Constructing APN Functions

Y. Yu,
L. Perrin

Constructing More Quadratic APN Functions with the QAM Method

Yuyin Yu[1] and Léo Perrin[2]

1, Guangzhou University, Guangzhou, China
2, Inria, Paris, France

September, 2021

Contents

Motivation

- In 2009, Browning and Dillon found one APN permutation in dimension 6, which was the first APN permutation in even dimensions. Their idea was to construct new APN functions and to check whether they are equivalent to permutations.
- So, constructing more APN functions may help to find new APN permutations in even dimensions .

Motivation

- In 2009, Browning and Dillon found one APN permutation in dimension 6, which was the first APN permutation in even dimensions. Their idea was to construct new APN functions and to check whether they are equivalent to permutations.
- So, constructing more APN functions may help to find new APN permutations in even dimensions .

We focus on constructing more quadratic APN functions in dimension 8.

- Edel and Pott listed 23 CCZ-inequivalent APN functions in dimension 8 (2009).
- Weng et al. and Yu et al. extended the length of the list to 8190 (2013).
- Beierle and Leander found another 12923 new quadratic APN functions (2020).

Our Contributions

- We present another 5412 new quadratic APN functions in dimension 8.
- We guess that the total number of CCZ-inequivalent APN functions in dimension 8 may exceed 50000.
- We guess that the full list of quadratic APN functions could be obtained by modifying the last two columns (and rows) of the corresponding QAM of x^3.

$$H_8 = \begin{pmatrix} 0 & g^{34} & g^{81} & g^{83} & g^{170} & g^{106} & \mathbf{x_{13}} & \mathbf{x_7} \\ g^{34} & 0 & g^{68} & g^{162} & g^{166} & g^{85} & \mathbf{x_{12}} & \mathbf{x_6} \\ g^{81} & g^{68} & 0 & g^{136} & g^{69} & g^{77} & \mathbf{x_{11}} & \mathbf{x_5} \\ g^{83} & g^{162} & g^{136} & 0 & g^{17} & g^{138} & \mathbf{x_{10}} & \mathbf{x_4} \\ g^{170} & g^{166} & g^{69} & g^{17} & 0 & g^{34} & \mathbf{x_9} & \mathbf{x_3} \\ g^{106} & g^{85} & g^{77} & g^{138} & g^{34} & 0 & \mathbf{x_8} & \mathbf{x_2} \\ \mathbf{x_{13}} & \mathbf{x_{12}} & \mathbf{x_{11}} & \mathbf{x_{10}} & \mathbf{x_9} & \mathbf{x_8} & 0 & \mathbf{x_1} \\ \mathbf{x_7} & \mathbf{x_6} & \mathbf{x_5} & \mathbf{x_4} & \mathbf{x_3} & \mathbf{x_2} & \mathbf{x_1} & 0 \end{pmatrix}.$$

APN & CCZ

Definition (APN)

A mapping $F : GF(2^n) \to GF(2^n)$ *is an APN (Almost perfect nonlinear) function, if the equation* $F(x+a) + F(x) = b$ *has at most two solutions for any* $a \in GF(2^n)^\star$ *and* $b \in GF(2^n)$*.*

Definition (CCZ-equivalence)

Suppose F *and* T *are two functions from* $GF(2^n)$ *to* $GF(2^n)$*, then* F *and* T *are* ***CCZ-equivalent*** *(Carlet-Charpin-Zinoviev equivalent) if there is an affine permutation which maps* G_F *to* G_T*, where* $G_F = \{(x, F(x)) : x \in GF(2^n)\}$ *is the graph of* F*, and* G_T *is the graph of* T*.*

One To One Correspondence

Definition (quadratic homogeneous functions)

Quadratic functions without linear or constant terms are called ***quadratic homogeneous functions****.*

$$F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in GF(2^n)[x].$$

Definition (QAM)

Let $H = (h_{u,v})_{n \times n}$ be an $n \times n$ matrix defined on $GF(2^n)$. the matrix H is called a ***QAM*** *(quadratic APN matrix) if*
1) H is symmetric and the elements in its main diagonal are all zeros.
2) Every nonzero linear combination of the n rows (or "columns" since H is symmetric) of H has rank $n-1$.

One To One Correspondence

Theorem

There exists a one to one correspondence between quadratic homogeneous APN functions and QAMs.

[1]

[1] Y. Yu, M. Wang, Y. Li, A matrix approach for constructing quadratic APN functions. Designs Codes and Cryptography 73, p.587-600 (2014).

How to Partition APN functions

- We could obtain 6794 APN functions by modifying a very small part (less than 0.5%) of the last two columns of the corresponding QAM of x^3.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language[J]. Journal of Symbolic Computation, 24(3-4) p. 235-265 (1997).

How to Partition APN functions

- We could obtain 6794 APN functions by modifying a very small part (less than 0.5%) of the last two columns of the corresponding QAM of x^3.
- We could patition them into different CCZ-inequivalence classes by coding theory [2]. However, this method becomes very slow when we need to check a large number of functions.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language[J]. Journal of Symbolic Computation, 24(3-4) p. 235-265 (1997).

How to Partition APN functions

Y. Yu,
L. Perrin

Definition

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a quadratic APN function, and let* $x \cdot y$ *denote a scalar product of* x *and* y *(where* x *and* y *are in* $\mathbb{F}_{2^n}$*). Then the ortho-derivative of* F *is the unique function* $\pi_F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *such that* $\pi_F(0) = 0$, $\pi_F(a) \neq 0$ *if* $a \neq 0$, *and such that*

$$\pi_F(a) \cdot \big(F(x+a) + F(x) + F(a) + F(0)\big) = 0$$

for all $a \in \mathbb{F}_{2^n}^*$ *and all* $x \in \mathbb{F}_{2^n}$.

How to Partition APN functions

- If two quadratic functions are EA-equivalent, then their ortho-derivatives are affine-equivalent. As a consequence, they need to have identical differential and extended Walsh spectra [3].

[3] A. Canteaut, A. Couvreur, L. Perrin, Recovering or Testing Extended-Affine Equivalence, https://eprint.iacr.org/2021/225.

[4] S. Yoshiara, Equivalences of quadratic APN functions. Journal of Algebraic Combinatorics, 35, p.461-475 (2011).

How to Partition APN functions

- If two quadratic functions are EA-equivalent, then their ortho-derivatives are affine-equivalent. As a consequence, they need to have identical differential and extended Walsh spectra [3].

- Two quadratic APN functions are EA-equivalent, if and only if they are CCZ-equivalent [4].

---

[3] A. Canteaut, A. Couvreur, L. Perrin, Recovering or Testing Extended-Affine Equivalence, https://eprint.iacr.org/2021/225.

[4] S. Yoshiara, Equivalences of quadratic APN functions. Journal of Algebraic Combinatorics, 35, p.461-475 (2011).

How to Partition APN functions

$$\Sigma_4^F(0) = \left\{ \sum_{i=0}^{3} F(x_i) : \{x_0, ..., x_3\} \in (\mathbb{F}_{2^n})^4, \text{ and } \sum_{i=0}^{3} x_i = 0 \right\}$$

The multisets $\Sigma_4^F(0)$ is an EA-class invariant [5].

[5] N. Kaleyski, Deciding EA-equivalence via invariants. Cryptography and Communications. 2021 Jul 27:1-20.

How to Partition APN functions

$$\Sigma_4^F(0) = \left\{ \sum_{i=0}^{3} F(x_i) : \{x_0, ..., x_3\} \in (\mathbb{F}_{2^n})^4, \text{ and } \sum_{i=0}^{3} x_i = 0 \right\}$$

The multisets $\Sigma_4^F(0)$ is an EA-class invariant [5].

Evaluating this invariant on our full set of function is quite practical, and 4655 distinct values were found. It also has the significant advantage over the ortho-derivative that it does not require the function investigated to be both quadratic and APN.

[5] N. Kaleyski, Deciding EA-equivalence via invariants. Cryptography and Communications. 2021 Jul 27:1-20.

How to Get the Conjectures

(1) In dimension 8, we can still construct a quadratic APN function every 24 hours with the QAM method, and there is an about 79% probability that it is new compared to all known ones.

How to Get the Conjectures

(1) In dimension 8, we can still construct a quadratic APN function every 24 hours with the QAM method, and there is an about 79% probability that it is new compared to all known ones.

(2) In dimension 7, when 230 (47%$=\frac{230}{488}$ of the total number) CCZ-inequivalent quadratic APN functions have been found, there is an about 79% probability that the next APN function constructed by the QAM method is new (i.e. not among the first 230).

How to Get the Conjectures

(1) In dimension 8, we can still construct a quadratic APN function every 24 hours with the QAM method, and there is an about 79% probability that it is new compared to all known ones.

(2) In dimension 7, when 230 (47%$=\frac{230}{488}$ of the total number) CCZ-inequivalent quadratic APN functions have been found, there is an about 79% probability that the next APN function constructed by the QAM method is new (i.e. not among the first 230).

(3) In dimension 6, when 6 (46%$=\frac{6}{13}$ of the total number) CCZ-inequivalent quadratic APN functions have been traversed, there is an about 75% probability that the next APN function constructed by the QAM method is not among the first 6 found.

How to Get the Conjectures

(1) In dimension 8, we can still construct a quadratic APN function every 24 hours with the QAM method, and there is an about 79% probability that it is new compared to all known ones.

(2) In dimension 7, when 230 (47%$=\frac{230}{488}$ of the total number) CCZ-inequivalent quadratic APN functions have been found, there is an about 79% probability that the next APN function constructed by the QAM method is new (i.e. not among the first 230).

(3) In dimension 6, when 6 (46%$=\frac{6}{13}$ of the total number) CCZ-inequivalent quadratic APN functions have been traversed, there is an about 75% probability that the next APN function constructed by the QAM method is not among the first 6 found.

Based on the above facts, we guess that the total number of CCZ-inequivalent quadratic APN functions in dimension 8 is at least twice the number of the known ones.

How to Get the Conjectures

(1) In dimension 6, we had to generate more than 200 (about 16×13) quadratic APN functions to obtain the full list of quadratic APN functions.

(2) In dimension 7, we had to generate more than 3000 (about 8×488) quadratic APN functions to obtain the full list of quadratic APN functions.

How to Get the Conjectures

(1) In dimension 6, we had to generate more than 200 (about 16×13) quadratic APN functions to obtain the full list of quadratic APN functions.

(2) In dimension 7, we had to generate more than 3000 (about 8×488) quadratic APN functions to obtain the full list of quadratic APN functions.

In dimension 8, we may need to generate more than 200000 (4×50000) quadratic APN functions in order to get the complete list. we can construct at least 2000000 quadratic APN functions after traversing x_1, x_2, …, x_{12} and x_{13} of H_8.

Thanks

The list of quadratic APN functions can be found at
`https://github.com/lpp-crypto/sboxU`

Yuyin Yu (yuyuyin@163.com)
Léo Perrin (leo.perrin@inria.fr)