $g \in G^*$ such that the map

$$\begin{array}{rccc} D_g : & H^X & \to & H^X \\ & f & \mapsto & D_g f \end{array}$$

is identically null (*i.e.* for each $f : X \to H$ and for each $x \in X$, $D_g f(x) = 0_H$).

First results

Proposition

Let $T(G)$ be the group of translations of G.
A function $f : G \to H$ is $T(G)$-perfect nonlinear if and only if f is classical (left) perfect nonlinear.

Proposition

Let $f : X \to H$.
If f is G-perfect nonlinear then for each subgroup G' of G, f is also G'-perfect nonlinear.

First results

Proposition

Let $T(G)$ be the group of translations of G.
A function $f : G \to H$ is $T(G)$-perfect nonlinear if and only if f is classical (left) perfect nonlinear.

Proposition

Let $f : X \to H$.
If f is G-perfect nonlinear then for each subgroup G' of G, f is also G'-perfect nonlinear.

Objective

- Traditional duality :
  Perfect nonlinearity $\Leftrightarrow$ Bentness (Carlet & Ding).
- Generalized duality :
  G-perfect nonlinearity $\Leftrightarrow$??

Objective

- Traditional duality :
  Perfect nonlinearity $\Leftrightarrow$ Bentness (Carlet & Ding).
- Generalized duality :
  G-perfect nonlinearity $\Leftrightarrow$??

Outline

1. G is an abelian group ;
2. G is a nonabelian group.

Outline

Assumptions and Notation

Let given (G, H, X) such that

- G and H are both finite abelian group ;
- X is a finite nonempty set ;
- G acts (at least) faithfully on X (by ϕ).

For $f : X \to Y$ and $x \in X$, we define $f_x : G \to Y$ by

$$f_x = f \circ \phi_x \ .$$

Assumptions and Notation

Let given (G, H, X) such that

- G and H are both finite abelian group ;
- X is a finite nonempty set ;
- G acts (at least) faithfully on X (by ϕ).

For $f : X \to Y$ and $x \in X$, we define $f_x : G \to Y$ by

$$f_x = f \circ \phi_x \ .$$

Assumptions and Notation

Let given (G, H, X) such that

- G and H are both finite abelian group ;
- X is a finite nonempty set ;
- G acts (at least) faithfully on X (by ϕ).

For $f : X \to Y$ and $x \in X$, we define $f_x : G \to Y$ by

$$f_x = f \circ \phi_x \ .$$

Assumptions and Notation

Let given (G, H, X) such that

- G and H are both finite abelian group ;
- X is a finite nonempty set ;
- G acts (at least) faithfully on X (by ϕ).

For $f : X \to Y$ and $x \in X$, we define $f_x : G \to Y$ by

$$f_x = f \circ \phi_x \ .$$

Assumptions and Notation

Let given (G, H, X) such that

- G and H are both finite abelian group ;
- X is a finite nonempty set ;
- G acts (at least) faithfully on X (by ϕ).

For $f : X \to Y$ and $x \in X$, we define $f_x : G \to Y$ by

$$f_x = f \circ \phi_x \ .$$

Dual characterization

Theorem

A function $f : X \to H$ is G-perfect nonlinear if and only if for each $\beta \in H^*$ and for each $g \in G$,

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

Informally speaking, f is G-perfect nonlinear if and only if f_x is bent on average over all $x \in X$.

Dual characterization

Theorem

A function $f : X \to H$ is G-perfect nonlinear if and only if for each $\beta \in H^*$ and for each $g \in G$,

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

Informally speaking, f is G-perfect nonlinear if and only if f_x is bent on average over all $x \in X$.

Outline

Outline

- Assumptions ;
- Recall on the theory of linear representations of groups ;
- Dual characterization of left-perfect nolinearity ;
- Dual characterization of G-perfect nonlinearity.

Outline

- Assumptions ;
- Recall on the theory of linear representations of groups ;
- Dual characterization of left-perfect nolinearity ;
- Dual characterization of G-perfect nonlinearity.

Outline

- Assumptions ;
- Recall on the theory of linear representations of groups ;
- Dual characterization of left-perfect nolinearity ;
- Dual characterization of G-perfect nonlinearity.

Outline

- Assumptions ;
- Recall on the theory of linear representations of groups ;
- Dual characterization of left-perfect nolinearity ;
- Dual characterization of G-perfect nonlinearity.

Outline

- Assumptions ;
- Recall on the theory of linear representations of groups ;
- Dual characterization of left-perfect nolinearity ;
- Dual characterization of G-perfect nonlinearity.

Assumptions

Let given (G, H, X) such that

- G is a finite nonabelian group ;
- H is a finite abelian group ;
- X is a finite nonempty set on which G left acts at least faithfully.

Assumptions

Let given (G, H, X) such that

- G is a finite nonabelian group ;
- H is a finite abelian group ;
- X is a finite nonempty set on which G left acts at least faithfully.

Assumptions

Let given (G, H, X) such that

- G is a finite nonabelian group ;
- H is a finite abelian group ;
- X is a finite nonempty set on which G left acts at least faithfully.

Assumptions

Let given (G, H, X) such that

- G is a finite nonabelian group ;
- H is a finite abelian group ;
- X is a finite nonempty set on which G left acts at least faithfully.

Recall on linear representations (1)

Definition

Let V be a $\mathbb{C}$-vector space of finite dimension $\dim_{\mathbb{C}}(V)$.
The unitary group $\mathbb{U}(V)$ is the group of bijective linear functions U such that $U^{-1} = U^*$.
A (unitary) linear representation of G on V is a group homorphism $\rho : G \to \mathbb{U}(V)$.

Recall on linear representations (1)

Definition

Let V be a $\mathbb{C}$-vector space of finite dimension $\dim_{\mathbb{C}}(V)$. The unitary group $\mathbb{U}(V)$ is the group of bijective linear functions U such that $U^{-1} = U^*$.
A (unitary) linear representation of G on V is a group homorphism $\rho : G \to \mathbb{U}(V)$.

Recall on linear representations (1)

Definition

Let V be a $\mathbb{C}$-vector space of finite dimension $\dim_{\mathbb{C}}(V)$.
The unitary group $\mathbb{U}(V)$ is the group of bijective linear functions U such that $U^{-1} = U^*$.
A (unitary) linear representation of G on V is a group homorphism $\rho : G \to \mathbb{U}(V)$.

Recall on linear representations (2)

Let $\rho : G \to \mathbb{U}(V)$ be a linear representation.

A subvector space W of V is said stable with respect to ρ if for each $g \in G$, the image by $\rho(g)$ of each element of W belongs to W.

A representation $\rho : G \to \mathbb{U}(V)$ is called irreducible if V and $\{0_V\}$ are the ony stable subvector spaces of V (with respect to ρ).

Recall on linear representations (2)

Let $\rho : G \rightarrow \mathbb{U}(V)$ be a linear representation.
A subvector space W of V is said stable with respect to ρ if for each $g \in G$, the image by $\rho(g)$ of each element of W belongs to W.
A representation $\rho : G \rightarrow \mathbb{U}(V)$ is called irreducible if V and $\{0_V\}$ are the ony stable subvector spaces of V (with respect to ρ).

Recall on linear representations (3)

Definition

Two representations ρ_1 and ρ_2 of G respectively on the vector spaces V_1 and V_2 are isomorphic if there is a vector space isomorphism $\Psi : V_1 \to V_2$ such that for all $g \in G$,

$$\Psi \circ \rho_1(g) = \rho_2(g) \circ \Psi \ .$$

Recall on linear representations (4)

One denotes $\widehat{G}$ a system of representatives of equivalence classes of irreducible representations of a given group G.

If G is commutative then $\widehat{G}$ is the dual group of G.

Unfortunatly if G is nonabelian then $\widehat{G}$ is no more a group !

Recall on linear representations (4)

One denotes $\widehat{G}$ a system of representatives of equivalence classes of irreducible representations of a given group G.

If G is commutative then $\widehat{G}$ is the dual group of G.

Unfortunatly if G is nonabelian then $\widehat{G}$ is no more a group !

Recall on linear representations (4)

One denotes $\widehat{G}$ a system of representatives of equivalence classes of irreducible representations of a given group G.

If G is commutative then $\widehat{G}$ is the dual group of G.

Unfortunatly if G is nonabelian then $\widehat{G}$ is no more a group !

Recall on linear representations (5)

Definition

Let $\varphi : G \rightarrow \mathbb{C}$ and $\rho \in \widehat{G}$ (associated with the vector space V). The Fourier transform of φ in ρ is given by

$$\widehat{\varphi}(\rho) = \sum_{x \in G} \varphi(x)\rho(x) \in End(V) \ .$$

Dual characterisation of left-perfect nonlinearity

Recall

Let G be a finite nonabelian group and H a finite abelian group. Let $f : G \to H$.
The function f is (left) perfect nonlinear if $\forall \alpha \in G^*$, $d_\alpha f : x \mapsto f(\alpha + x) - f(x)$ is balanced.

Theorem

A function $f : G \to H$ is (left) perfect nonlinear if and only if $\forall \beta \in H^*$ and $\forall \rho \in \widehat{G}$ ($\rho : G \to \mathbb{U}(V)$),

$$(\widehat{\chi_H^\beta \circ f(\rho)}) \circ (\widehat{\chi_H^\beta \circ f(\rho)})^* = |G| Id_V .$$

Dual characterisation of left-perfect nonlinearity

Recall

Let G be a finite nonabelian group and H a finite abelian group. Let $f : G \to H$.
The function f is (left) perfect nonlinear if $\forall \alpha \in G^*$, $d_\alpha f : x \mapsto f(\alpha + x) - f(x)$ is balanced.

Theorem

A function $f : G \to H$ is (left) perfect nonlinear if and only if $\forall \beta \in H^*$ and $\forall \rho \in \widehat{G}$ ($\rho : G \to \mathbb{U}(V)$),

$$(\widehat{\chi_H^\beta \circ f}(\rho)) \circ (\widehat{\chi_H^\beta \circ f}(\rho))^* = |G| Id_V \,.$$

Dual characterisation of left-perfect nonlinear (cont'd)

Using the trace of endomorphisms, we obtain

$$\| \widehat{\chi_H^{\beta} \circ f}(\rho) \|^2 = |G| \dim_{\mathbb{C}}(V) \ .$$

Question

Is it a sufficient condition for (left) perfect nonlinearity ?

Dual characterisation of left-perfect nonlinear (cont'd)

Using the trace of endomorphisms, we obtain

$$\| \widehat{\chi_H^{\beta} \circ f}(\rho) \|^2 = |G| \dim_{\mathbb{C}}(V) \ .$$

Question

Is it a sufficient condition for (left) perfect nonlinearity ?

Dual characterisation of G-perfect nonlinearity

Recall

Let G be a finite nonabelian group that acts (at least faithfully) on a finite nonempty set X and let H be a finite abelian group. Let $f : X \to H$.
The function f is G-perfect nonlinear if $\forall g \in G^*$, $D_g f : x \mapsto f(g.x) - f(x)$ is balanced.

Objective

Find the dual characterization of such G-perfect nonlinear functions.

Dual characterisation of G-perfect nonlinearity

Recall

Let G be a finite nonabelian group that acts (at least faithfully) on a finite nonempty set X and let H be a finite abelian group. Let $f : X \to H$.
The function f is G-perfect nonlinear if $\forall g \in G^*$, $D_g f : x \mapsto f(g.x) - f(x)$ is balanced.

Objective

Find the dual characterization of such G-perfect nonlinear functions.

Dual characterisation of G-perfect nonlinearity (cont'd)

Dual characterization

A function $f : X \to H$ is G-perfect nonlinear if and only if $\forall \beta \in H^*$ and $\forall \rho \in \widehat{G}$,

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

As in the abelian case, this is also a notion of bentness in average but this time we use the dual characterization of left perfect nonlinear functions rather than the classical one.

Dual characterisation of G-perfect nonlinearity (cont'd)

Dual characterization

A function $f : X \to H$ is G-perfect nonlinear if and only if $\forall \beta \in H^*$ and $\forall \rho \in \widehat{G}$,

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

As in the abelian case, this is also a notion of bentness in average but this time we use the dual characterization of left perfect nonlinear functions rather than the classical one.

Outline

Definition and Combinatorial characterization

Definition

Let G be a finite group (not necessarily abelian) that (left) acts (at least) faithfully on a finite nonempty set X. Let $D \subset X$.

D is a G-(v, k, λ)-difference set of X if

- $v = |X|$;
- $k = |D|$;
- For each $g \in G^*$, the equation $x = g.y$ has λ solutions (x, y) in D^2.

Definition and Combinatorial characterization

Definition

Let G be a finite group (not necessarily abelian) that (left) acts (at least) faithfully on a finite nonempty set X. Let $D \subset X$.

D is a G-(v, k, λ)-difference set of X if

- $v = |X|$;
- $k = |D|$;
- For each $g \in G^*$, the equation $x = g.y$ has λ solutions (x, y) in D^2.

Definition and Combinatorial characterization

Definition

Let G be a finite group (not necessarily abelian) that (left) acts (at least) faithfully on a finite nonempty set X. Let $D \subset X$.

D is a G-(v, k, λ)-difference set of X if

- $v = |X|$;
- $k = |D|$;
- For each $g \in G^*$, the equation $x = g.y$ has λ solutions (x, y) in D^2.

Definition and Combinatorial characterization

Definition

Let G be a finite group (not necessarily abelian) that (left) acts (at least) faithfully on a finite nonempty set X. Let $D \subset X$.

D is a G-(v, k, λ)-difference set of X if

- $v = |X|$;
- $k = |D|$;
- For each $g \in G^*$, the equation $x = g.y$ has λ solutions (x, y) in D^2.

Definition and Combinatorial characterization (cont'd)

Proposition

Let G be a finite group (not necessarily abelian) that (left) acts (at least) faithfully on a finite nonempty set X. We also suppose that $|X| \equiv 0 \pmod 4$. Let $f : X \to \mathbb{Z}_2$.
The function f is G-perfect nonlinear if and only if its support S_f is a G-(v, k, λ)-difference set of X such that

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

Outline

Odd dimension

Theorem

Let m and n be two odd integers. Then it is possible to construct a function $f : \mathbb{Z}_{2m+n} \to \{0, 1\}$ which is $\mathbb{Z}_n$-bent.

Remark

Because m and n are odd integers there is no classical bent function from $\mathbb{Z}_{2m+n}$ to $\{0, 1\}$ or also from $\mathbb{Z}_n$ to $\{0, 1\}$.

Odd dimension

Theorem

Let m and n be two odd integers. Then it is possible to construct a function $f : \mathbb{Z}_{2m+n} \to \{0,1\}$ which is $\mathbb{Z}_n$-bent.

Remark

Because m and n are odd integers there is no classical bent function from $\mathbb{Z}_{2m+n}$ to $\{0,1\}$ or also from $\mathbb{Z}_n$ to $\{0,1\}$.

Odd dimension

Theorem

Let m and n be two odd integers. Then it is possible to construct a function $f : \mathbb{Z}_{2m+n} \to \{0, 1\}$ which is $\mathbb{Z}_n$-bent.

Remark

Because m and n are odd integers there is no classical bent function from $\mathbb{Z}_{2m+n}$ to $\{0, 1\}$ or also from $\mathbb{Z}_n$ to $\{0, 1\}$.

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-perfect nonlinear.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

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

□

Plane dimension

Theorem

Let $f : GF(2^m) \rightarrow GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-perfect nonlinear.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

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

$\square$

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-perfect nonlinear.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

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

□

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-perfect nonlinear.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

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

□

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-perfect nonlinear.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

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

□

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-perfect nonlinear.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

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

□

MERCI !

Allez les Bleus !

MERCI !

Allez les Bleus !