Differential equivalence of APN functions: results and open problems

Anastasiya Gorodilova

Sobolev Institute of Mathematics,
Novosibirsk State University

3d International Workshop on
Boolean Functions and Their Applications

Loen, Norway
18 June 2018

The differential equivalence of APN functions

The associated Boolean function

Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to itself.

Definition 1 ([1])

The associated Boolean function $\gamma_F(a, b)$ *in* $2n$ *variables of* F *is defined as follows: it takes value* 1 *iff* $a \neq \mathbf{0}$ *and* $F(x) + F(x + a) = b$ *has solutions.*

Why this function is of interest?

- F is almost perfect nonlinear (APN) iff $\mathrm{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$;
- F is almost bent (AB) iff γ is a bent function.

[1] Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15, 125–156 (1998).

The differential equivalence: definition

We introduce the following notation.

Definition 2 ([2])

Two functions F, G from $\mathbb{F}_2^n$ to itself are called differentially equivalent if $\gamma_F = \gamma_G$. Denote the differential equivalence class of F by $\mathcal{DE}_F$.

Further we will focus only on APN functions.

Proposition 1

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function, $n > 1$. Then $F_{c,d}(x) = F(x + c) + d$ is differentially equivalent to F for all $c, d \in \mathbb{F}_2^n$ and all the functions $F_{c,d}$ are pairwise distinct.

We call functions $F_{c,d}$ as trivially differentially equivalent functions to F.

[2] Gorodilova A.A.: On a remarkable property of APN Gold functions // Cryptology ePrint Archive, Report 2016/286 (2016).

General open problem on the differential equivalence

Problem 1 ([3])

Is it possible to find a systematic way, given an APN function F, to build another function G such that $\gamma_F = \gamma_G$?

Problem 1 (modified)

- *Is it possible to describe the differential equivalence class of a given APN function?*
- *Do there exist functions which are not trivially differentially equivalent to a given APN function?*

[3] Carlet C.: Open Questions on Nonlinearity and on APN Functions. Arithmetic of Finite Fields, Lecture Notes in Computer Science. 9061, 83–107 (2015).

EA-invariant

Definition 3

F and G are called extended affine equivalent (EA-equivalent) if $G = A' \circ F \circ A'' + A$, where A', A'' are affine permutations and A is affine.

Proposition 2

Let F, G be EA-equivalent functions. Then $|\mathcal{DE}_F| = |\mathcal{DE}_G|$.

So, we can study the differential equivalence classes of EA-representatives.

Open problem on CCZ-invariant

Definition 4 ([1])

Two functions F and G are said to be Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent) if their graphs $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ and $\mathcal{G}_G = \{(x, G(x)) : x \in \mathbb{F}_2^n\}$ are affine equivalent.

Problem 2

Is the cardinality of the differential equivalence class of an APN function a CCZ-equivalence invariant?

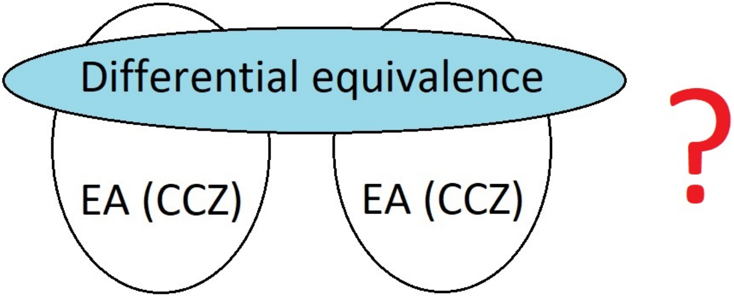
As stated in [4] the answer to this question is positive.

[4] Canteaut A., Boura C., Jean J. and Suder V.: On Sboxes sharing the same DDT. Abstracts of BFA-2018.

Open problem on connection between the differential equivalence and EA- (CCZ-) equivalence

Problem 3

Do there exist two differentially equivalent APN functions which are not EA- (CCZ-) equivalent?



By now such two APN functions have not been found.

The differential equivalence of quadratic APN functions

Quadratic APN functions

Definition 5

F is quadratic if degree of its algebraic normal form is 2.

Let

$$B_a(F) = \{F(x) + F(x+a) : \ x \in \mathbb{F}_2^n\}$$

for a vector $a \in \mathbb{F}_2^n$.

- F is APN iff $|B_a(F)| = 2^{n-1}$ for all nonzero a.
- if F is quadratic, then $B_a(F)$ is an affine hyperplane for all nonzero a.

Quadratic APN functions and crooked functions

In [5] definition of the crooked functions was introduced and it was generalized to the following:

Definition 6

F is called generalized crooked if $B_a(F)$ is an affine hyperplane for all $a \neq \mathbf{0}$.

Problem 4 ([6])

Are all crooked functions quadratic?

If "yes", then there are no nonquadratic functions differentially equivalent to a given quadratic APN function.

[5] Bending T. D., Fon-Der-Flaass D.: Crooked functions, bent functions, and distance regular graphs. Electron. J. Combin. 5 (1) (1998) R34.

[6] Kyureghyan G.: Crooked maps in $\mathbb{F}_2^n$. Finite Fields Their Appl. 13(3), 713–726 (2007)

Open problem on adding affine functions

There always exist 2^{2n} trivially differentially equivalent functions to a given APN function. Do there exist other?

- If F is quadratic, then all these 2^{2n} trivial functions are obtained by adding to F affine functions $A_{c,d}(x) = F(x) + F(x+c) + d$.

Problem 5

What affine functions do not change the associated Boolean function γ_F when adding to a quadratic APN function F?

APN Gold functions

Theorem 1

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Gold function $F(x) = x^{2^k+1}$, where $\gcd(k, n) = 1$. Then the following statements hold:

- *if $n = 4t$ for some t and $k = n/2 \pm 1$, then there exist exactly $2^{2n+n/2}$ distinct affine functions A such that F and $F + A$ are differentially equivalent; all of them are of the form $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k} + \delta x^{2^j}$, where $\alpha, \lambda, \delta \in \mathbb{F}_{2^n}$, $\delta = \delta^{2^{n/2}}$, and $j = k - 1$ for $k = n/2 + 1$ and $j = n - 1$ for $k = n/2 - 1$;*
- *otherwise there exist exactly 2^{2n} distinct affine functions A such that F and $F + A$ are differentially equivalent; all of them are of the form $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k}$, where $\alpha, \lambda \in \mathbb{F}_{2^n}$.*

Total numbers of affine functions A on $\mathbb{F}_2^n$ such that F and $F+A$ are differentially equivalent

n	# EA classes	# affine functions A: $F+A \in \mathcal{DE}_F$
2	1	2^4
3	1	2^6
4	1 [7]	2^{10}
5	2 [7]	for all 2 classes: 2^{10}
6	13 [8,9]	for 12 classes: 2^{12}; for 1 class: 2^{13}
7	$\geq$ 487 [10]	for all known 487 classes: 2^{14}
8	$\geq$ 8179 [10]	for 1 class from known 8179: 2^{20} for other 8178 classes: 2^{16}

[7] Brinkman M., Leander G.: On the classification of APN functions up to dimension five. Proc. of the International Workshop on Coding and Cryptography 2007 dedicated to the memory of Hans Dobbertin. Versailles, France, 39–48 (2007).
[8] Browning K. A., Dillon J. F., Kibler R. E., McQuistan M. T.: APN Polynomials and Related Codes. Journal of Combinatorics, Information and System Science, Special Issue in honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday, vol. 34, no. 1-4, pp. 135–159 (2009).
[9] Edel Y.: Quadratic APN functions as subspaces of alternating bilinear forms. Contact Forum Coding Theory and Cryptography III, Belgium (2009), pp. 11–24 (2011).
[10] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. 73, 587–600 (2014).

Properties of the associated Boolean function of a quadratic APN function

The associated function of a quadratic APN function

Let F be a quadratic APN function on $\mathbb{F}_2^n$.

Then γ_F is of the form

$$\gamma_F(a,b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1,$$

where $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$ are uniquely defined from

$$B_a(F) = \{y \in \mathbb{F}_2^n : \ \Phi_F(a) \cdot y = \varphi_F(a)\}$$

for all $a \neq \mathbf{0}$ and $\Phi_F(\mathbf{0}) = \mathbf{0}$, $\varphi_F(\mathbf{0}) = 1$.

Note that $B_a(F)$ is a linear subspace iff $\varphi_F(a) = 0$.

Φ_F — what is this?

Let us denote $A_v^F = \{a \in \mathbb{F}_2^n : \ \Phi_F(a) = v\}$ for $v \in \mathbb{F}_2^n$.

Proposition 3 ([1])

Let F be a quadratic APN function in n variables, n is odd. Then Φ_F is a permutation; therefore, γ_F is a bent function of Maiorana–McFarland type.

Thus, when n is odd, all A_v^F, $v \in \mathbb{F}_2^n$, are pairwise distinct and each of them consists of one element. We prove the following theorem for even n.

Theorem 2

Let F be a quadratic APN function in n variables, n is even. Then $A_v^F \cup \{\mathbf{0}\}$ is a linear subspace of even dimension for any $v \in \mathbb{F}_2^n$.

Φ_F — what is this?

Value distribution of Φ_F for even n.

n	# EA classes		$\#\{v \in \mathbb{F}_2^n : \lvert A_v^F \rvert = k\}$, $k = 3$	$k = 15$
4	1		5	–
6	13	for 12 classes:	21	–
		for 1 class:	16	1
8	≥ 8179	for 7680 classes:	85	–
		for 487 classes:	80	1
		for 12 classes:	75	2

Φ_F — what is this?

Theorem 3

Let F be a quadratic APN function in n variables, n is odd, $n \geq 3$. Then $\deg(\Phi_F) \leq n-2$.

The bound of theorem 4 is tight for all known quadratic APN functions in not more than 8 variables (including also even numbers).

Moreover, it holds that all their component functions are of degree $n-2$.

For example, for an APN Gold function we have $\Phi_F(a) = (a^{2^k+1})^{-1}$, $\Phi_F(\mathbf{0}) = \mathbf{0}$, and $\deg(\Phi_F) = n-2$.

The linear spectrum of quadratic APN functions

The linear spectrum: definition

Let $F, L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where F is a quadratic APN function and L is linear.

Then $B_a(F+L)$ equals $B_a(F)$ or $\mathbb{F}_2^n \setminus B_a(F)$ for all $a \in \mathbb{F}_2^n$.

Let us denote $k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : \; B_a(F) = B_a(F+L)\}|$.

Definition 7

The linear spectrum of a quadratic APN function F in n variables is the vector $\Lambda^F = (\lambda_0^F, \ldots, \lambda_{2^n-1}^F)$, where λ_k^F is the number of linear functions L such that $k_L^F = k$.

It is easy to see that $\sum_{k=0}^{2^n-1} \lambda_k^F = 2^{n^2}$.

The linear spectrum: invariant

Proposition 4

The linear spectrum of a quadratic APN function is

- *a differential equivalence invariant;*
- *a EA-equivalence invariant.*

Let F be a quadratic APN function in n variables. Then

$n = 3$	$\Lambda^F = (0, 56, 0, 280, 0, 168, 0, 8)$
$n = 4$	$\Lambda^F = (0, 0, 0, 0, 0, 15552, 0, 25920, 0, 17280, 0, 5760, 0, 960, 0, 64)$
$n = 5$	2 classes with distinct spectra
$n = 6$	13 classes with pairwise distinct spectra except one pair having equal spectrum

The linear spectrum: zero values

Theorem 4

Let F be a quadratic APN function in n variables, $n > 1$. Then the following statements hold:

- $\lambda_k^F = 0$ *for all even* k, $0 \leq k \leq 2^n - 2$;
- *if* n *is even, then* $\lambda_k^F = 0$ *for all* $0 \leq k < (2^n - 1)/3$.

Let F be a quadratic APN function in n variables. Then

$n = 3$	$\Lambda^F = (0,\ 56,\ 0,\ 280,\ 0,\ 168,\ 0,\ 8)$
$n = 4$	$\Lambda^F = (0,\ 0,\ 0,\ 0,\ 0,\ 15552,\ 0,\ 25920,\ 0,\ 17280,\ 0,\ 5760,\ 0,\ 960,\ 0,\ 64)$
$n = 5$	2 classes with distinct spectra
$n = 6$	13 classes with pairwise distinct spectra except one pair having equal spectra

Differential equivalent functions in small number of variables

Based on results about the linear spectra, properties of γ_F, we computationally obtained a classification of differentially nonequivalent quadratic APN functions up to 6 variables.

Theorem 5

Let F be a quadratic APN function in n variables, $n = 2, 3, 4, 5, 6$. Then each differentially equivalent to F quadratic APN function G is represented as follows: $G = F + A$, where A is an affine function. Moreover, the number K of such functions A equals 2^{2n} for all functions except functions from two EA-equivalence classes with the following representatives:

- *$n = 4$: APN Gold function $F(x) = x^3$, $K = 2^{10}$;*
- *$n = 6$: APN function*
  $F(x) = \alpha^7 x^3 + x^5 + \alpha^3 x^9 + \alpha^4 x^{10} + x^{17} + \alpha^6 x^{18}$, $K = 2^{13}$.

Thank you for your attention!