On the Generalization of Butterfly Structure

Yongqiang Li[a,b], Shizhu Tian[a,b], Yuyin Yu[c] and Mingsheng Wang[a,b]

a. State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences
b. School of Cyber Security, University of Chinese Academy of Sciences
c. School of Mathematics and Information Science, Guangzhou University

FSE 2018, Bruges, Belgium

March 7, 2018

On the Generalization of Butterfly Structure

Yongqiang Li[a,b], Shizhu Tian[a,b], Yuyin Yu[c] and Mingsheng Wang[a,b]

a. State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences
b. School of Cyber Security, University of Chinese Academy of Sciences
c. School of Mathematics and Information Science, Guangzhou University

FSE 2018, Bruges, Belgium

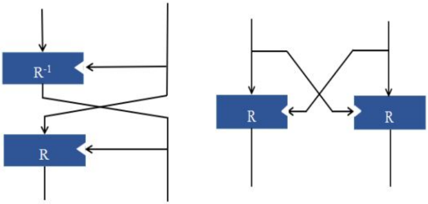
March 7, 2018

Outlines

1. Backgroud
2. Our generalization and main result
3. Proofs
4. Comparison
5. Future work

Butterfly Structure

A structure that serves infinite family of permutations over $\mathbb{F}_{2^{2n}}$.



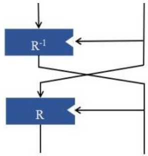
The open butterfly H_R The closed butterfly V_R

- $R_y : x \mapsto R(x, y)$ is a permutation over $\mathbb{F}_{2^n}$ for all y in $\mathbb{F}_{2^n}$;
- $\mathrm{H_R}$ is an involution;
- $\mathrm{H_R}$ and $\mathrm{V_R}$ are CCZ-equivalent;

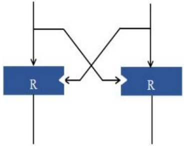
Origin

Crypto 2016, Perrin et.al. reverse-engineered the only known APN permutation over $\mathbb{F}_{2^6}$ and discover this structure.

$$R(x,y) = (x + \alpha y)^3 + y^3$$



The open butterfly H_R



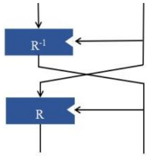
The closed butterfly V_R

- $\alpha \neq 0, 1$ and odd n:
  - Differential uniformity: at most 4;
  - Algebraic degree: $n+1$ or n for H_R and 2 for V_R;
  - Non-linearity: $2^{2n-1} - 2^n$?
- $\alpha = 1$ and odd n: $H_R \Leftrightarrow F^e$ (3-round Feistel) with
  - Differential spectrum: $\{0, 4\}$;
  - Non-linearity: $2^{2n-1} - 2^n$;
  - Algebraic degree: n for H_R and 2 for V_R;

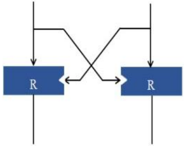
$n > 3$, more APN permutations from H_R?

Previous generalizations

TIT 2017, Anne Canteaut et. al.: $(x+\alpha y)^3 + y^3 \Rightarrow \ (x+\alpha y)^3 + \beta y^3$ with $\alpha, \beta \neq 0$.



The open butterfly H_R

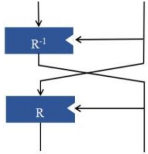


The closed butterfly V_R

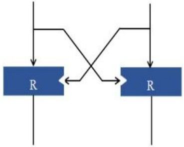
- $\beta = (1+\alpha)^3$ and odd n:
  - Differential uniformity: 2^{n+1};
  - Non-linearity: $2^{2n-1} - 2^{(3n-1)/2}$;
  - Algebraic degree: n for H_R and 2 for V_R;
- $n = 3, \mathrm{Tr}(\alpha) = 0$ and $\beta \in \{\alpha^3 + \alpha, \alpha^3 + 1/\alpha\}$:
  - Differential uniformity: 2;
  - Non-linearity: $2^{2n-1} - 2^n$;
  - Algebraic degree: $n+1$ for H_R and 2 for V_R;
- Otherwise for odd n:
  - Differential uniformity: 4;
  - Non-linearity: $2^{2n-1} - 2^n$;
  - Algebraic degree: $n+1$ or n for H_R with $1 + \alpha\beta + \alpha^4 = (\beta + \alpha + \alpha^3)^2$ and 2 for V_R;

Previous generalizations

FSE 2018, Shihui Fu et. al.: $(x+\alpha y)^3 + y^3 \Rightarrow (x+\alpha y)^{2^i+1} + y^{2^i+1}$ with $\gcd(i,n) = 1$



The open butterfly H_R



The closed butterfly V_R

- $\alpha \neq 0, 1$ and odd n:
  - Differential uniformity: at most 4;
  - Algebraic degree: $n+1$ or n for H_R and 2 for V_R;
  - Non-linearity: $2^{2n-1} - 2^n$
- $\alpha = 1$ and odd n: $H_R \Leftrightarrow F^e$ and V_R is a permutation.
  - Differential uniformity: 4;
  - Non-linearity: $2^{2n-1} - 2^n$;
  - Algebraic degree: n for H_R and 2 for V_R;

$$
\begin{tikzcd}
 & (x+\alpha y)^3 + \beta y^3 \arrow[dr, dashed] & \\
(x+\alpha y)^3 + y^3 \arrow[ur] \arrow[dr] \arrow[rr, dashed] & & (x+\alpha y)^{2^i+1} + \beta y^{2^i+1} \\
 & (x+\alpha y)^{2^i+1} + y^{2^i+1} \arrow[ur, dashed] &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & (x+\alpha y)^3+\beta y^3 \arrow[d, dotted] \\
(x+\alpha y)^3+y^3 \arrow[ur] \arrow[dr] \arrow[r, dotted] & (x+\alpha y)^{2^i+1}+\beta y^{2^i+1} \\
 & (x+\alpha y)^{2^i+1}+y^{2^i+1} \arrow[u, dotted]
\end{tikzcd}
$$

- How about the properties of more generalized butterflies?

$$(x+\alpha y)^e + y^e \Rightarrow (x+\alpha y)^e + \beta y^e$$

where $e = (2^i+1) \times 2^t$ with $\gcd(i,n) = 1$.

$$
\begin{tikzcd}
 & (x+\alpha y)^3+\beta y^3 \arrow[dr, dotted] & \\
(x+\alpha y)^3+y^3 \arrow[ur] \arrow[dr] \arrow[rr, dotted] & & (x+\alpha y)^{2^i+1}+\beta y^{2^i+1} \\
 & (x+\alpha y)^{2^i+1}+y^{2^i+1} \arrow[ur, dotted] &
\end{tikzcd}
$$

- How about the properties of more generalized butterflies?

$$(x+\alpha y)^e+y^e \Rightarrow (x+\alpha y)^e+\beta y^e$$

  where $e=(2^i+1)\times 2^t$ with $\gcd(i,n)=1$.

- The case of even n?

Our generalization and main result

$R(x,y) = (x+\alpha y)^e + \beta y^e$ where $e = (2^i + 1) \times 2^t$.
$(\alpha, \beta \neq 0$ with $\beta \neq (\alpha+1)^{2^i+1})$

Our generalization and main result

$R(x, y) = (x + \alpha y)^e + \beta y^e$ where $e = (2^i + 1) \times 2^t$.
$(\alpha, \beta \neq 0$ with $\beta \neq (\alpha + 1)^{2^i+1})$

- odd n, $\gcd(i, n) = 1$:
  - Differential uniformity: at most 4;
  - Non-linearity: $2^{2n-1} - 2^n$;
  - Algebraic degree: $n + 1$ or n for $\mathrm{H_R}$ with $\beta^{2^i-1}\left(\alpha^{2^i-1} + \alpha^{2^i+1} + \beta\right)^{2^i+1} = \left(1 + \alpha^{2^{i+1}} + \beta\alpha^{2^i-1}\right)^{2^i+1}$ and 2 for $\mathrm{V_R}$.

Our generalization and main result

$R(x,y) = (x+\alpha y)^e + \beta y^e$ where $e = (2^i+1) \times 2^t$.
$(\alpha, \beta \neq 0$ with $\beta \neq (\alpha+1)^{2^i+1})$

- odd n, $\gcd(i,n) = 1$:
    - Differential uniformity: at most 4;
    - Non-linearity: $2^{2n-1} - 2^n$;
    - Algebraic degree: $n+1$ or n for $\mathrm{H_R}$ with $\beta^{2^i-1}\left(\alpha^{2^i-1} + \alpha^{2^i+1} + \beta\right)^{2^i+1} = \left(1 + \alpha^{2^{i+1}} + \beta\alpha^{2^i-1}\right)^{2^i+1}$ and 2 for $\mathrm{V_R}$.
- $\gcd(i,n) = k$ and $\mathrm{Tr}\left(\frac{\beta}{\beta^2+(\alpha^2+1)^{2^i+1}}\right) = 1$ for $\mathrm{V_R}$:
    - Differential uniformity: at most 2^{2k};
    - Non-linearity: at least $2^{2n-1} - 2^{n+k_1-1}$, $k_1 = \gcd(2i,n)$;
    - Algebraic degree: 2.

Key point

Determine the number of solutions of a system of linear equations.

$$\begin{cases} a_1x^{2^i} + a_2x + b_1y^{2^i} + b_2y = c_1 \\ a_3x^{2^i} + a_4x + b_3y^{2^i} + b_4y = c_2. \end{cases}$$

Key point

Determine the number of solutions of a system of linear equations.

$$\begin{cases} a_1x^{2^i} + a_2x + b_1y^{2^i} + b_2y = c_1 \\ a_3x^{2^i} + a_4x + b_3y^{2^i} + b_4y = c_2. \end{cases}$$

$$\Downarrow$$

Investigate the kernel of

$$L(x,y) = A \begin{pmatrix} x^{2^i} \\ x \end{pmatrix} + B \begin{pmatrix} y^{2^i} \\ y \end{pmatrix}$$

with $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$

Relative results

Theorem 1

Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ *be two nonzero matrices over* $\mathbb{F}_{2^n}$*, and* i *be an integer with* $\gcd(i, n) = k$*. Let*

$$L(x, y) = A \begin{pmatrix} x^{2^i} \\ x \end{pmatrix} + B \begin{pmatrix} y^{2^i} \\ y \end{pmatrix}$$

be a linear mapping from $\mathbb{F}_{2^n}^2$ *to* $\mathbb{F}_{2^n}^2$*. Then,* $|\ker(L(x, y))| \leq 2^{2k} \Leftrightarrow$

1. *When* $\mathrm{rank}(A) = 1$, $\mathrm{rank}\left(\begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ a_3 & a_4 & b_3 & b_4 \end{pmatrix}\right) = 2$.
2. *When* $\mathrm{rank}(A) = 2$*, there does not exist* $\lambda \in \mathbb{F}_{2^n}^*$*, such that*

$$\begin{pmatrix} a_1\lambda^{2^i} & a_2\lambda \\ a_3\lambda^{2^i} & a_4\lambda \end{pmatrix} = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

Relative results

Lemma 1

Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ *be two matrices over* $\mathbb{F}_{2^n}$*, and* i *be an integer with* $\gcd(i, n) = k$*. Let*

$$L(x, y) = A \begin{pmatrix} x^{2^i} \\ x \end{pmatrix} + B \begin{pmatrix} y^{2^i} \\ y \end{pmatrix}$$

be a linear mapping from $\mathbb{F}_{2^n}^2$ *to* $\mathbb{F}_{2^n}^2$*. If*

$$(a_1b_3 + a_3b_1) \neq 0 \text{ or } (a_2b_4 + a_4b_2) \neq 0,$$

$|\ker(L(x, y))| \leq 2^{2k}$.

Remark: Lemma 1 can be used to reduce the proof of the non-linearity of functions generated by 3-round Feistel network. ($\alpha = 1$)

An application of Lemma 1

n is odd, $\gcd(i,n)=1$ and $(a,c)\neq(0,0)\in\mathbb{F}_{2^n}^2$,

$$\begin{cases} a^{2^i}x^{2^{2i}}+ax+c^{2^i}y^{2^{2i}}+cy=0 \\ c^{2^i}x^{2^{2i}}+cx+(a+c)^{2^i}y^{2^{2i}}+(a+c)y=0. \end{cases}$$

has at most 4 solutions.

- $\gcd(2i,n)=\gcd(i,n)=1$
- $a^{2^i}(a+c)^{2^i}+c^{2^{i+1}}=0 \Leftrightarrow a(a+c)+c^2=0$
- $a^2+ac+c^2=0$ can not hold: For any $c\in\mathbb{F}_{2^n}^*$,

$$z^2+cz+c=0 \Leftrightarrow (z/c)^2+(z/c)+1=0$$

  has no solutions since $\mathrm{Tr}(1)=1$.

Proof of differential uniformity

Prove the system of linear equations below has at most 4 solutions for any $(a, b) \neq (0, 0) \in \mathbb{F}_{2^n}^2$.

$$\begin{cases} R_{\alpha,\beta}^{2^i+1}(x, y) + R_{\alpha,\beta}^{2^i+1}(x + a, y + b) + R_{\alpha,\beta}^{2^i+1}(a, b) = 0 \\ R_{\alpha,\beta}^{2^i+1}(y, x) + R_{\alpha,\beta}^{2^i+1}(y + b, x + a) + R_{\alpha,\beta}^{2^i+1}(b, a) = 0 \end{cases}$$

Proof of differential uniformity

Prove the system of linear equations below has at most 4 solutions for any $(a, b) \neq (0, 0) \in \mathbb{F}_{2^n}^2$.

$$\begin{cases} R_{\alpha,\beta}^{2^i+1}(x, y) + R_{\alpha,\beta}^{2^i+1}(x + a, y + b) + R_{\alpha,\beta}^{2^i+1}(a, b) = 0 \\ R_{\alpha,\beta}^{2^i+1}(y, x) + R_{\alpha,\beta}^{2^i+1}(y + b, x + a) + R_{\alpha,\beta}^{2^i+1}(b, a) = 0 \end{cases}$$

$$\Downarrow \gamma = \alpha^{2^i+1} + \beta$$

$$\begin{cases} (a + \alpha b)x^{2^i} + (a + \alpha b)^{2^i} x + (\alpha^{2^i} a + \gamma b)y^{2^i} + (\alpha a^{2^i} + \gamma b^{2^i})y = 0 \\ (\gamma a + \alpha^{2^i} b)x^{2^i} + (\gamma a^{2^i} + \alpha b^{2^i})x + (\alpha a + b)y^{2^i} + (\alpha a + b)^{2^i} y = 0 \end{cases}$$

Proof of differential uniformity

Prove the system of linear equations below has at most 4 solutions for any $(a,b) \neq (0,0) \in \mathbb{F}_{2^n}^2$.

$$\begin{cases} R_{\alpha,\beta}^{2^i+1}(x,y) + R_{\alpha,\beta}^{2^i+1}(x+a,y+b) + R_{\alpha,\beta}^{2^i+1}(a,b) = 0 \\ R_{\alpha,\beta}^{2^i+1}(y,x) + R_{\alpha,\beta}^{2^i+1}(y+b,x+a) + R_{\alpha,\beta}^{2^i+1}(b,a) = 0 \end{cases}$$

$$\Downarrow \gamma = \alpha^{2^i+1} + \beta$$

$$\begin{cases} (a+\alpha b)x^{2^i} + (a+\alpha b)^{2^i}x + (\alpha^{2^i}a+\gamma b)y^{2^i} + (\alpha a^{2^i} + \gamma b^{2^i})y = 0 \\ (\gamma a + \alpha^{2^i}b)x^{2^i} + (\gamma a^{2^i} + \alpha b^{2^i})x + (\alpha a + b)y^{2^i} + (\alpha a + b)^{2^i}y = 0 \end{cases}$$

Applying the Lemma 1, we need to prove

$$\begin{aligned} (a+\alpha b)(\alpha a + b) &= (\gamma a + \alpha^{2^i}b)(\alpha^{2^i}a + \gamma b) \\ (a+\alpha b)^{2^i}(\alpha a + b)^{2^i} &= (\gamma a^{2^i} + \alpha b^{2^i})(\alpha a^{2^i} + \gamma b^{2^i}) \end{aligned}$$

cannot hold simultaneously.

$$\Updownarrow$$

Proof of differential uniformity

$$(\gamma\alpha^{2^i} + \alpha)a^2 + (\gamma^2 + \alpha^{2^{i+1}} + \alpha^2 + 1)ab + (\gamma\alpha^{2^i} + \alpha)b^2 = 0$$
$$(\gamma\alpha + \alpha^{2^i})a^{2^{i+1}} + (\gamma^2 + \alpha^{2^{i+1}} + \alpha^2 + 1)a^{2^i}b^{2^i} + (\gamma\alpha + \alpha^{2^i})b^{2^{i+1}} = 0.$$

Proof of differential uniformity

$$(\gamma\alpha^{2^i} + \alpha)a^2 + (\gamma^2 + \alpha^{2^{i+1}} + \alpha^2 + 1)ab + (\gamma\alpha^{2^i} + \alpha)b^2 = 0$$

$$(\gamma\alpha + \alpha^{2^i})a^{2^{i+1}} + (\gamma^2 + \alpha^{2^{i+1}} + \alpha^2 + 1)a^{2^i}b^{2^i} + (\gamma\alpha + \alpha^{2^i})b^{2^{i+1}} = 0.$$

$b = 0$: $\gamma\alpha^{2^i} + \alpha = \gamma\alpha + \alpha^{2^i} = 0$ can not hold ;
$b \neq 0$: set $y = a/b$, the corresponding equations have no common solutions.

Proof of differential uniformity

$$(\gamma\alpha^{2^i} + \alpha)a^2 + (\gamma^2 + \alpha^{2^{i+1}} + \alpha^2 + 1)ab + (\gamma\alpha^{2^i} + \alpha)b^2 = 0$$
$$(\gamma\alpha + \alpha^{2^i})a^{2^{i+1}} + (\gamma^2 + \alpha^{2^{i+1}} + \alpha^2 + 1)a^{2^i}b^{2^i} + (\gamma\alpha + \alpha^{2^i})b^{2^{i+1}} = 0.$$

$b = 0$: $\gamma\alpha^{2^i} + \alpha = \gamma\alpha + \alpha^{2^i} = 0$ can not hold ;
$b \neq 0$: set $y = a/b$, the corresponding equations have no common solutions.

Lemma 2

Let n be odd and i be an integer with $\gcd(i, n) = 1$, $\alpha, \beta \in \mathbb{F}_{2^n}^*$. Let $\gamma = \alpha^{2^i+1} + \beta$, $D = \gamma\alpha^{2^i} + \alpha$, $E = (\alpha+1)^{2^i+1} + \beta$, $F = \alpha^{2^i} + \gamma\alpha$. Suppose $E \neq 0$. Then the equations

$$Dx^2 + E^2x + D = 0 \quad \text{and} \quad Fx^{2^{i+1}} + E^2x^{2^i} + F = 0$$

do not have common solutions in $\mathbb{F}_{2^n}$.

Proof of Non-linearity

Prove that for $(a,b),(c,d) \in \mathbb{F}_{2^n}^2$ with $(a,b) \neq (0,0)$,

$$|\lambda_{\mathsf{V}}((c,d),(a,b))| \leq 2^{n+1}.$$

Proof of Non-linearity

Prove that for $(a,b),(c,d) \in \mathbb{F}_{2^n}^2$ with $(a,b) \neq (0,0)$,

$$|\lambda_{\mathsf{V}}((c,d),(a,b))| \leq 2^{n+1}.$$

(1) Compute $\lambda_{\mathsf{V}}((c,d),(a,b))$:

Proof of Non-linearity

Prove that for $(a,b),(c,d) \in \mathbb{F}_{2^n}^2$ with $(a,b) \neq (0,0)$,

$$|\lambda_{\mathsf{V}}((c,d),(a,b))| \leq 2^{n+1}.$$

(1) Compute $\lambda_{\mathsf{V}}((c,d),(a,b))$: Let $\gamma = \alpha^{2^i+1} + \beta$

$$\lambda_{\mathsf{V}}((c,d),(a,b)) = \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{f(x,y)} \leq \mathcal{L}(f).$$

Proof of Non-linearity

Prove that for $(a,b),(c,d) \in \mathbb{F}_{2^n}^2$ with $(a,b) \neq (0,0)$,

$$|\lambda_{\mathsf{V}}((c,d),(a,b))| \leq 2^{n+1}.$$

(1) Compute $\lambda_{\mathsf{V}}((c,d),(a,b))$: Let $\gamma = \alpha^{2^i+1} + \beta$

$$\lambda_{\mathsf{V}}((c,d),(a,b)) = \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{f(x,y)} \leq \mathcal{L}(f).$$

$$f(x,y) = \mathrm{Tr}(Ax^{2^i+1} + Bx^{2^i}y + Cxy^{2^i} + Dy^{2^i+1})$$

with

$$A = a + b\gamma, B = a\alpha + b\alpha^{2^i}, C = a\alpha^{2^i} + b\alpha, D = a\gamma + b.$$

Proof of Non-linearity

(2) Determine $\mathcal{L}(f)$:

Proof of Non-linearity

(2) Determine $\mathcal{L}(f)$:

Lemma [Anne Canteaut, Sebastien Duval, Leo Perrin. TIT 2017]

Let f be a quadratic Boolean function of n variables. Let $\mathrm{LS}(f)$ denote the linear space of f, i.e.

$$\mathrm{LS}(f) = \{a \in \mathbb{F}_{2^n} : D_a f(x) = \varepsilon, \forall x \in \mathbb{F}_{2^n}\},$$

where $\varepsilon \in \{0,1\}$. Then, $s = \dim \mathrm{LS}(f)$ has the same parity as n and $\mathcal{L}(f) = 2^{\frac{n+s}{2}}$. Moreover, the Walsh coeficients of f take 2^{n-s} times the value $\pm 2^{\frac{n+s}{2}}$ and $(2^n - 2^{n-s})$ times the value 0.

Proof of Non-linearity

(3) Prove $s = \dim \mathrm{LS}(f) = 2$:

Proof of Non-linearity

(3) Prove $s = \dim \mathrm{LS}(f) = 2$:

$$D_{(u,v)}f(x,y) = c$$

$$\Updownarrow$$

Proof of Non-linearity

(3) Prove $s = \dim \mathrm{LS}(f) = 2$:

$$D_{(u,v)}f(x,y) = c$$

$$\Updownarrow$$

$$\begin{cases} A^{2^i}u^{2^{2i}} + Au + C^{2^i}v^{2^{2i}} + Bv = 0, \\ B^{2^i}u^{2^{2i}} + Cu + D^{2^i}v^{2^{2i}} + Dv = 0. \end{cases}$$

Proof of Non-linearity

(3) Prove $s = \dim \mathrm{LS}(f) = 2$:

$$D_{(u,v)}f(x,y) = c$$

$$\Updownarrow$$

$$\begin{cases} A^{2^i}u^{2^{2i}} + Au + C^{2^i}v^{2^{2i}} + Bv = 0, \\ B^{2^i}u^{2^{2i}} + Cu + D^{2^i}v^{2^{2i}} + Dv = 0. \end{cases}$$

- $\begin{pmatrix} A^{2^i} & A \\ B^{2^i} & C \end{pmatrix}$ and $\begin{pmatrix} C^{2^i} & B \\ D^{2^i} & D \end{pmatrix}$ are nonzero matrices.

Proof of Non-linearity

(3) Prove $s = \dim \mathrm{LS}(f) = 2$:

$$D_{(u,v)} f(x,y) = c$$

$$\Updownarrow$$

$$\begin{cases} A^{2^i} u^{2^{2i}} + Au + C^{2^i} v^{2^{2i}} + Bv = 0, \\ B^{2^i} u^{2^{2i}} + Cu + D^{2^i} v^{2^{2i}} + Dv = 0. \end{cases}$$

- $\begin{pmatrix} A^{2^i} & A \\ B^{2^i} & C \end{pmatrix}$ and $\begin{pmatrix} C^{2^i} & B \\ D^{2^i} & D \end{pmatrix}$ are nonzero matrices.
- Discuss the rank of $\begin{pmatrix} A^{2^i} & A \\ B^{2^i} & C \end{pmatrix}$ and $\begin{pmatrix} A^{2^i} & A & C^{2^i} & B \\ B^{2^i} & C & D^{2^i} & D \end{pmatrix}$

in cases according to Theorem 1.

Comparison

Compare the number of CCZ-equivalent classes of V_R from different butterflies over a certain field.

Comparison

Compare the number of CCZ-equivalent classes of V_R from different butterflies over a certain field.

- Choose parameters:
  - $n = 5$ (the smallest for comparison)
  - $i = 1, 2$ ($\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is EA-equivalent to $\mathsf{V}_{\alpha,\beta^{2^{n-i}}}^{2^{n-i}+1}$)

Comparison

Compare the number of CCZ-equivalent classes of V_R from different butterflies over a certain field.

- Choose parameters:
  - $n = 5$ (the smallest for comparison)
  - $i = 1, 2$ ($\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is EA-equivalent to $\mathsf{V}_{\alpha,\beta^{2^{n-i}}}^{2^{n-i}+1}$)
- Determine all the CCZ-equivalent classes of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$
  - $S = \{\mathsf{V}_{\alpha,\beta}^{2^i+1} : \alpha, \beta \in \mathbb{F}_{2^5}^*, \beta \neq (\alpha+1)^{2^i+1}, i = 1, 2\}$;
  - Choose $h \in S$, $S_h = \{f \in S : \text{IsEquivalent}(\tilde{C}_f, \tilde{C}_h) \text{ eq true}\}$;
  - Store S_h and let $S := S \setminus S_h$;
  - Repeat until $S = \emptyset$.

Experimental results

CCZ-inequivalence functions/permutations over $\mathbb{F}_{2^5}^2$ constructed with butterfly structure:

$R(x,y)$	Represent elements	Number
$i=1,\ \beta=1$	$\alpha=1, g^{33}, g^{99}, g^{165}, g^{231}, g^{363}, g^{495}$	7
$i=2,\ \beta=1$	$\alpha=1, g^{33}, g^{99}, g^{165}, g^{363}, g^{495}$	6
$i=1,\ \beta\neq 1$	$(\alpha,\beta)=(1,g^{33}), (1,g^{165}), (g^{33},g^{33}),$ $(g^{33},g^{165}), (g^{33},g^{693}), (g^{33},g^{726})$	6
$i=2,\ \beta\neq 1$	$(\alpha,\beta)=(1,g^{33}), (1,g^{363}), (1,g^{495}),$ $(g^{33},g^{99}), (g^{33},g^{132}), (g^{33},g^{198}), (g^{99},g^{165})$	7

The case of $\gcd(i, n) = k$

The case of $\gcd(i, n) = k$

Theorem 2

Let n, i be integers with $\gcd(i, n) = k$, $\alpha, \beta \in \mathbb{F}_{2^n}^*$ and $\beta \neq (\alpha + 1)^{2^i+1}$. Let $R_{\alpha,\beta}^{2^i+1}(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$ and

$$\mathsf{V}_{\alpha,\beta}^{2^i+1}(x, y) = (R_{\alpha,\beta}^{2^i+1}(x, y), R_{\alpha,\beta}^{2^i+1}(y, x)).$$

If $\mathrm{Tr}\left(\frac{\beta}{\beta^2+(\alpha^2+1)^{2^i+1}}\right) = 1$, then the following statements hold.

1. *The differential uniformity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is at most 2^{2k}.*
2. *The nonlinearity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is at least $2^{2n-1} - 2^{n+k_1-1}$, where $k_1 = \gcd(2i, n)$.*

The case of $\gcd(i, n) = k$

Theorem 2

Let n, i be integers with $\gcd(i, n) = k$, $\alpha, \beta \in \mathbb{F}_{2^n}^*$ and $\beta \neq (\alpha + 1)^{2^i+1}$. Let $R_{\alpha,\beta}^{2^i+1}(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$ and

$$\mathsf{V}_{\alpha,\beta}^{2^i+1}(x, y) = (R_{\alpha,\beta}^{2^i+1}(x, y), R_{\alpha,\beta}^{2^i+1}(y, x)).$$

If $\mathrm{Tr}\left(\frac{\beta}{\beta^2+(\alpha^2+1)^{2^i+1}}\right) = 1$, then the following statements hold.

1. *The differential uniformity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is at most 2^{2k}.*
2. *The nonlinearity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is at least $2^{2n-1} - 2^{n+k_1-1}$, where $k_1 = \gcd(2i, n)$.*

Remark: we can get differentially 4-uniform functions $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ over $\mathbb{F}_{2^n}^2$ for any even n with $\gcd(i, n) = 1$.

Future work

Future work

- More APN permutations from the generalized butterflies?
  (A sufficient condition for $|\ker(L(x,y))| \leq 2^k$?)

Future work

- More APN permutations from the generalized butterflies?

  (A sufficient condition for $|\ker(L(x,y))| \leq 2^k$?)

- Conditions that make $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ a permutation?

  Permutations that are CCZ-equivalent to $\mathsf{V}_{\alpha,\beta}^{2^i+1}$?

Thank you!