Differentially 4-Uniform Permutations with the Best Known Nonlinearity from Butterflies

Shihui Fu, Xiutao Feng and Baofeng Wu

Key Laboratory of Mathematics Mechanization,
Academy of Mathematics and Systems Science, Chinese Academy of Sciences

March 7, 2018

S-boxes

Many block ciphers use S-boxes to serve as the confusion components. The S-boxes are usually needed to satisfy the following conditions:

S-boxes

Many block ciphers use S-boxes to serve as the confusion components. The S-boxes are usually needed to satisfy the following conditions:

- Defined over the finite field $\mathbb{F}_{2^{2k}}$ (for the easiness of implementation);

S-boxes

Many block ciphers use S-boxes to serve as the confusion components. The S-boxes are usually needed to satisfy the following conditions:

- Defined over the finite field $\mathbb{F}_{2^{2k}}$ (for the easiness of implementation);
- Permutation (to obtain the correctness of decryption);

S-boxes

Many block ciphers use S-boxes to serve as the confusion components. The S-boxes are usually needed to satisfy the following conditions:

- Defined over the finite field $\mathbb{F}_{2^{2k}}$ (for the easiness of implementation);
- Permutation (to obtain the correctness of decryption);
- Low differential uniformity (to resist differential attacks);

S-boxes

Many block ciphers use S-boxes to serve as the confusion components. The S-boxes are usually needed to satisfy the following conditions:

- Defined over the finite field $\mathbb{F}_{2^{2k}}$ (for the easiness of implementation);
- Permutation (to obtain the correctness of decryption);
- Low differential uniformity (to resist differential attacks);
- High nonlinearity (to resist linear attacks);

S-boxes

Many block ciphers use S-boxes to serve as the confusion components. The S-boxes are usually needed to satisfy the following conditions:

- Defined over the finite field $\mathbb{F}_{2^{2k}}$ (for the easiness of implementation);
- Permutation (to obtain the correctness of decryption);
- Low differential uniformity (to resist differential attacks);
- High nonlinearity (to resist linear attacks);
- Not too low algebraic degree (to resist higher order differential attacks or algebraic attacks).

An Example

A well-known example:

AES uses the inverse function, namely, x^{-1} over $\mathbb{F}_{2^8}$ as its S-box for that it has very good cryptographic properties:

An Example

A well-known example:

AES uses the inverse function, namely, x^{-1} over $\mathbb{F}_{2^8}$ as its S-box for that it has very good cryptographic properties:

- its differential uniformity is 4;

An Example

A well-known example:

AES uses the inverse function, namely, x^{-1} over $\mathbb{F}_{2^8}$ as its S-box for that it has very good cryptographic properties:

- its differential uniformity is 4;
- its nonlinearity is optimal (i.e., 112);

An Example

A well-known example:

AES uses the inverse function, namely, x^{-1} over $\mathbb{F}_{2^8}$ as its S-box for that it has very good cryptographic properties:

- its differential uniformity is 4;
- its nonlinearity is optimal (i.e., 112);
- its algebraic degree is optimal as well (i.e., 7).

Vectorial Boolean Functions

Definition (Vectorial Boolean Functions)

Let n and m be two positive integers, The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n, m)-functions or vectorial Boolean functions. Specially, when $m = 1$, we call these $(n, 1)$-functions Boolean functions.

Vectorial Boolean Functions

Definition (Vectorial Boolean Functions)

Let n and m be two positive integers, The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n,m)-functions or vectorial Boolean functions. Specially, when $m=1$, we call these $(n,1)$-functions Boolean functions.

- An (n,m)-function has the following coordinate form:

$$\begin{aligned}&F(x_1,x_2,\cdots,x_n)\\=&(f_1(x_1,x_2,\cdots,x_n),f_2(x_1,x_2,\cdots,x_n),\cdots,f_m(x_1,x_2,\cdots,x_n)),\end{aligned}$$

where each coordinate $f_i(x_1,x_2,\cdots,x_n), 1\le i\le m$ is a Boolean function.

Algebraic Normal Form

Algebraic Normal Form (ANF)

An (n,m)-function F can be uniquely represented as an element of $\mathbb{F}_2^m[x_1,x_2,\cdots,x_n]/\langle x_1^2+x_1,x_2^2+x_2,\cdots,x_n^2+x_n\rangle$:

$$F(x)=\sum_{I\in\mathcal{P}(N)} a_I\left(\prod_{i\in I} x_i\right)=\sum_{I\in\mathcal{P}(N)} a_I x^I,$$

where $\mathcal{P}(N)$ denotes the power set of $N=\{1,2,\cdots,n\}$, and $a_I\in\mathbb{F}_2^m$.

Algebraic Normal Form

Algebraic Normal Form (ANF)

An (n, m)-function F can be uniquely represented as an element of $\mathbb{F}_2^m[x_1, x_2, \cdots, x_n]/\langle x_1^2 + x_1, x_2^2 + x_2, \cdots, x_n^2 + x_n\rangle$:

$$F(x) = \sum_{I \in \mathcal{P}(N)} a_I \left(\prod_{i \in I} x_i\right) = \sum_{I \in \mathcal{P}(N)} a_I x^I,$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, 2, \cdots, n\}$, and $a_I \in \mathbb{F}_2^m$.

The algebraic degree of the function is by definition the global degree of its ANF:

$$\deg(F) = \max\{|I| : a_I \neq (0, 0, \cdots, 0); I \in \mathcal{P}(N)\}$$

Univariate Polynomial Representation

A second representation of (n,m)-functions when $m=n$

Any (n,n)-function F admits a unique univariate polynomial representation over $\mathbb{F}_{2^n}[x]/\langle x^{2^n}+x\rangle$, of degree at most 2^n-1:

$$F(x)=\sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

Univariate Polynomial Representation

A second representation of (n, m)-functions when $m = n$

Any (n, n)-function F admits a unique univariate polynomial representation over $\mathbb{F}_{2^n}[x]/\langle x^{2^n} + x\rangle$, of degree at most $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

- The algebraic degree of F is equal to the maximum *2-weight* $w_2(i)$ of i such that $c_i \neq 0$, where $w_2(l)$ is the number of nonzero coefficients $l_j \in \mathbb{F}_2$ in the binary expansion $l = \sum_{j=0}^{n-1} l_j 2^j$.

Differential Uniformity

Definition (Differential Uniformity)

For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the differential uniformity of $F(x)$ is denoted as

$$\Delta_F = \max\{\delta_F(a, b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\},$$

where $\delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}|$.

Differential Uniformity

Definition (Differential Uniformity)

For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the differential uniformity of $F(x)$ is denoted as

$$\Delta_F = \max\{\delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\},$$

where $\delta_F(a,b) = |\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}|$.

- The *differential spectrum* of $F(x)$ is the multiset

$$\{* \ \delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n} \ *\}.$$

Differential Uniformity

Obviously, if x_0 is a solution of $F(x+a)+F(x)=b$, so is x_0+a. Thus the differential uniformity must be even. The smallest possible value is 2. These functions which achieve this bound are called *almost perfect nonlinear (APN)* functions.

Examples

- Gold function x^{2^i+1}, $1 \le i \le \frac{n-1}{2}$, $\gcd(i,n)=1$ (Gold 1968);
- Kasami function $x^{2^{2i}-2^i+1}$, $1 \le i \le \frac{n-1}{2}$, $\gcd(i,n)=1$ (Kasami 1971);
- Welch function x^{2^t+3}, $n=2t+1$ (Niho 1972);
- ...

Since APN functions have the lowest differential uniformity, they are the most ideal choices for S-box.

Since APN functions have the lowest differential uniformity, they are the most ideal choices for S-box.

However, all the known APN functions are not permutations when the extension degree is even except for one sporadic example over $\mathbb{F}_{2^6}$ found by Dillon. (the BIG APN problem)

Since APN functions have the lowest differential uniformity, they are the most ideal choices for S-box.

However, all the known APN functions are not permutations when the extension degree is even except for one sporadic example over $\mathbb{F}_{2^6}$ found by Dillon. (the BIG APN problem)

A natural tradeoff method is to use differentially 4-uniform permutations as S-boxes. It is interesting to construct more differentially 4-uniform permutations with high nonlinearity and algebraic degree.

Nonlinearity

Walsh transform

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we define the *Walsh transform* of F as

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bF(x)+ax)}, \quad a, b \in \mathbb{F}_{2^n},$$

where $\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{n-1}}$ is the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

Nonlinearity

Walsh transform

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we define the *Walsh transform* of F as

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bF(x)+ax)}, \quad a, b \in \mathbb{F}_{2^n},$$

where $\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{n-1}}$ is the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

The multiset $\Lambda_F = \{* \ \mathcal{W}_F(a,b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^* \ *\}$ is called the *Walsh spectrum* of the function F.

Nonlinearity

Definition (Nonlinearity)

The *nonlinearity* of F is defined as

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*} |\mathcal{W}_F(a,b)|.$$

Nonlinearity

Definition (Nonlinearity)

The *nonlinearity* of F is defined as

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*} |\mathcal{W}_F(a,b)|.$$

- If n is odd the nonlinearity of F satisfies the inequality $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$, and in case of equality F is called *almost bent* function.

Nonlinearity

Definition (Nonlinearity)

The *nonlinearity* of F is defined as

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*} |\mathcal{W}_F(a,b)|.$$

- If n is odd the nonlinearity of F satisfies the inequality $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$, and in case of equality F is called *almost bent* function.
- While n is even, the known maximum nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$. It is conjectured that $\mathcal{NL}(F)$ is upper bounded by $2^{n-1} - 2^{\frac{n}{2}}$. These functions which meet this bound are usually called *optimal (maximal) nonlinear* functions.

Butterfly Structures

Definition (Butterfly Structures)

Let k be a positive integer and $\alpha \in \mathbb{F}_{2^k}$, e be an integer such that the mapping $x \mapsto x^e$ is a permutation over $\mathbb{F}_{2^k}$ and $R_z[e,\alpha](x) = (x+\alpha z)^e + z^e$ be a keyed permutation. The Butterfly Structures are defined as follows:

Butterfly Structures

Definition (Butterfly Structures)

Let k be a positive integer and $\alpha \in \mathbb{F}_{2^k}$, e be an integer such that the mapping $x \mapsto x^e$ is a permutation over $\mathbb{F}_{2^k}$ and $R_z[e,\alpha](x) = (x+\alpha z)^e + z^e$ be a keyed permutation. The Butterfly Structures are defined as follows:

- the *Open Butterfly Structure* with branch size k, exponent e and coefficient α is the function denoted H_e^α defined by:

$$\mathrm{H}_e^\alpha(x,y) = \left(R_{R_y^{-1}[e,\alpha](x)}[e,\alpha](y), R_y^{-1}[e,\alpha](x)\right),$$

Butterfly Structures

Definition (Butterfly Structures)

Let k be a positive integer and $\alpha \in \mathbb{F}_{2^k}$, e be an integer such that the mapping $x \mapsto x^e$ is a permutation over $\mathbb{F}_{2^k}$ and $R_z[e,\alpha](x) = (x+\alpha z)^e + z^e$ be a keyed permutation. The Butterfly Structures are defined as follows:

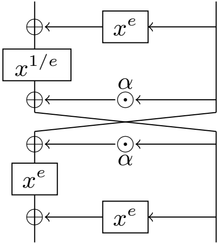
- the *Open Butterfly Structure* with branch size k, exponent e and coefficient α is the function denoted H_e^α defined by:

$$\mathsf{H}_e^\alpha(x,y) = \left(R_{R_y^{-1}[e,\alpha](x)}[e,\alpha](y), R_y^{-1}[e,\alpha](x)\right),$$

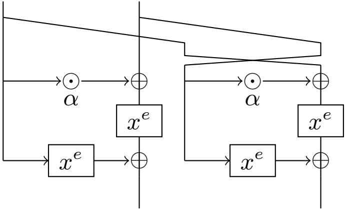
- the *Closed Butterfly Structure* with branch size k, exponent e and coefficient α is the function denoted V_e^α defined by:

$$\mathsf{V}_e^\alpha(x,y) = (R_x[e,\alpha](y), R_y[e,\alpha](x)).$$

Butterfly Structures



(a) Open butterfly H_e^α (bijective).



(b) Closed butterfly V_e^α.

The Algebraic Forms of Butterfly Structures

- Open Butterfly Structure

$$\begin{aligned}&\mathsf{H}_e^{\alpha}(x,y)\\ &=\left(\left(y+\alpha(x+y^e)^{\frac{1}{e}}+\alpha^2 y\right)^e+\left((x+y^e)^{\frac{1}{e}}+\alpha y\right)^e,(x+y^e)^{\frac{1}{e}}+\alpha y\right)\end{aligned}$$

- Closed Butterfly Structure

$$\mathsf{V}_e^{\alpha}(x,y)=((\alpha x+y)^e+x^e,(x+\alpha y)^e+y^e)$$

Generalised Butterfly Structures

Definition (Generalised Butterflies)

Let R be a bivariate polynomials of $\mathbb{F}_{2^k}$ such that $R_y : x \mapsto R(x, y)$ is a permutation of $\mathbb{F}_{2^k}$ for all y in $\mathbb{F}_{2^k}$. The Generalised Butterfly Structures are defined as follows:

Generalised Butterfly Structures

Definition (Generalised Butterflies)

Let R be a bivariate polynomials of $\mathbb{F}_{2^k}$ such that $R_y : x \mapsto R(x,y)$ is a permutation of $\mathbb{F}_{2^k}$ for all y in $\mathbb{F}_{2^k}$. The Generalised Butterfly Structures are defined as follows:

- the *Open Generalised Butterfly Structure* with branch size k is the function denoted H_R defined by:

$$\mathrm{H}_R(x,y) = \left(R_{R_y^{-1}(x)}(y), R_y^{-1}(x)\right),$$

Generalised Butterfly Structures

Definition (Generalised Butterflies)

Let R be a bivariate polynomials of $\mathbb{F}_{2^k}$ such that $R_y : x \mapsto R(x, y)$ is a permutation of $\mathbb{F}_{2^k}$ for all y in $\mathbb{F}_{2^k}$. The Generalised Butterfly Structures are defined as follows:

- the *Open Generalised Butterfly Structure* with branch size k is the function denoted H_R defined by:

$$\mathrm{H}_R(x, y) = \left(R_{R_y^{-1}(x)}(y), R_y^{-1}(x)\right),$$

- the *Closed Generalised Butterfly Structure* with branch size k is the function denoted V_R defined by:

$$\mathrm{V}_R(x, y) = (R(x, y), R(y, x)).$$

Generalised Butterfly Structures

(a) Open Generalised Butterfly H_R.

(b) Closed Generalised Butterfly V_R.

Figure: The Generalised Butterfly Structures.

Equivalence Relations

- Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *extended affine equivalent (EA-equivalent)*, if $G(x) = A_1(F(A_2(x))) + A_3(x)$, where $A_1(x)$, $A_2(x)$ are affine permutations over $\mathbb{F}_{2^n}$ and $A_3(x)$ is an affine function over $\mathbb{F}_{2^n}$.

Equivalence Relations

- Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *extended affine equivalent (EA-equivalent)*, if $G(x) = A_1(F(A_2(x))) + A_3(x)$, where $A_1(x)$, $A_2(x)$ are affine permutations over $\mathbb{F}_{2^n}$ and $A_3(x)$ is an affine function over $\mathbb{F}_{2^n}$.

- They are called *CCZ-equivalent (Carlet-Charpin-Zinoviev equivalent)* if there exists an affine permutation over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ which maps $\mathcal{G}_F$ to $\mathcal{G}_G$, where $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ is the graph of F, and $\mathcal{G}_G$ is the graph of G.

Equivalence Relations

- Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *extended affine equivalent (EA-equivalent)*, if $G(x) = A_1(F(A_2(x))) + A_3(x)$, where $A_1(x)$, $A_2(x)$ are affine permutations over $\mathbb{F}_{2^n}$ and $A_3(x)$ is an affine function over $\mathbb{F}_{2^n}$.

- They are called *CCZ-equivalent (Carlet-Charpin-Zinoviev equivalent)* if there exists an affine permutation over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ which maps $\mathcal{G}_F$ to $\mathcal{G}_G$, where $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ is the graph of F, and $\mathcal{G}_G$ is the graph of G.

- H_e^{α} (H_R) and V_e^{α} (V_R) are CCZ-equivalent.

The Motivation of This Research

Theorem (Perrin et al. CRYPTO'16)

Let V_e^α *and* H_e^α *respectively be the closed and open* $2k$*-bit butterflies with exponent* $e = 3 \times 2^t$ *for some* t*, coefficient* α *not in* $\{0, 1\}$ *and* k *odd. Then:*

1. V_e^α *is quadratic, and half of the coordinates of* H_e^α *have algebraic degree* k*, the other half have algebraic degree* $k + 1$*;*
2. *The differential uniformity of both* H_e^α *and* V_e^α *are at most equal to 4.*

The Motivation of This Research

Theorem (Perrin et al. CRYPTO'16)

Let V_e^α and H_e^α respectively be the closed and open $2k$-bit butterflies with exponent $e = 3 \times 2^t$ for some t, coefficient α not in $\{0, 1\}$ and k odd. Then:

1. *V_e^α is quadratic, and half of the coordinates of H_e^α have algebraic degree k, the other half have algebraic degree $k+1$;*
2. *The differential uniformity of both H_e^α and V_e^α are at most equal to 4.*

A Conjecture

The nonlinearity of butterfly structures of H_e^α and V_e^α operating on $2k$ bits are equal to $2^{2k-1} - 2^k$ for every odd k, $e = 3 \times 2^t$ and $\alpha \neq 0, 1$.

Cryptographic Properties of Generalised Butterflies

Theorem (Canteaut-Duval-Perrin, 2017, TIT)

The cryptographic properties of the generalised butterflies $\mathsf{V}_{\alpha,\beta}$ *and* $\mathsf{H}_{\alpha,\beta}$ *which are based on functions* $R : (x, y) \mapsto (x + \alpha y)^3 + \beta y^3$ *with* $\alpha, \beta \neq 0$ *are as follows:*

Cryptographic Properties of Generalised Butterflies

Theorem (Canteaut-Duval-Perrin, 2017, TIT)

The cryptographic properties of the generalised butterflies $\mathsf{V}_{\alpha,\beta}$ *and* $\mathsf{H}_{\alpha,\beta}$ *which are based on functions* $R : (x, y) \mapsto (x + \alpha y)^3 + \beta y^3$ *with* $\alpha, \beta \neq 0$ *are as follows:*

1. *the algebraic degree of* $\mathsf{V}_{\alpha,\beta}$ *is always equal to 2;*

Cryptographic Properties of Generalised Butterflies

Theorem (Canteaut-Duval-Perrin, 2017, TIT)

The cryptographic properties of the generalised butterflies $\mathsf{V}_{\alpha,\beta}$ *and* $\mathsf{H}_{\alpha,\beta}$ *which are based on functions* $R : (x, y) \mapsto (x + \alpha y)^3 + \beta y^3$ *with* $\alpha, \beta \neq 0$ *are as follows:*

1. *the algebraic degree of* $\mathsf{V}_{\alpha,\beta}$ *is always equal to 2;*
2. *if* $k = 3$*,* $\alpha \neq 0$*,* $\mathrm{Tr}(\alpha) = 0$ *and* $\beta \in \{\alpha^3 + \alpha, \alpha^3 + 1/\alpha\}$ *then the butterflies are APN, have a nonlinearity equal to* $2^{2k-1} - 2^k$ *and the algebraic degree of* $\mathsf{H}_{\alpha,\beta}$ *is equal to* $k + 1$*;*

Theorem (Canteaut-Duval-Perrin, 2017, TIT)

The cryptographic properties of the generalised butterflies $\mathsf{V}_{\alpha,\beta}$ *and* $\mathsf{H}_{\alpha,\beta}$ *which are based on functions* $R : (x, y) \mapsto (x + \alpha y)^3 + \beta y^3$ *with* $\alpha, \beta \neq 0$ *are as follows:*

1. *the algebraic degree of* $\mathsf{V}_{\alpha,\beta}$ *is always equal to 2;*
2. *if* $k = 3$*,* $\alpha \neq 0$*,* $\mathrm{Tr}(\alpha) = 0$ *and* $\beta \in \{\alpha^3 + \alpha, \alpha^3 + 1/\alpha\}$ *then the butterflies are APN, have a nonlinearity equal to* $2^{2k-1} - 2^k$ *and the algebraic degree of* $\mathsf{H}_{\alpha,\beta}$ *is equal to* $k + 1$*;*
3. *if* $\beta = (1 + \alpha)^3$ *then the differential uniformity is equal to* 2^{k+1}*, the nonlinearity is equal to* $2^{2k-1} - 2^{\frac{3k-1}{2}}$ *and the algebraic degree of* $\mathsf{H}_{\alpha,\beta}$ *is equal to* k*;*

Cryptographic Properties of Generalised Butterflies

Theorem (Canteaut-Duval-Perrin, 2017, TIT)

The cryptographic properties of the generalised butterflies $\mathsf{V}_{\alpha,\beta}$ *and* $\mathsf{H}_{\alpha,\beta}$ *which are based on functions* $R : (x, y) \mapsto (x + \alpha y)^3 + \beta y^3$ *with* $\alpha, \beta \neq 0$ *are as follows:*

1. *the algebraic degree of* $\mathsf{V}_{\alpha,\beta}$ *is always equal to 2;*
2. *if* $k = 3$, $\alpha \neq 0$, $\mathrm{Tr}(\alpha) = 0$ *and* $\beta \in \{\alpha^3 + \alpha, \alpha^3 + 1/\alpha\}$ *then the butterflies are APN, have a nonlinearity equal to* $2^{2k-1} - 2^k$ *and the algebraic degree of* $\mathsf{H}_{\alpha,\beta}$ *is equal to* $k + 1$*;*
3. *if* $\beta = (1 + \alpha)^3$ *then the differential uniformity is equal to* 2^{k+1}*, the nonlinearity is equal to* $2^{2k-1} - 2^{\frac{3k-1}{2}}$ *and the algebraic degree of* $\mathsf{H}_{\alpha,\beta}$ *is equal to* k*;*
4. *otherwise, the differential uniformity is equal to 4, the nonlinearity is equal to* $2^{2k-1} - 2^k$ *and algebraic degree of* $\mathsf{H}_{\alpha,\beta}$ *is either* k *or* $k + 1$*. It is equal to* k *if and only if* $1 + \alpha\beta + \alpha^4 = (\beta + \alpha + \alpha^3)^2$*.*

Main Results

Main Results

- The differential uniformity of both H_e^α and V_e^α are at most equal to 4, where $e = (2^i + 1) \times 2^t$, coefficient $\alpha \neq 0, 1$, k odd and $\gcd(i, k) = 1$;

Main Results

- The differential uniformity of both H_e^α and V_e^α are at most equal to 4, where $e = (2^i + 1) \times 2^t$, coefficient $\alpha \neq 0, 1$, k odd and $\gcd(i, k) = 1$;
- We prove that the nonlinearity equality are true for every odd k, $e = (2^i + 1) \times 2^t$ and $\alpha \neq 0$, which gives independently a solution to the conjecture by the way;

Main Results

- The differential uniformity of both H_e^α and V_e^α are at most equal to 4, where $e = (2^i + 1) \times 2^t$, coefficient $\alpha \neq 0, 1$, k odd and $\gcd(i, k) = 1$;
- We prove that the nonlinearity equality are true for every odd k, $e = (2^i + 1) \times 2^t$ and $\alpha \neq 0$, which gives independently a solution to the conjecture by the way;
- We show that V_e^1 for $e = (2^i + 1) \times 2^t$ are permutations over $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Main Results

Theorem (Nontrivial Case)

For any $0 \le t \le k-1$, $0 \le i \le k-1$, $\gcd(k,i)=1$, $\alpha \in \mathbb{F}_{2^k}$, *and* $\alpha \neq 0,1$, *let* H_e^α *and* V_e^α *be the open and closed* $2k$*-bit butterfly structures with exponent* $e=(2^i+1)\times 2^t$ *and coefficient* α. *Then*

Main Results

Theorem (Nontrivial Case)

For any $0 \le t \le k-1$, $0 \le i \le k-1$, $\gcd(k,i)=1$, $\alpha \in \mathbb{F}_{2^k}$, *and* $\alpha \neq 0, 1$, *let* H_e^α *and* V_e^α *be the open and closed* $2k$*-bit butterfly structures with exponent* $e = (2^i+1) \times 2^t$ *and coefficient* α*. Then*

1. V_e^α *has algebraic degree 2. The open butterfly* H_e^α *has algebraic degree* $k+1$*;*

Main Results

Theorem (Nontrivial Case)

For any $0 \le t \le k-1$, $0 \le i \le k-1$, $\gcd(k,i)=1$, $\alpha \in \mathbb{F}_{2^k}$, and $\alpha \ne 0, 1$, let H_e^α and V_e^α be the open and closed $2k$-bit butterfly structures with exponent $e = (2^i+1) \times 2^t$ and coefficient α. Then

1. *V_e^α has algebraic degree 2. The open butterfly H_e^α has algebraic degree $k+1$;*
2. *The differential uniformity of both H_e^α and V_e^α are at most equal to 4;*

Main Results

Theorem (Nontrivial Case)

For any $0 \le t \le k-1$, $0 \le i \le k-1$, $\gcd(k,i)=1$, $\alpha \in \mathbb{F}_{2^k}$, *and* $\alpha \neq 0, 1$, *let* H_e^α *and* V_e^α *be the open and closed* $2k$*-bit butterfly structures with exponent* $e = (2^i+1)\times 2^t$ *and coefficient* α. *Then*

1. V_e^α *has algebraic degree 2. The open butterfly* H_e^α *has algebraic degree* $k+1$;
2. *The differential uniformity of both* H_e^α *and* V_e^α *are at most equal to 4;*
3. *The nonlinearity of both* H_e^α *and* V_e^α *are equal to* $2^{2k-1}-2^k$, *namely, optimal, and their extended Walsh spectrum are* $\{0, 2^k, 2^{k+1}\}$.

Main Results

Theorem (Trivial Cases)

For any $0 \le t \le k-1$ *and* $0 \le i \le k-1$, $\gcd(i,k) = 1$, *let* H_e^1 *and* V_e^1 *be the open and closed* $2k$*-bit butterfly structures with exponent* $e = (2^i + 1) \times 2^t$ *and coefficient* $\alpha = 1$. *then*

Theorem (Trivial Cases)

For any $0 \leq t \leq k-1$ and $0 \leq i \leq k-1$, $\gcd(i,k) = 1$, let H_e^1 and V_e^1 be the open and closed $2k$-bit butterfly structures with exponent $e = (2^i + 1) \times 2^t$ and coefficient $\alpha = 1$. then

1. *Both H_e^1 and V_e^1 are permutations over $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$;*

Theorem (Trivial Cases)

For any $0 \le t \le k-1$ *and* $0 \le i \le k-1$, $\gcd(i,k)=1$, *let* H_e^1 *and* V_e^1 *be the open and closed* $2k$*-bit butterfly structures with exponent* $e=(2^i+1)\times 2^t$ *and coefficient* $\alpha=1$*. then*

1. *Both* H_e^1 *and* V_e^1 *are permutations over* $\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$*;*
2. *The algebraic degree of* H_e^1 *and* V_e^1 *are equal to* k *and 2 respectively;*

Main Results

Theorem (Trivial Cases)

For any $0 \leq t \leq k-1$ *and* $0 \leq i \leq k-1$, $\gcd(i,k)=1$, *let* H_e^1 *and* V_e^1 *be the open and closed* $2k$*-bit butterfly structures with exponent* $e=(2^i+1)\times 2^t$ *and coefficient* $\alpha=1$*. then*

1. *Both* H_e^1 *and* V_e^1 *are permutations over* $\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$*;*
2. *The algebraic degree of* H_e^1 *and* V_e^1 *are equal to* k *and 2 respectively;*
3. *The differential uniformity of both* H_e^1 *and* V_e^1 *are equal to 4 and their differential spectrums are* $\{0,4\}$*;*

Main Results

Theorem (Trivial Cases)

For any $0 \leq t \leq k-1$ *and* $0 \leq i \leq k-1$, $\gcd(i,k)=1$, *let* H_e^1 *and* V_e^1 *be the open and closed* $2k$*-bit butterfly structures with exponent* $e=(2^i+1)\times 2^t$ *and coefficient* $\alpha=1$. *then*

1. *Both* H_e^1 *and* V_e^1 *are permutations over* $\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$;
2. *The algebraic degree of* H_e^1 *and* V_e^1 *are equal to* k *and 2 respectively;*
3. *The differential uniformity of both* H_e^1 *and* V_e^1 *are equal to 4 and their differential spectrums are* $\{0,4\}$;
4. *The nonlinearity of both* H_e^1 *and* V_e^1 *are equal to* $2^{2k-1}-2^k$, *namely, optimal, and their Walsh spectrums are* $\{0,\pm 2^{k+1}\}$.

Two Key Lemmas

Two Key Lemmas

Two Key Lemmas

Two Key Lemmas

- Suppose k and i are two integers such that $\gcd(i,k)=1$. For any $c_1,c_2,c_3\in\mathbb{F}_{2^k}$ with not all zero, then the following equation

$$c_1x^{2^{2i}}+c_2x^{2^i}+c_3x=0$$

has at most 4 solutions in $\mathbb{F}_{2^k}$.

Two Key Lemmas

Two Key Lemmas

- Suppose k and i are two integers such that $\gcd(i,k)=1$. For any $c_1, c_2, c_3 \in \mathbb{F}_{2^k}$ with not all zero, then the following equation

$$c_1 x^{2^{2i}} + c_2 x^{2^i} + c_3 x = 0$$

  has at most 4 solutions in $\mathbb{F}_{2^k}$.

- Suppose k is an odd integer and $\gcd(i,k)=1$. For any $c_1, c_2, c_3 \in \mathbb{F}_{2^k}$ with not all zero, then the following equation

$$c_1 x^{2^{4i}} + c_2 x^{2^{2i}} + c_3 x = 0$$

  has at most 4 solutions in $\mathbb{F}_{2^k}$.

The Proof of Differential Uniformity

Let $u, v, a, b \in \mathbb{F}_{2^k}$ and $(u, v) \neq (0, 0)$. Then we need to prove that

$$\mathsf{V}_e^{\alpha}(x, y) + \mathsf{V}_e^{\alpha}(x + u, y + v) = (a, b),$$

has at most 4 solutions in $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$,

The Proof of Differential Uniformity

Let $u, v, a, b \in \mathbb{F}_{2^k}$ and $(u, v) \neq (0, 0)$. Then we need to prove that

$$\mathsf{V}_e^{\alpha}(x, y) + \mathsf{V}_e^{\alpha}(x + u, y + v) = (a, b),$$

has at most 4 solutions in $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, which is equivalent to the following linear homogeneous system of equations

$$\begin{cases} \left(\alpha^{2^i}(\alpha u + v) + u\right) x^{2^i} + \left(\alpha(\alpha u + v)^{2^i} + u^{2^i}\right) x \\ \qquad\qquad + (\alpha u + v) y^{2^i} + (\alpha u + v)^{2^i} y = 0, \\ (\alpha v + u) x^{2^i} + (\alpha v + u)^{2^i} x + \left(\alpha^{2^i}(\alpha v + u) + v\right) y^{2^i} \\ \qquad\qquad + \left(\alpha(\alpha v + u)^{2^i} + v^{2^i}\right) y = 0 \end{cases}$$

has at most 4 solutions in $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

The Proof of Nonlinearity

Let $a, b, c, d \in \mathbb{F}_{2^k}$, and $(c, d) \neq (0, 0)$. Then we have

$$\mathcal{W}_F^2((a,b),(c,d)) = \sum_{x,y \in \mathbb{F}_{2^k}} (-1)^{F(x,y)} \cdot \sum_{u,v \in \mathbb{F}_{2^k}} (-1)^{F(x+u,y+v)}$$

The Proof of Nonlinearity

Let $a, b, c, d \in \mathbb{F}_{2^k}$, and $(c, d) \neq (0, 0)$. Then we have

$$\begin{aligned}\mathcal{W}_F^2((a,b),(c,d)) &= \sum_{x,y\in\mathbb{F}_{2^k}} (-1)^{F(x,y)} \cdot \sum_{u,v\in\mathbb{F}_{2^k}} (-1)^{F(x+u,y+v)} \\ &= \sum_{x,y,u,v\in\mathbb{F}_{2^k}} (-1)^{F(x,y)+F(x+u,y+v)}\end{aligned}$$

The Proof of Nonlinearity

The Proof of Nonlinearity

Let $a, b, c, d \in \mathbb{F}_{2^k}$, and $(c, d) \neq (0, 0)$. Then we have

$$\begin{aligned}
\mathcal{W}_F^2((a,b),(c,d)) &= \sum_{x,y \in \mathbb{F}_{2^k}} (-1)^{F(x,y)} \cdot \sum_{u,v \in \mathbb{F}_{2^k}} (-1)^{F(x+u,y+v)} \\
&= \sum_{x,y,u,v \in \mathbb{F}_{2^k}} (-1)^{F(x,y)+F(x+u,y+v)} \\
&= 2^{2k} \cdot \sum_{u,v \in R(c,d)} (-1)^{f(u,v)},
\end{aligned}$$

where

$$\begin{aligned}
f(x,y) = &\mathrm{Tr}\Big((\alpha^{2^i+1} c + c + d) x^{2^i+1} + (\alpha^{2^i+1} d + c + d) y^{2^i+1} \\
&+ (\alpha^{2^i} c + \alpha d) x^{2^i} y + (\alpha c + \alpha^{2^i} d) x y^{2^i} + ax + by \Big),
\end{aligned}$$

The Proof of Nonlinearity

and $R(c,d)$ is the solution set of the following system of equations with variables u, v

$$\begin{cases} \left(\alpha^{2^i+1}c+c+d\right)^{2^i} u^{2^{2i}} + \left(\alpha^{2^i+1}c+c+d\right) u \\ \qquad + \left(\alpha c+\alpha^{2^i}d\right)^{2^i} v^{2^{2i}} + \left(\alpha^{2^i}c+\alpha d\right) v = 0, \\ \left(\alpha^{2^i}c+\alpha d\right)^{2^i} u^{2^{2i}} + \left(\alpha c+\alpha^{2^i}d\right) u \\ \qquad + \left(\alpha^{2^i+1}d+c+d\right)^{2^i} v^{2^{2i}} + \left(\alpha^{2^i+1}d+c+d\right) v = 0. \end{cases}$$

The core part: $\dim_{\mathbb{F}_2} R(c,d) = 0$ or 2.

The bijective of closed butterfly structure

For any $u, v \in \mathbb{F}_{2^k}$, where $(u, v) \neq (0, 0)$, it is sufficient to show that

$$\mathsf{V}_e^1(x, y) + \mathsf{V}_e^1(x + u, y + v) = (0, 0),$$

has no solution in $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

The bijective of closed butterfly structure

For any $u, v \in \mathbb{F}_{2^k}$, where $(u, v) \neq (0, 0)$, it is sufficient to show that

$$\mathsf{V}_e^1(x, y) + \mathsf{V}_e^1(x+u, y+v) = (0, 0),$$

has no solution in $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.
This is to say that the following system of equations

$$\begin{cases} vx^{2^i} + v^{2^i}x + (u+v)y^{2^i} + (u+v)^{2^i}y = (u+v)^{2^i+1} + u^{2^i+1}, \\ (u+v)x^{2^i} + (u+v)^{2^i}x + uy^{2^i} + u^{2^i}y = (u+v)^{2^i+1} + v^{2^i+1} \end{cases}$$

has no solution in $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

The Nonlinearity

The proof procedure of the nonlinearity of trivial case is mainly based on the following lemma.

Lemma

Let i be an integer such that $0 \le i \le k-1$ and $\gcd(k,i) = 1$. Then for any $(c,d) \in \mathbb{F}_{2^k}^2$ with $(c,d) \neq (0,0)$, the following system of equations in variables u and v

$$\begin{cases} du^{2^i} + (du)^{2^{k-i}} + (c+d)v^{2^i} + ((c+d)v)^{2^{k-i}} = 0, \\ (c+d)u^{2^i} + ((c+d)u)^{2^{k-i}} + cv^{2^i} + (cv)^{2^{k-i}} = 0 \end{cases}$$

has exactly 4 solutions in $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Conclusion

Conclusion

- We further study the butterfly structures and show that they always have very good cryptographic properties;

Conclusion

- We further study the butterfly structures and show that they always have very good cryptographic properties;
- We prove that their nonlinearities are optimal in a general case;

Conclusion

- We further study the butterfly structures and show that they always have very good cryptographic properties;
- We prove that their nonlinearities are optimal in a general case;
- We prove that the closed butterfly structure with trivial coefficient is also a permutation.

Open Problems

Open Problems

- **The BIG APN problem**: Is there a tuple $k, R(x, y)$ where $k > 3$ is an integer, such that $\mathrm{H}_R(x, y)$ operating on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ is APN?

Open Problems

- **The BIG APN problem**: Is there a tuple $k, R(x, y)$ where $k > 3$ is an integer, such that $\mathrm{H}_R(x, y)$ operating on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ is APN?
- Find more k, e, α where e is an integer and $\alpha \in \mathbb{F}_{2^k}$, such that H_e^α operating on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ for even k is differential 4-uniform. (E.g., in the case $k = 6$ there does exist α such that H_5^α is differential 4-uniform)

Open Problems

- **The BIG APN problem**: Is there a tuple $k, R(x,y)$ where $k > 3$ is an integer, such that $\mathrm{H}_R(x,y)$ operating on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ is APN?
- Find more k, e, α where e is an integer and $\alpha \in \mathbb{F}_{2^k}$, such that H_e^α operating on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ for even k is differential 4-uniform. (E.g., in the case $k = 6$ there does exist α such that H_5^α is differential 4-uniform)
- Find more classes of differentially 4-uniform permutations with the optimal nonlinearity and high algebraic degree from **other functions over subfields or other structures**.

Thanks!