The second-order zero differential spectra of some functions over finite fields

Kirpa Garg

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

Boolean Functions and their Applications (BFA)

Voss, Norway
September 03-08, 2023

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

Outline

- Notations and definitions
- Boomerang Connectivity Table (BCT)
- Feistel Boomerang Connectivity Table (FBCT)
- Second-order zero differential spectra
- Our results

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 let η be the quadratic character of $\mathbb{F}_q$ defined by

$$\eta(X) := \begin{cases} 1 & \text{if } X \text{ is square of an element of } \mathbb{F}_q^*, \\ -1 & \text{otherwise.} \end{cases}$$

- We shall use Tr to denote the trace function from $\mathbb{F}_{2^n} \to \mathbb{F}_2$, i.e., $\mathrm{Tr}(X) = \sum_{i=0}^{n-1} X^{2^i}$.

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.

Boomerang attack

- In 1999, Wagner[3] introduced a new attack on block ciphers, which is called the boomerang attack.
- The boomerang attack may be thought of as an extension to the differential attack.
- In Eurocrypt 2018, Cid et al.[4] introduced the notion of Boomerang Connectivity Table (BCT), to analyze the boomerang attack.

---

[3] D. Wagner, *The boomerang attack,* In: L. R. Knudsen (ed.) Fast Software Encryption-FSE 1999. LNCS 1636, Springer, Berlin, Heidelberg, pp. 156–170, 1999.

[4] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, *Boomerang connectivity table: a new cryptanalysis tool*. In: Nielsen J., Rijmen V. (eds.), Advances in Cryptology, EUROCRYPT 2018, LNCS 10821, Springer, Cham, pp. 683–714, 2018.

Boomerang Connectivity Table (BCT)

Definition (Cid et al., 2018)

For any $a, b \in \mathbb{F}_{2^n}$, the BCT entry of the invertible function f at point (a, b), denoted by $\mathcal{B}_f(a, b)$, is the number of solutions in $\mathbb{F}_{2^n}$ of the following equation

$$f^{-1}(f(x) + b) + f^{-1}(f(x + a) + b) = a$$

[5] C. Boura, A. Canteaut, *On the boomerang uniformity of cryptographic Sboxes*, IACR Trans. Symmetric Cryptol., vol. 2018, no. 3, 290–310, 2018.

Boomerang Connectivity Table (BCT)

Definition (Cid et al., 2018)

For any $a, b \in \mathbb{F}_{2^n}$, the BCT entry of the invertible function f at point (a, b), denoted by $\mathcal{B}_f(a, b)$, is the number of solutions in $\mathbb{F}_{2^n}$ of the following equation

$$f^{-1}(f(x) + b) + f^{-1}(f(x + a) + b) = a$$

To quantify the resistance of a function against the boomerang attack, Boura and Canteaut[5] introduced the concept of boomerang uniformity.

Boomerang Uniformity

The Boomerang uniformity of function f, denoted by Γ_f is given by:

$$\Gamma_f = \max\{\beta_f(a, b) | a, b \in \mathbb{F}_q^*\}.$$

[5] C. Boura, A. Canteaut, *On the boomerang uniformity of cryptographic Sboxes*, IACR Trans. Symmetric Cryptol., vol. 2018, no. 3, 290–310, 2018.

This definition is only valid for a Substitution Permutation Network (SPN) cipher.

What about Feistel ciphers?

Feistel Boomerang Connectivity Table

- Recently, in 2020, Boukerrou, Huynh, Lallemand, Mandal, Minier[6] extended this idea to Feistel ciphers.
- Feistel ciphers have the practical advantage that decryption is performed by executing the same function as for encryption, here the S-boxes may not be bijective.

[6] H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal and M. Minier, *On the Feistel counterpart of the boomerang connectivity table,* IACR Trans. Symmetric Cryptol. 1 (2020), 331–362.

Feistel Boomerang Connectivity Table (FBCT)

Definition (Boukerrou et al., 2020)

For any $a, b \in \mathbb{F}_{2^n}$, the FBCT entry of the function f at point (a, b), denoted by $FBCT_f(a, b)$, is number of solutions $X \in \mathbb{F}_{2^n}$ of the following equation

$$f(X + a + b) + f(X + b) + f(X + a) + f(X) = 0.$$

Feistel Boomerang Connectivity Table (FBCT)

Definition (Boukerrou et al., 2020)

For any $a, b \in \mathbb{F}_{2^n}$, the FBCT entry of the function f at point (a, b), denoted by $FBCT_f(a, b)$, is number of solutions $X \in \mathbb{F}_{2^n}$ of the following equation

$$f(X + a + b) + f(X + b) + f(X + a) + f(X) = 0.$$

Feistel Boomerang Uniformity

The F-Boomerang uniformity, denoted by β_f, is given by

$$\beta_f = \max_{a \neq 0, b \neq 0, a \neq b} FBCT_f(a, b).$$

Second-order zero differential uniformity

Second-order zero differential spectra

For any function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $a, b \in \mathbb{F}_{p^n}$, the second-order zero differential spectra of f with respect to a, b, denoted by $\nabla_f(a, b)$ is defined as

$$\#\{X \in \mathbb{F}_{p^n} : f(X + a + b) - f(X + b) - f(X + a) + f(X) = 0\}.$$

Second-order zero differential uniformity

The second-order zero differential uniformity of f, is given by

$$\nabla_f = \begin{cases} \max\{\nabla_f(a, b) : a \neq b, a, b \in \mathbb{F}_{2^n} \setminus \{0\}\} & \text{if } p = 2 \\ \max\{\nabla_f(a, b) : a, b \in \mathbb{F}_{p^n} \setminus \{0\}\} & \text{if } p > 2. \end{cases}$$

Properties of FBCT

- The entries of FBCT of f are the second-order zero differential spectra of f and the F-Boomerang uniformity is the second-order zero differential uniformity of f in even characteristic.
- All the non trivial second-order zero differential spectra of APN functions in even characteristic are 0.
- Thus any non-APN function has Feistel boomerang uniformity higher or equal to 4.

Our results

- We first considered a power function $F(X) = X^{2^{\frac{n+3}{2}}-1}$ over $\mathbb{F}_{2^n}$, a differentially 6-uniform[7] function, where n is odd and show that F attains the best possible value of FBCT, i.e. 4.

[7] C. Blondeau, L. Perrin, *More differentially 6-uniform power functions,* Des. Codes Cryptogr. 73 (2014), 487–505.

Our results

- We first considered a power function $F(X) = X^{2^{\frac{n+3}{2}}-1}$ over $\mathbb{F}_{2^n}$, a differentially 6-uniform[7] function, where n is odd and show that F attains the best possible value of FBCT, i.e. 4.

Theorem 1

Let $F(X) = X^d$ be a power function of $\mathbb{F}_{2^n}$, where $d = 2^{\frac{n+3}{2}} - 1$ and n is odd. Let $s = \frac{n+3}{2}$, $A = \dfrac{a^{2^s}b + ab^{2^s}}{ab(a+b)}$, $a_0 = A^{2^s+2} + a^4b^4 + a^4 + b^4$, $w_1 = \frac{a_0}{b^2(a+b)^2}, w_2 = \frac{a_0}{a^2(a+b)^2}, w_3 = \frac{a_0}{a^2b^2}$. Then for $a, b \in \mathbb{F}_{2^n}$,

$$\nabla_F(a,b) = \begin{cases} 4 & \text{if } \mathrm{Tr}(w_1) = \mathrm{Tr}(w_2) = \mathrm{Tr}(w_3) = 0 \\ 2^n & \text{if } ab = 0 \text{ or } a = b \\ 0 & \text{otherwise.} \end{cases} \quad (2.1)$$

Thus, F is second-order zero differential 4-uniform (that is, the Feistel boomerang uniformity of F is 4).

[7] C. Blondeau, L. Perrin, *More differentially 6-uniform power functions,* Des. Codes Cryptogr. 73 (2014), 487–505.

Idea of the proof

- For $a, b \in \mathbb{F}_{2^n}$, we consider the equation:

$$F(X + a + b) + F(X + b) + F(X + a) + F(X) = 0.$$

Idea of the proof

- For $a, b \in \mathbb{F}_{2^n}$, we consider the equation:

$$F(X + a + b) + F(X + b) + F(X + a) + F(X) = 0.$$

- If $ab = 0$ and $a = b$, then $\nabla_F(a, b) = 2^n$.

Idea of the proof

- For $a, b \in \mathbb{F}_{2^n}$, we consider the equation:

$$F(X + a + b) + F(X + b) + F(X + a) + F(X) = 0.$$

- If $ab = 0$ and $a = b$, then $\nabla_F(a, b) = 2^n$.
- Let $ab \neq 0$ and $a \neq b$, then $X \in \{0, a, b, a + b\}$ is a solution if $a^{2^{\frac{n+3}{2}}-2} = b^{2^{\frac{n+3}{2}}-2}$, which is not possible.

Idea of the proof

- For $a, b \in \mathbb{F}_{2^n}$, we consider the equation:

$$F(X+a+b)+F(X+b)+F(X+a)+F(X)=0.$$

- If $ab=0$ and $a=b$, then $\nabla_F(a,b)=2^n$.
- Let $ab \neq 0$ and $a \neq b$, then $X \in \{0,a,b,a+b\}$ is a solution if $a^{2^{\frac{n+3}{2}}-2}=b^{2^{\frac{n+3}{2}}-2}$, which is not possible.
- For $X \notin \{0,a,b,a+b\}$, we simplify the above equation and get

$$X^{2^s}+AX^2+BX=0,$$

where $s=\frac{n+3}{2}$, $A=\dfrac{a^{2^s}b+ab^{2^s}}{ab(a+b)}$ and $B=\dfrac{a^{2^s}b^2+a^2b^{2^s}}{ab(a+b)}$.

Continued...

We then have two cases.

Case 1. If $A = 0$, then $a^{2^s-1} = b^{2^s-1}$ and after some computations we reduce $X^{2^s} + AX^2 + BX = 0$ to the linearized polynomial

$$X(X^{2^s-1} + b^{2^s-1}) = 0.$$

Notice that, $X^{2^s-1} = b^{2^s-1}$ can have either seven solutions or one solution. Among these possible eight solutions (including $X = 0$) of the linearized polynomial $X(X^{2^s-1} + b^{2^s-1}) = 0$, the four solutions come from the set $\{0, a, b, a + b\}$, which we have already discarded. Hence, for $A = 0$, we would have at most four solutions.

Continued...

Case 2. Next, we have $A \neq 0$. Then we can reduce $X^{2^s} + AX^2 + BX = 0$ using some computations to the following equation

$$X^8 + A^{2^s}(AX+B)^2X^2 + B^{2^s}(AX+B)X = 0.$$

One can computationally verify that each of the member of the set $\{0, a, b, a+b\}$ is a solution of the above equation which is not true and will further reduce it to a degree four equation given below:

$$X^4 + (a^2+b^2+ab)X^2 + ab(a+b)X + A^{2^s+2} + a^4 + b^4 + (ab)^4 = 0.$$

We analyze the degree four equation via a Lemma given by Leonard and Williams[8] and show that the above four degree equation has at most four solutions $X \in \mathbb{F}_{2^n}$.

[8] P. A. Leonard, K. S. Williams, *Quartics over* $GF(2^n)$. Proc. Amer. Math. Soc. 36:2 (1972), 347–350.

Continued...

Lemma

Let $f(x) = x^4 + a_2x^2 + a_1x + a_0 \in \mathbb{F}_{2^n}[x]$ with $a_0a_1 \neq 0$ and the companion cubic $g(y) = y^3 + a_2y + a_1$ with the roots r_1, r_2, r_3. When the roots exist in $\mathbb{F}_{2^n}$, we set $w_i = a_0r_i^2/a_1^2$. We write a polynomial h as $h = (1, 2, 3, \ldots)$ over some field to mean that it decomposes as a product of degree $1, 2, 3, \ldots$, over that field. Then the factorization of $f(x)$ over $\mathbb{F}_{2^n}$ is characterized as follows:

(i) $f = (1, 1, 1, 1) \Leftrightarrow g = (1, 1, 1)$ and $\mathrm{Tr}\,(w_1) = \mathrm{Tr}\,(w_2) = \mathrm{Tr}\,(w_3) = 0$;

(ii) $f = (2, 2) \Leftrightarrow g = (1, 1, 1)$ and $\mathrm{Tr}\,(w_1) = 0, \mathrm{Tr}\,(w_2) = \mathrm{Tr}\,(w_3) = 1$;

(iii) $f = (1, 3) \Leftrightarrow g = (3)$;

(iv) $f = (1, 1, 2) \Leftrightarrow g = (1, 2)$ and $\mathrm{Tr}\,(w_1) = 0$;

(v) $f = (4) \Leftrightarrow g = (1, 2)$ and $\mathrm{Tr}\,(w_1) = 1$.

Our results

Our next considered function was introduced by Tan, Qu, Tan and Li[9] who showed that when n is even, the permutation polynomial $F(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ is differentially 4-uniform. Further, Hasan, Pal and Stănică[10] studied the c-differential and boomerang uniformities of $F(X)$. In the next theorem, we studied FBCT of this function.

[9] Y. Tan, L. Qu, C. H. Tan, C. Li, *New families of differentially 4-uniform permutations over* $\mathbb{F}_{2^{2k}}$, in Sequences and Their Applications-SETA (Lecture Notes in Computer Science), vol. 7280, T. Helleseth and J. Jedwab, Eds. Heidelberg, Germany: Springer, 2012, pp. 25–39.

[10] S. U. Hasan, M. Pal, P. Stănică, *The c-Differential Uniformity and Boomerang Uniformity of Two Classes of Permutation Polynomials*, IEEE Trans. Inf. Theory 68 (2022), 679–691.

Theorem 2

Let $F(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ be a function over $\mathbb{F}_{2^n}$, where n is even. Then for $a, b \in \mathbb{F}_{2^n}$, then $\nabla_F(a,b) =$

$$\begin{cases} 4 & \text{if } \mathrm{Tr}(b^{-1}) = \mathrm{Tr}(b^{-1}\omega) = \mathrm{Tr}(b^{-1}\omega^2) = 0, \mathrm{Tr}(w_4) = \mathrm{Tr}(b^3) = 1, \\ & \text{or } \mathrm{Tr}(w_4) = \mathrm{Tr}(b^3) = 0 \text{ and } \mathrm{Tr}(b^{-1}) = 1, \\ & \text{or } \mathrm{Tr}(w_4) = \mathrm{Tr}(b^3) = 0 \text{ and } \mathrm{Tr}(b^{-1}\omega) = 1, \\ & \text{or } \mathrm{Tr}(w_4) = \mathrm{Tr}(b^3) = 0 \text{ and } \mathrm{Tr}(b^{-1}\omega^2) = 1, \\ & \text{or } \mathrm{Tr}(w_1) = \mathrm{Tr}(w_2) = \mathrm{Tr}(w_3) = \mathrm{Tr}\left(\frac{ab(a+b)}{a^2+b^2+ab(a+b)+ab+1}\right) = 1, \\ 8 & \text{if } \mathrm{Tr}(w_4) = \mathrm{Tr}(b^{-1}) = \mathrm{Tr}(b^{-1}\omega) = \mathrm{Tr}(b^{-1}\omega^2) = 0, \mathrm{Tr}(b^3) = 1, \\ 2^n & \text{if } ab = 0 \text{ or } a = b, \\ 0 & \text{otherwise,} \end{cases}$$

where ω is a cube roots of unity, $w_1 = \frac{a}{b(a+b)}, w_2 = \frac{b}{a(a+b)}, w_3 = \frac{a+b}{ab}$ and $w_4 = \frac{b^3}{b^3+1}$. Moreover, F is second-order zero differential 8-uniform (that is, the Feistel boomerang uniformity of F is 8).

Second order differential spectra (odd characteristic)

Li, Yue and Tang[11] further studied the second-order zero differential spectra of APN functions and those with low diferential uniformity in odd characteristic.

p	d	condition	Δ_F	∇_F
$p > 3$	3	any	2	1
$p = 3$	$3^n - 3$	$n > 1$ is odd	2	2
$p > 2$	$p^n - 2$	$p^n \equiv 2 \pmod 3$	2	1
$p > 3$	$p^m + 2$	$n = 2m$, $p^m \equiv 1 \pmod 3$	2	1
$p = 3$	$3^n - 2$	any	3	3
p	$p^n - 2$	$p^n \equiv 1 \pmod 3$	3	3

Table: Second-order differential uniformity (odd characteristic)

[11] X. Li, Q. Yue, D. Tang, *The second-order zero differential spectra of almost perfect nonlinear functions and the inverse function in odd characteristic*, Cryptogr. Commun. 14:3 (2022), 653–662.

Second order differential spectra (odd characteristic)

We further extend their work by investigating the second-order zero differential spectra of two power functions, whose differential uniformities are studied by Helleseth, Rong and Sandberg.[12]

- $F(X) = X^d$, where $d = \frac{2p^n-1}{3}$ over $\mathbb{F}_{p^n}$, for $p^n \equiv 2 \pmod 3$ is an APN function.
- $F(X) = X^d$, where $d = \frac{p^k+1}{2}$, has differential uniformity at most $\gcd(\frac{p^k-1}{2}, p^{2n}-1)$.

[12] T. Helleseth, C. Rong, D. Sandberg *New families of almost perfect nonlinear power mappings,* IEEE Trans. Inf. Theory 45:2 (1999), 475–485.

Our results

Theorem 3

Let $F(X) = X^d$ be a function of $\mathbb{F}_{p^n}$, where $d = \frac{2p^n-1}{3}$, $p^n \equiv 2 \pmod 3$. Then for $a, b \in \mathbb{F}_{p^n}$,

$$\nabla_F(a,b) = \begin{cases} 1 & \text{if } ab \neq 0 \\ p^n & \text{if } ab = 0. \end{cases}$$

Moreover, F is second-order zero differential 1-uniform.

Our results

Theorem 4

Let $F(X) = X^d$ be a power function of $\mathbb{F}_{p^n}$, where $d = \frac{p^k+1}{2}$, and $\gcd(k, 2n) = 1$. Let $p > 3$. Then for $a, b \in \mathbb{F}_{p^n}$,

$$\nabla_F(a,b) = \begin{cases} 0 & \text{if } ab \neq 0, \text{and } \eta(D) = -1 \\ 1 & \text{if } ab \neq 0, \text{and } \eta(D) = 0 \\ \frac{p-3}{2} & \text{if } ab \neq 0, \text{and } \eta(D) = 1 \\ p^n & \text{if } ab = 0 \end{cases}$$

where $D = \frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}$, u is a primitive $(p-1)$-th root of unity in $\mathbb{F}^*_{p^{2n}}$. Moreover, F is second-order zero differential $\frac{p-3}{2}$-uniform.

Conclusion

p	$F(X)$	condition	Δ_F	∇_F
2	$X^{2^{\frac{n+3}{2}}-1}$	n is odd	6	4
2	$X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$	n is even	4	8
$p > 3$	$X^{\frac{p^k+1}{2}}$	$\gcd(2n, k) = 1$	$\leq \gcd(\frac{p^k-1}{2}, p^{2n} - 1)$	$\frac{p-3}{2}$
$p = 3$	$X^{\frac{p^n-1}{2}+2}$	n is odd	4	3

Table: Second-order differential uniformity for functions over finite fields

Conclusion

1. We compute the second-order zero differential spectra of some APN power functions and functions with low differential uniformity.

2. It is worthwhile to look into more functions with low differential uniformity and investigate their second-order zero differential spectrum.

Thank you for your attention!