The c-differential uniformity of some classes of permutation polynomials

Kirpa Garg

Department of Mathematics
Indian Institute of Technology Jammu
kirpa.garg@iitjammu.ac.in

Algebraic and Combinatorial Methods for Coding and Cryptography

Marseille, France
February 20-24, 2023

(Joint work with S.U. Hasan and P. Stănică)

Outline

- Notations and definitions
- Additive character and Weil sum
- Walsh transform
- The c-differential uniformity of some classes of permutation polynomials
- Conclusions

Notations and definitions

- We denote, by $\mathbb{F}_q$, the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer.
- By $\mathbb{F}_q^* = \langle g \rangle$, we denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$, where g is a primitive element of $\mathbb{F}_q$.
- We call a polynomial $f \in \mathbb{F}_q[X]$, a permutation polynomial (PP) over $\mathbb{F}_q$ if the associated mapping $X \mapsto f(X)$ is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$.
- We shall use Tr_m^n to denote the (relative) trace function from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, i.e., $\mathrm{Tr}_m^n(X) = \sum_{i=0}^{\frac{n-m}{m}} X^{p^{mi}}$, where m and n are positive integers and $m|n$. When $m = 1$, we use Tr to denote the absolute trace.

Additive character and Weil sum

Definition

The canonical additive character is a homomorphism $\chi_1 : \mathbb{F}_q \to \mathbb{C}$ of the additive group of $\mathbb{F}_q$ defined as follows

$$\chi_1(X) = \exp\left(\frac{2\pi i \operatorname{Tr}(X)}{p}\right),$$

where $\mathbb{C}$ is the field of complex numbers and $\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace defined by $\operatorname{Tr}(X) = X + X^p + X^{p^2} + \cdots + X^{p^{n-1}}$.

Additive character and Weil sum

Definition

The canonical additive character is a homomorphism $\chi_1 : \mathbb{F}_q \to \mathbb{C}$ of the additive group of $\mathbb{F}_q$ defined as follows

$$\chi_1(X) = \exp\left(\frac{2\pi i \operatorname{Tr}(X)}{p}\right),$$

where $\mathbb{C}$ is the field of complex numbers and $\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace defined by $\operatorname{Tr}(X) = X + X^p + X^{p^2} + \cdots + X^{p^{n-1}}$.

Definition

Let χ is an additive character of $\mathbb{F}_q$ and $f(X)$ is a polynomial in $\mathbb{F}_q[X]$. Then the Weil sum of the function f, is defined as follows

$$\sum_{X \in \mathbb{F}_q} \chi(f(X)).$$

Characters and Equations over Finite Fields

- It is easy to observe that over finite fields of characteristic p, the canonical additive character can be written as

  $\chi_1(X) = \omega^{\mathrm{Tr}(X)}$, where ω is a complex primitive p^{th} root of unity.

- Character sums are also useful in counting the number of solutions of certain equations or system of equations over finite fields.
- For instance, the number of solutions $(X_1, X_2, \ldots, X_n) \in \mathbb{F}_q^n$ of the equation $f(X_1, X_2, \ldots, X_n) = b$, is given by

$$\frac{1}{q} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \chi_1(\beta(f(X_1, X_2, \ldots, X_n) - b)),$$

or equivalently,

$$\frac{1}{q} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \omega^{\mathrm{Tr}(\beta(f(X_1, X_2, \ldots, X_n) - b))}.$$

Walsh transform

Definition

For a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the Walsh transform of F at $v \in \mathbb{F}_{p^n}$, is defined as

$$\mathcal{W}_F(v) = \sum_{X \in \mathbb{F}_{p^n}} \omega^{F(X) - \mathrm{Tr}(vX)},$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a complex primitive pth root of unity.

Differential uniformity

- Substitution boxes play a very crucial role in the design of secure cryptographic primitives, such as block ciphers.
- Differential attack, introduced by Biham and Shamir[1] is one of the most efficient attack on the substitution boxes used in the block cipher.
- To quantify the degree of security of a substitution box, against the differential attack, Nyberg[2] introduced the notion of differential uniformity (DU).

[1] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptol. 4(1) (1991), 3–72.

[2] K. Nyberg, *Differentially uniform mappings for cryptography.* In: Helleseth T. (eds.), Advances in Cryptology–EUROCRYPT 1993, LNCS 765, Springer, Berlin, Heidelberg, pp. 55–64, 1994.

Differential uniformity

Definition

For any function $f : \mathbb{F}_q \to \mathbb{F}_q$ and $a \in \mathbb{F}_q$, the derivative of f in the direction a, denoted by $D_f(X, a)$, is defined as

$$D_f(X, a) := f(X + a) - f(X)$$

for all $X \in \mathbb{F}_q$.

Differential uniformity

Definition

For any function $f : \mathbb{F}_q \to \mathbb{F}_q$ and $a \in \mathbb{F}_q$, the derivative of f in the direction a, denoted by $D_f(X, a)$, is defined as

$$D_f(X, a) := f(X + a) - f(X)$$

for all $X \in \mathbb{F}_q$.

Definition

For any $a, b \in \mathbb{F}_q$, the Difference Distribution Table (DDT) entry at point (a, b), denoted by $\Delta_f(a, b)$, is defined as

$$\Delta_f(a, b) := |\{X \in \mathbb{F}_q \mid D_f(X, a) = b\}|.$$

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a,b) \mid a,b \in \mathbb{F}_q, a \neq 0\}.$$

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a,b) \mid a,b \in \mathbb{F}_q, a \neq 0\}.$$

- When $\Delta_f = \delta$, we say that the function f is δ-uniform.

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a,b) \mid a,b \in \mathbb{F}_q, a \neq 0\}.$$

- When $\Delta_f = \delta$, we say that the function f is δ-uniform.
- When $\delta = 1$, we say that the function f is perfect nonlinear (PN) function.

Differential uniformity

Definition

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a,b) \mid a,b \in \mathbb{F}_q, a \neq 0\}.$$

- When $\Delta_f = \delta$, we say that the function f is δ-uniform.
- When $\delta = 1$, we say that the function f is perfect nonlinear (PN) function.
- When $\delta = 2$, we say that the function f is almost perfect nonlinear (APN) function.

Multiplicative differentials

- In 2002, Borisov et al.[3] introduced the notion of multiplicative differentials of the form $(f(cX), f(X))$ and used this new type of differentials to attack some existing ciphers.

[3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative differentials*. In: J. Daemen and V. Rijmen (eds.) Proceedings of Fast Software Encryption - FSE 2002. Lecture Notes in Comput. Sci., Springer, Berlin, Heidelberg, vol. 2365 (2002), 17–33.

[4] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inform. Theory 66:9 (2020), 5781–5789.

Multiplicative differentials

- In 2002, Borisov et al.[3] introduced the notion of multiplicative differentials of the form $(f(cX), f(X))$ and used this new type of differentials to attack some existing ciphers.
- In 2020, Ellingsen et al.[4] defined a new (output) multiplicative differential in the following way.

[3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative differentials*. In: J. Daemen and V. Rijmen (eds.) Proceedings of Fast Software Encryption - FSE 2002. Lecture Notes in Comput. Sci., Springer, Berlin, Heidelberg, vol. 2365 (2002), 17–33.

[4] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inform. Theory 66:9 (2020), 5781–5789.

The c-differential uniformity

Definition (Ellingsen et. al, 2020)

For any function f from a finite field $\mathbb{F}_q$ to itself and for any $a, c \in \mathbb{F}_q$, the (multiplicative) c-derivative of f with respect to a is defined as

$$_cD_f(X, a) := f(X + a) - cf(X) \text{ for all } X \in \mathbb{F}_q.$$

The c-differential uniformity

Definition (Ellingsen et. al, 2020)

For any function f from a finite field $\mathbb{F}_q$ to itself and for any $a, c \in \mathbb{F}_q$, the (multiplicative) c-derivative of f with respect to a is defined as

$$_cD_f(X, a) := f(X + a) - cf(X) \text{ for all } X \in \mathbb{F}_q.$$

Definition (Ellingsen et al., 2020)

For $a, b \in \mathbb{F}_q$, the c-Difference Distribution Table (cDDT) entry of f at point (a, b), denoted by $_c\Delta_f(a, b)$, is given by

$$_c\Delta_f(a, b) := |\{X \in \mathbb{F}_q : \ _cD_f(X, a) = b\}|.$$

The c-differential uniformity

Definition (Ellingsen et al., 2020)

The c-differential uniformity (cDU) of f, denoted as ${}_c\Delta_f$, is defined as

$$ {}_c\Delta_f := \max\{{}_c\Delta_F(a,b) : a,b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ if } c = 1\}. $$

The c-differential uniformity

Definition (Ellingsen et al., 2020)

The c-differential uniformity (cDU) of f, denoted as ${}_c\Delta_f$, is defined as

$$ {}_c\Delta_f := \max\{{}_c\Delta_F(a,b) : a,b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ if } c = 1\}. $$

- When ${}_c\Delta_f = \delta$ then we say that the function f is (c,δ)-uniform.

The c-differential uniformity

Definition (Ellingsen et al., 2020)

The c-differential uniformity (cDU) of f, denoted as ${}_c\Delta_f$, is defined as

$$ {}_c\Delta_f := \max\{{}_c\Delta_F(a,b) : a,b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ if } c = 1\}. $$

- When ${}_c\Delta_f = \delta$ then we say that the function f is (c,δ)-uniform.
- When ${}_c\Delta_f = 1$ then f is called perfect c-nonlinear (PcN) function.

The c-differential uniformity

Definition (Ellingsen et al., 2020)

The c-differential uniformity (cDU) of f, denoted as ${}_c\Delta_f$, is defined as

$$ {}_c\Delta_f := \max\{{}_c\Delta_F(a,b) : a,b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ if } c = 1\}. $$

- When ${}_c\Delta_f = \delta$ then we say that the function f is (c,δ)-uniform.
- When ${}_c\Delta_f = 1$ then f is called perfect c-nonlinear (PcN) function.
- When ${}_c\Delta_f = 2$ then f is called almost perfect c-nonlinear (APcN) function.

Steps towards applications

- D. Bartoli, L. Kölsch and G. Micheli, *Differential biases, c-differential uniformity, and their relation to differential attacks*, `arXiv:2208.03884`, (2022).
- N. Anbar, T. Kalayci, W. Meidl, C. Riera, P. Stănică, *P$\wp$N functions, complete mappings and quasigroup difference sets* , `https://arxiv.org/abs/2212.12943` (2022).

Permutation Polynomials

In 2018, Li et al. [5]showed that the following functions are permutation polynomials :

- $F_1(X) = (X^{2^m} + X + \delta)^{2^{2m}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$.

[5]L. Li, S. Wang, C. Li, and X. Zeng, *Permutation polynomials* $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ *over* $\mathbb{F}_{p^n}$, Finite Fields Appl. 51 (2018), 31–61.

Permutation Polynomials

In 2018, Li et al. [5]showed that the following functions are permutation polynomials :

- $F_1(X) = (X^{2^m} + X + \delta)^{2^{2m}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$.
- $F_2(X) = (X^{2^m} + X + \delta)^{2^{im-1}+2^{m-1}} + X$ over $\mathbb{F}_{2^n}$, where $i \in \{2, 3\}$, $\gcd((i-1)m - 1, 3m) = 1$, $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$.

[5]L. Li, S. Wang, C. Li, and X. Zeng, *Permutation polynomials* $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ *over* $\mathbb{F}_{p^n}$, Finite Fields Appl. 51 (2018), 31–61.

Permutation Polynomials

In 2018, Li et al. [5]showed that the following functions are permutation polynomials :

- $F_1(X) = (X^{2^m} + X + \delta)^{2^{2m}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$.
- $F_2(X) = (X^{2^m} + X + \delta)^{2^{im-1}+2^{m-1}} + X$ over $\mathbb{F}_{2^n}$, where $i \in \{2, 3\}$, $\gcd((i-1)m - 1, 3m) = 1$, $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$.
- $F_3(X) = (X^{3^m} - X + \delta)^{3^{2m-1}+2\cdot 3^{m-1}} + X$ over $\mathbb{F}_{3^n}$, where $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$.

[5]L. Li, S. Wang, C. Li, and X. Zeng, *Permutation polynomials* $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ *over* $\mathbb{F}_{p^n}$, Finite Fields Appl. 51 (2018), 31–61.

Permutation Polynomials

In 2018, Li et al. [5]showed that the following functions are permutation polynomials :

- $F_1(X) = (X^{2^m} + X + \delta)^{2^{2m}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$.
- $F_2(X) = (X^{2^m} + X + \delta)^{2^{im-1}+2^{m-1}} + X$ over $\mathbb{F}_{2^n}$, where $i \in \{2, 3\}$, $\gcd((i-1)m - 1, 3m) = 1$, $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$.
- $F_3(X) = (X^{3^m} - X + \delta)^{3^{2m-1}+2\cdot 3^{m-1}} + X$ over $\mathbb{F}_{3^n}$, where $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$.
- $F_4(X) = (X^{p^m} - X + \delta)^{p^{m+1}+1} + X$, where $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$, such that $\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\dfrac{\mathrm{Tr}_m^{2m}(\delta)+1}{\mathrm{Tr}_m^{2m}(\delta)}$ is a $(p-1)$-th power in $\mathbb{F}_{p^m}$.

[5]L. Li, S. Wang, C. Li, and X. Zeng, *Permutation polynomials* $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ *over* $\mathbb{F}_{p^n}$, Finite Fields Appl. 51 (2018), 31–61.

Results

- There are only a few general non-trivial classes of PcN functions over binary finite fields.
- Our purpose: find more general classes of such low cDU functions.

We computed the c-differential uniformity of the prior four classes of permutation polynomials. In particular, our work adds to very few known classes of PcN functions.

Theorem 1 (First class)

Let $F_1(X) = (X^{2^m} + X + \delta)^{2^{2m}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$. Let $\Gamma_1 := \{\delta \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^{3m}(\delta) = 1\}$. Then:

1. F_1 is PcN for all $c \in \mathbb{F}_{2^m} \setminus \{1\}$ and for all $\delta \in \mathbb{F}_{2^n}$;
2. F_1 is APcN for all $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \Gamma_1$;
3. F_1 is of c-differential uniformity ≤ 4 for all $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \mathbb{F}_{2^n} \setminus \Gamma_1$.

Idea of the proof

- Recall that the c-DDT entry ${}_c\Delta_{F_1}(a,b)$ at the point (a,b) of the function $F_1(X)$ is given by the number of solutions $X \in \mathbb{F}_q$ of the equation $F_1(X+a) + cF_1(X) = b$ which can be further written as

$$(1+c)F_1(X) + \mathrm{Tr}_m^{3m}((a^{2^{2m}} + a^{2^m})X) = b + F_1(a) + \delta^{2^{2m}+1}.$$

Idea of the proof

- Recall that the c-DDT entry ${}_c\Delta_{F_1}(a,b)$ at the point (a,b) of the function $F_1(X)$ is given by the number of solutions $X \in \mathbb{F}_q$ of the equation $F_1(X+a)+cF_1(X)=b$ which can be further written as

$$(1+c)F_1(X)+\mathrm{Tr}_m^{3m}((a^{2^{2m}}+a^{2^m})X)=b+F_1(a)+\delta^{2^{2m}+1}.$$

- Thus, the # of solutions $X \in \mathbb{F}_q$ of the above eqn, ${}_c\Delta_{F_1}(a,b)$, is given by

$$\frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}\left(\beta\left((1+c)F_1(X)+\mathrm{Tr}_m^{3m}((a^{2^{2m}}+a^{2^m})X)+b+F_1(a)+\delta^{2^{2m}+1}\right)\right)}$$

$$=\frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(F_1(a)+b+\delta^{2^{2m}+1}))}$$

$$\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}\left(\beta(1+c)F_1(X)+\beta\mathrm{Tr}_m^{3m}((a^{2^{2m}}+a^{2^m})X)\right)}$$

- We can further simplify the above expression to get,

$$ {}_c\Delta_{F_1}(a,b) = \frac{1}{2^n} \sum_{\beta \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(F_1(a)+b+\delta^{2^{2m}+1}))} \sum_{X \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(uX^{2^{m+1}}+vX\right)} $$

where,

$$ u = \mathrm{Tr}_m^{3m}((1+c)\beta), $$
$$ v = \delta^{2^m}\mathrm{Tr}_m^{3m}((1+c)\beta) + ((1+c)\beta)^{2^{3m-1}} + \beta(1+c)(1+\mathrm{Tr}_m^{3m}(\delta)) + (a^{2^{2m}} + a^{2^m})\mathrm{Tr}_m^{3m}(\beta). $$

- Let S_0 and S_1 be the sums corresponding to $\mathrm{Tr}_m^{3m}((1+c)\beta) = 0$ and $\mathrm{Tr}_m^{3m}((1+c)\beta) \neq 0$, respectively. Then ${}_c\Delta_{F_1}(a,b) = \frac{1}{2^n}(S_0 + S_1)$.

Case 1.

Let $c \in \mathbb{F}_{2^m} \setminus \{1\}$ and $\delta \in \mathbb{F}_{2^n}$.

- We first considered the sum S_0 as given below.

$$S_0 = 2^n + \sum_{\substack{\beta \in \mathbb{F}_{2^n}^* \\ \mathrm{Tr}_m^{3m}(\beta)=0}} (-1)^{\mathrm{Tr}(\beta(F_1(a)+b+c\delta^{2^{2m}+1}))}$$

$$\sum_{X \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}((((1+c)\beta)^{2^{3m-1}} + (1+c)(1+\mathrm{Tr}_m^{3m}(\delta))\beta)X)} = 2^n$$

The above equality is because:

1. When $\mathrm{Tr}_m^{3m}(\delta) = 1$, $((1+c)\beta)^{2^{3m-1}} X$ is a permutation over $\mathbb{F}_{2^n}$, thus making the inner sum vanish.
2. When $\mathrm{Tr}_m^{3m}(\delta) \neq 1$, $((1+c)\beta)^{2^{3m-1}} + (1+c)(1+\mathrm{Tr}_m^{3m}(\delta))\beta$ vanishes for two values of β, namely, $\beta = 0$ and $\beta = \beta_1$. One can show that, $\mathrm{Tr}_m^{3m}(\beta_1) \neq 0$, and thus we can exclude β_1 from the inner sum of S_0.

Case 1.

- Next, we compute the sum S_1, using the walsh transform.

$$S_1 = \sum_{\substack{\beta \in \mathbb{F}_{2^n} \\ \mathrm{Tr}_m^{3m}(\beta) \neq 0}} (-1)^{\mathrm{Tr}(\beta(F_1(a)+b+c\delta^{2^{2m}+1}))} \mathcal{W}_G(v),$$

where $\mathcal{W}_G(v)$ is the Walsh coefficient of the trace of the function $G : X \mapsto uX^{2^m+1}$. We show that $\mathcal{W}_G(v) = 0$, and hence, $S_1 = 0$ using the following lemma.

Lemma

Let $u \in \mathbb{F}_{2^m}^*$ and $G(X) := uX^{2^m+1}$ be a function on $\mathbb{F}_{2^n}$, where $n = 3m$. Then $\mathcal{W}_G(v) = 0$ if $\mathrm{Tr}(v) = 0$.

- Hence, ${}_c\Delta_{F_1}(a, b) = \frac{1}{2^n}(S_0 + S_1) = 1$.

Case 2.

Let $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \Gamma_1$.

- In this case, S_0 is given by the following expression.

$$S_0 = \sum_{\substack{\beta \in \mathbb{F}_{2^n} \\ \mathrm{Tr}_m^{3m}((1+c)\beta)=0}} (-1)^{\mathrm{Tr}(\beta(F_1(a)+b+c\delta^{2^{2m}+1}))}$$
$$\sum_{X \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}((((1+c)\beta)^{2^{3m-1}} + (a^{2^{2m}} + a^{2^m})\mathrm{Tr}_m^{3m}(\beta))X)}$$

We will have two subcases:

1. $S_0 = 2^n$ for those pairs $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying $a^{2^{2m}} + a^{2^m} = 0$.
2. $S_0 = 2^{n+1}$ or those pairs $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying $a^{2^{2m}} + a^{2^m} \neq 0$ and $b = c\delta^{2^{2m}+1} + F_1(a)$. This is due to two solutions $\beta = 0$ and $\beta = \beta_1$ of the following equation: $\dfrac{(1+c)\beta)^{2^{3m-1}}}{a^{2^{2m}} + a^{2^m}} + \mathrm{Tr}_m^{3m}(\beta) = 0.$

From the above subcases, we have $S_0 = 2^{n+1}$.

Case 2.

- Next, we compute S_1, using the walsh transform.

$$S_1 = \sum_{\substack{\beta \in \mathbb{F}_{2^n} \\ \mathrm{Tr}_m^{3m}(\beta) \neq 0}} (-1)^{\mathrm{Tr}(\beta(F_1(a)+b+c\delta^{2^{2m}+1}))} \mathcal{W}_G(v),$$

  where $\mathcal{W}_G(v)$ is the Walsh coefficient of the trace of the function $G : X \mapsto uX^{2^m+1}$. Using the similar arguments as in Case 1, one can show that $S_1 = 0$.
- This gives us, ${}_c\Delta_{F_1}(a,b) = \frac{1}{2^n}(S_0 + S_1) = 2$.

Case 3.

Let $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \mathbb{F}_{2^n} \setminus \Gamma_1$.

- The expression for the sum S_0 is given as:

$$S_0 = \sum_{\substack{\beta \in \mathbb{F}_{2^n} \\ \mathrm{Tr}_m^{3m}((1+c)\beta)=0}} (-1)^{\mathrm{Tr}(\beta(F_1(a)+b+c\delta^{2^{2m}+1}))}$$
$$\sum_{X \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}((((1+c)\beta)^{2^{3m-1}}+\beta(1+c)(1+\mathrm{Tr}_m^{3m}(\delta))+(a^{2^{2m}}+a^{2^m})\mathrm{Tr}_m^{3m}(\beta))X)}.$$

We conclude that $S_0 \leq 2^{n+2}$ by giving the following lemma.

Lemma

Let m be a positive integer, $a \in \mathbb{F}_{2^n}$, where $n = 3m$. Furthermore, let $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_m^{3m}(\delta) \neq 1$ and $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Then the following equation

$$((1+c)X)^{2^{-1}} + (1+c)(1+\mathrm{Tr}_m^{3m}(\delta))X + (a^{2^{2m}} + a^{2^m})\mathrm{Tr}_m^{3m}(X) = 0 \quad (4.1)$$

has at most four solutions in $\mathbb{F}_{2^n}$ under the restriction that $\mathrm{Tr}_m^{3m}((1+c)X) = 0$.

Case 3.

- Next, we compute S_1.

$$S_1 = \sum_{\substack{\beta \in \mathbb{F}_{2^n} \\ \mathrm{Tr}_m^{3m}((1+c)\beta) \neq 0}} (-1)^{\mathrm{Tr}(\beta(F_1(a)+b+c\delta^{2^{2m}+1}))} \sum_{X \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}}(uX^{2^m+1} + vX),$$

  where $\mathcal{W}_G(v)$ is the Walsh coefficient of the trace of the function $G : X \mapsto uX^{2^m+1}$. Using the similar arguments as in Case 1, one can show that $S_1 = 0$.

- This gives us, ${}_c\Delta_{F_1}(a, b) = \frac{1}{2^n}(S_0 + S_1) \leq 4$.

Results

Theorem 2 (Second Class)

Let $F_2(X) = (X^{2^m} + X + \delta)^{2^{2m-1}+2^{m-1}} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m, \delta \in \mathbb{F}_{2^n}$ and $m \not\equiv 1 \pmod 3$.
Let $\Gamma_0 := \{\delta \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^{3m}(\delta) = 0\}$. Then:

1. F_2 is PcN for all $c \in \mathbb{F}_{2^m} \setminus \{1\}$ and for all $\delta \in \mathbb{F}_{2^n}$;
2. F_2 is APcN for all $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \Gamma_0$;
3. F_2 is of c-differential uniformity ≤ 4 for all $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \mathbb{F}_{2^n} \setminus \Gamma_0$.

Permutations over $\mathbb{F}_{p^n}$ with low c-differential uniformity

Theorem 3 (Third Class)

Let $F_3(X) = (X^{3^m} - X + \delta)^{3^{2m-1}+2\cdot 3^{m-1}} + X$ over $\mathbb{F}_{3^n}$, where $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. Let $\Gamma_0 := \{\delta \in \mathbb{F}_{3^n} : \mathrm{Tr}_m^{2m}(\delta) = 0\}$. Then:

i. F_3 is PcN for all $c \in \mathbb{F}_{3^m} \setminus \{1\}$ and for all $\delta \in \mathbb{F}_{3^n}$;

ii. F_3 is PcN for all $c \in \mathbb{F}_{3^n} \setminus \mathbb{F}_{3^m}$ and for all $\delta \in \Gamma_0$. Moreover, it is of c-differential uniformity 3 for all $c \in \mathbb{F}_{3^n} \setminus \mathbb{F}_{3^m}$ and for all $\delta \in \mathbb{F}_{3^n} \setminus \Gamma_0$.

Permutations over $\mathbb{F}_{p^n}$ with low c-differential uniformity

Theorem 3 (Third Class)

Let $F_3(X) = (X^{3^m} - X + \delta)^{3^{2m-1}+2\cdot 3^{m-1}} + X$ over $\mathbb{F}_{3^n}$, where $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. Let $\Gamma_0 := \{\delta \in \mathbb{F}_{3^n} : \mathrm{Tr}_m^{2m}(\delta) = 0\}$. Then:

i. F_3 is PcN for all $c \in \mathbb{F}_{3^m} \setminus \{1\}$ and for all $\delta \in \mathbb{F}_{3^n}$;

ii. F_3 is PcN for all $c \in \mathbb{F}_{3^n} \setminus \mathbb{F}_{3^m}$ and for all $\delta \in \Gamma_0$. Moreover, it is of c-differential uniformity 3 for all $c \in \mathbb{F}_{3^n} \setminus \mathbb{F}_{3^m}$ and for all $\delta \in \mathbb{F}_{3^n} \setminus \Gamma_0$.

Theorem 4 (Fourth Class)

Let $F_4(X) = (X^{p^m} - X + \delta)^{p^{m+1}+1} + X$ over $\mathbb{F}_{p^n}$, where $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$, where $\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\frac{\mathrm{Tr}_m^{2m}(\delta)-1}{\mathrm{Tr}_m^{2m}(\delta)}$ is a $(p-1)$-th power in $\mathbb{F}_{p^m}$. Then

i. F_4 is PcN for all $c \in \mathbb{F}_{p^m} \setminus \{1\}$;

ii. F_4 is of c-differential uniformity p for all $c \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$.

Idea of proof

- We know that for any $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, the c-DDT entry ${}_c\Delta_{F_4}(a, b)$ is given by the number of solutions $X \in \mathbb{F}_{p^n}$ of the following equation $F_4(X + a) - cF_4(X) = b$, or, equivalently,

$$(1-c)F_4(X) + \mathrm{Tr}_m^{2m}(aX^{p^{m+1}} + (a^{p^{m+1}} - a^p)X - aX^p) + F_4(a) - \delta^{p^{m+1}+1} = b.$$

- Also one can recall that the number of solutions $X \in \mathbb{F}_{p^n}$ of the above Equation, ${}_c\Delta_{F_4}(a, b)$, is given by

$${}_c\Delta_F(a,b) = \frac{1}{p^n} \sum_{\beta \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}\left(\beta\left(F(a)-b-\delta^{p^{m+1}+1}\right)\right)} \sum_{X \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}\left(\beta((1-c)F(X)+\mathrm{Tr}_m^{2m}(aX^{p^{m+1}}+(a^{p^{m+1}}-a^p)X-aX^p)\right)},$$

where $\omega = e^{2\pi i/p}$, a complex primitive p^{th} root of unity.

- We can further rewrite the equation as,

$$
{}_c\Delta_{F_4}(a,b) = \frac{1}{p^n} \sum_{\beta \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(\beta(F(a)-b-c\delta^{p^{m+1}+1}))} \sum_{X \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(u_1 X^{p^{m-1}+1} - u_2 X^{p+1} + vX)},
$$

where,

$$
\begin{aligned}
u_1 &= \mathrm{Tr}_m^{2m}(\beta(1-c))^{p^{m-1}} \\
u_2 &= \mathrm{Tr}_m^{2m}(\beta(1-c)) \\
v &= (\beta(1-c)\delta)^{p^{2m-1}} - (\beta(1-c)\delta)^{p^{m-1}} + (\beta(1-c)\delta^{p^{m+1}})^{p^m} \\
&\quad + \beta(1-c)(1-\delta^{p^{m+1}}) + (a-a^{p^m})^{p^{m-1}} \mathrm{Tr}_m^{2m}(\beta^{p^{m-1}}) \\
&\quad + (a^{p^{m+1}} - a^p)\mathrm{Tr}_m^{2m}(\beta).
\end{aligned}
$$

- Next, we split the above sum depending on whether $\mathrm{Tr}_m^{2m}((1+c)\beta)$ is 0 or not, namely S_0 and S_1. Then ${}_c\Delta_{F_4}(a,b) = \frac{1}{p^n}(S_0 + S_1)$.

Case 1.

Let $c \in \mathbb{F}_{p^m} \setminus \{1\}$.

- First consider the sum S_0 as given below.

$$S_0 = \sum_{\substack{\beta \in \mathbb{F}_{p^n} \\ \mathrm{Tr}_m^{2m}(\beta)=0}} \omega^{\mathrm{Tr}(\beta(F_4(a)-b-c\delta^{p^{m+1}+1}))} \sum_{X \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}\left(-(\beta(1-c))^{p^{m-1}} \mathrm{Tr}_m^{2m}(\delta^{p^{m-1}})X+(1-c)\beta(1-\mathrm{Tr}_m^{2m}(\delta^p))X\right)}$$

Next we compute S_0 for the following possibilities of δ:

- When $\mathrm{Tr}_m^{2m}(\delta) = 0$, then the inner sum in S_0 becomes zero, except for $\beta = 0$ and hence we have $S_0 = p^n$.
- When $\mathrm{Tr}_m^{2m}(\delta) \neq 0$ and $\gamma^{p-1} = \frac{\mathrm{Tr}_m^{2m}(\delta)-1}{\mathrm{Tr}_m^{2m}(\delta)}$ for some $\gamma \in \mathbb{F}_{p^m}$, then the inner sum in S_0 is zero for $\beta = 0$ and $\beta = \beta_1 = \frac{\alpha}{\gamma(1-c)(1-\mathrm{Tr}_m^{2m}(\delta))^{p+1}}$ for $\alpha \in \mathbb{F}_{p^n}$ such that $\alpha^{p-1} = 1$. But $\mathrm{Tr}_m^{2m}(\beta_1) \neq 0$, hence making $S_0 = p^n$.

Case 1.

- Next, we consider the sum S_1.

$$S_1 = \sum_{\substack{\beta \in \mathbb{F}_{p^n} \\ \mathrm{Tr}_m^{2m}(\beta) \neq 0}} \omega^{\mathrm{Tr}(\beta(F_4(a) - b - c\delta^{p^{m+1}+1}))} \sum_{X \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}\left(u_1 X^{p^{m-1}+1} - u_2 X^{p+1} + vX\right)}$$

$$= \sum_{\substack{\beta \in \mathbb{F}_{p^n} \\ \mathrm{Tr}_m^{2m}(\beta) \neq 0}} \omega^{\mathrm{Tr}(\beta(F_4(a) - b - c\delta^{p^{m+1}+1}))} \mathcal{W}_G(-v),$$

where, $\mathcal{W}_G(-v)$ is Walsh transform of trace of function $G : X \mapsto u_1 X^{p^{m-1}+1} - u_2 X^{p+1}$ at $-v$.

- Next, we use the following lemma [6] to show $S_1 = 0$.

Lemma

Let m be a positive integer and $n = 2m$. Also, let $a_i \in \mathbb{F}_{p^n} (i = 0, \ldots, m)$ for an odd prime p. Then the absolute square of Walsh transform coefficient of the function $f(X) = \mathrm{Tr}\left(\sum_{i=0}^{m} a_i X^{p^i+1}\right)$ at $v \in \mathbb{F}_{p^n}$ is given by

$$|\mathcal{W}_f(v)|^2 = \begin{cases} p^{n+\ell} & \text{if } f(X) + \mathrm{Tr}(-vX) \equiv 0 \text{ on Ker } (L) \\ 0 & \text{otherwise,} \end{cases}$$

where ℓ is dimension of kernel of the linearized polynomial $L(X) = \sum_{i=0}^{m} (a_i X^{p^i} + (a_i X)^{p^{n-i}})$.

- Hence ${}_c\Delta_{F_4}(a, b) = \frac{1}{p^n}(S_0 + S_1) = 1$.

[6] T. Helleseth and A. Kholosha, *Monomial and quadratic bent functions over the finite fields of odd characteristic.* IEEE Trans. Inf. Theory 52, no. 5 (2006), 2018–2032.

Case 2.

Let $c \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$. We consider the following subcases to compute S_0.

- **Subcase 1.** Let $\mathrm{Tr}_m^{2m}(\delta) = 0$ then we have,

$$S_0 = \sum_{\substack{\beta \in \mathbb{F}_{p^n} \\ \mathrm{Tr}_m^{2m}(\beta(1-c))=0}} \omega^{\mathrm{Tr}(\beta(F_4(a)-b-c\delta^{p^{m+1}+1}))} \sum_{X \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}\left((\beta(1-c)+(a-a^{p^m})^{p^{m-1}}\mathrm{Tr}_m^{2m}(\beta^{p^{m-1}})+(a^{p^{m+1}}-a^p)\mathrm{Tr}_m^{2m}(\beta))X\right)}.$$

Now to compute the inner sum in S_0, we need to look for solutions $\beta \in \mathbb{F}_{p^n}$ of the equation given below,

$$\beta(1-c) + (a-a^{p^m})^{p^{m-1}}\mathrm{Tr}_m^{2m}(\beta^{p^{m-1}}) + (a^{p^{m+1}} - a^p)\mathrm{Tr}_m^{2m}(\beta) = 0.$$

or, equivalently $A\beta^p + B\beta = 0$, where

$$A = \left(1 - c + (a^{p^m} - a)^p \left(1 - \frac{1-c}{(1-c)^{p^m}}\right)\right)^p,$$

$$B = (a^{p^m} - a)\left(1 - \frac{(1-c)}{(1-c)^{p^m}}\right).$$

Case 2.

Next, we show that the equation $A\beta^p + B\beta = 0$, except for $\beta = 0$, has $p-1$ solutions in $\mathbb{F}_{p^n}$ only if $\frac{-B}{A}$ is $(p-1)$th power of some element in $\mathbb{F}_{p^n}$, by giving the following lemma.

Case 2.

Next, we show that the equation $A\beta^p + B\beta = 0$, except for $\beta = 0$, has $p-1$ solutions in $\mathbb{F}_{p^n}$ only if $\frac{-B}{A}$ is $(p-1)$th power of some element in $\mathbb{F}_{p^n}$, by giving the following lemma.

Lemma

Let $c \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$, $n = 2m$. With the following notations

$$A = \left(1 - c + (a^{p^m} - a)^p \left(1 - \frac{1-c}{(1-c)^{p^m}}\right)\right)^p,$$

$$B = (a^{p^m} - a)\left(1 - \frac{(1-c)}{(1-c)^{p^m}}\right),$$

then there exists $a \in \mathbb{F}_{p^n}$ such that $A + Bd^{p-1} = 0$, for some $d \in \mathbb{F}_{p^n}$.

Case 2.

Next, we show that the equation $A\beta^p + B\beta = 0$, except for $\beta = 0$, has $p-1$ solutions in $\mathbb{F}_{p^n}$ only if $\frac{-B}{A}$ is $(p-1)$th power of some element in $\mathbb{F}_{p^n}$, by giving the following lemma.

Lemma

Let $c \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$, $n = 2m$. With the following notations

$$A = \left(1 - c + (a^{p^m} - a)^p \left(1 - \frac{1-c}{(1-c)^{p^m}}\right)\right)^p,$$

$$B = (a^{p^m} - a)\left(1 - \frac{(1-c)}{(1-c)^{p^m}}\right),$$

then there exists $a \in \mathbb{F}_{p^n}$ such that $A + Bd^{p-1} = 0$, for some $d \in \mathbb{F}_{p^n}$.

It is easy to see that for those pairs $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ for which $b = F_4(a) - c\delta^{p^{m+1}+1}$, we have $S_0 = p^{n+1}$; and for the other pairs $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, we have $S_0 = 0$. This gives us $S_0 = p^{n+1}$.

Case 2.

- **Subcase 2.**

  Let $\frac{\mathrm{Tr}_m^{2m}(\delta)-1}{\mathrm{Tr}_m^{2m}(\delta)} = \gamma^{p-1}$ for $\gamma \in \mathbb{F}_{p^m}$. Now, S_0 is given by

$$S_0 = \sum_{\substack{\beta\in\mathbb{F}_{p^n} \\ \mathrm{Tr}_m^{2m}(\beta(1-c))=0}} \omega^{\mathrm{Tr}(\beta(F_4(a)-b-c\delta^{p^{m+1}+1}))} \sum_{X\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}\left(\left(\frac{\beta(1-c)}{1-\gamma^{p-1}}\right)^{p^{2m-1}}X\right)}$$
$$\omega^{\mathrm{Tr}\left(\left(\beta(1-c)\left(1-\frac{1}{1-\gamma^{p-1}}\right)^{p}+(a-a^{p^m})^{p^{m-1}}\mathrm{Tr}_m^{2m}(\beta^{p^{m-1}})-(a-a^{p^m})^{p}\mathrm{Tr}_m^{2m}(\beta)\right)X\right)}.$$

  After solving the equation in the inner sum S_0, one can see that if $a \in \mathbb{F}_{p^m}$, then $S_0 = p^{n+1}$. Otherwise, it will either have exactly one solution $\beta = 0$ or p solutions in $\mathbb{F}_{p^n}$. Then using the same arguments as in the case of $\mathrm{Tr}_m^{2m}(\delta) = 0$, we get that either $S_0 = p^n$, or $S_0 = p^{n+1}$.

- Thus for the both subcases, we have $S_0 = p^{n+1}$.

Case 2.

- Next, we have

$$S_1 = \sum_{\substack{\beta \in \mathbb{F}_{p^n} \\ \mathrm{Tr}_m^{2m}(\beta(1-c)) \neq 0}} \omega^{\mathrm{Tr}(\beta(F_4(a)-b-c\delta^{p^{m+1}+1}))} \sum_{X \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}(u_1 X^{p^{m-1}+1} - u_2 X^{p+1} + vX)}.$$

  By following similar arguments as given for S_1 in the Case 1, we can easily show that $S_1 = 0$.

- Thus, ${}_c\Delta_{F_4}(a,b) = \frac{1}{p^n}(S_0 + S_1) = p$.

Conclusions

i. We compute the c-differential uniformity of four classes of permutation polynomials.

ii. In particular, our work adds to the very few known classes of PcN functions over binary fields.

iii. The used methods include discrete Fourier transforms, Weil sums and a very detailed analysis of those equations. The introduced techniques might be of interest on their own.

The preprint is available at `https://arxiv.org/abs/2212.01931v1`

Thank you for your attention!