Constructing More Quadratic APN Functions with the QAM Method

Yuyin Yu* and Léo Perrin**

*School of Mathematics and Information Sciences, Guangzhou University, Guangzhou 510006, China
**Inria, Paris, France

Abstract

We found 5412 new quadartic APN on $\mathbb{F}_{2^8}$ with the QAM method, thus bringing the number of known CCZ-inequivalent APN functions on $\mathbb{F}_{2^8}$ to 26525. Unfortunately, none of these new functions are CCZ-equivalent to permutations. A (to the best of our knowledge) complete list of known quadratic APN functions, including our new ones, has been pushed to `sboxU` for ease of study by others.

In this paper, we recall how to construct new QAMs from a known one, and present how used the ortho-derivative method to figure out which of our new functions fall into different CCZ-classes. Based on these results and on others on smaller fields, we make to conjectures: that the full list of quadratic APN functions on $\mathbb{F}_{2^8}$ could be obtained using the QAM approached (provided enormous computing power), and that the total number of CCZ-inequivalent APN functions may overcome 50000.

1 Introduction

Browning and Dillon [3] found the first APN permutation in dimension 6. Their idea is to check the CCZ-equivalent [5] classes of a quadratic APN function. If an APN function is CCZ-equivalent to a permutation, then they can find an APN permutation. Browning and Dillon provided a method to find APN permutations. Firstly, finding more APN functions, secondly, checking whether there exist permutations in their CCZ-equivalent classes. Thus, we are motivated to find more new APN functions. In this paper, we focus on how to construct quadratic APN functions in small dimensions, especially in dimension 8. Edel and Pott [7] listed 23 CCZ-inequivalent APN functions on $\mathbb{F}_{2^8}$. Weng et al.[9] and Yu et al.[11] extended the length of the list to 8190. A very recent breakthrough was achieved by Beierle and Leander [1] [2], where 12923 new quadratic APN functions were found in dimension 8. Before this paper, 21113 CCZ-inequivalent quadratic APN functions are found in dimension 8. We give other 5412 new quadratic APN functions. Thus, the number of CCZ-inequivalent quadratic APN functions in dimension 8 increase to 26525.

We will recall how to modify a QAM to get some new QAMs in what follows. Related theory and algorithm can be found in [11]. A discussion of our results on 8 bits, including conjectures about 8-bit APN functions, are presented in Section 4

2 Notation

The following notations and results are needed to understand our work.

$\mathbf{M}_\alpha$: Suppose $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, Let $M_\alpha \in \mathbb{F}_{2^n}^{n\times n}$ with $M_\alpha[i,u] = \alpha_u^{2^{i-1}}$ for $1 \le u, i \le n$. M_α^t is the transpose of M_α.

Rank: Let $\eta_1, \eta_2, \ldots, \eta_m$ be m elements on $\mathbb{F}_{2^n}$ $(m, n \ge 1)$, and $B = (\eta_1, \eta_2, \ldots, \eta_m) \in \mathbb{F}_{2^n}^m$, $\mathrm{Span}(B) = \mathrm{Span}(\eta_1, \eta_2, \ldots, \eta_m)$ denotes the subspace spanned by $\{\eta_1, \eta_2, \ldots, \eta_m\}$ over $\mathbb{F}_2$. $\mathrm{Rank}_{\mathbb{F}_2}(B) = \mathrm{Rank}_{\mathbb{F}_2}\{\eta_1, \eta_2, \ldots, \eta_m\}$ is the dimension of $\mathrm{Span}(B)$.

$\mathbf{C_F}$: Let $F(x) = \sum_{1\le t<i\le n} c_{i,t}x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$ be a homogeneous quadratic function, then the coefficient matrix C_F is an $n\times n$ matrix such that $C_F[t,i] = C_F[i,t] = c_{i,t}$ for $1 \le t < i \le n$ and $C_F[i,i] = 0$ for $1 \le i \le n$.

For any homogeneous quadratic function $F(x)$, if $H = M_\alpha^t C_F M_\alpha$, then H is a symmetric matrix over $\mathbb{F}_{2^n}$ with main diagonal elements zeros. In our algorithm, we choose the normal basis to construct the matrix M_α for simplicity. Suppose

$$\alpha \;=\; \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \;=\; \{\gamma, \gamma^2, \ldots, \gamma^n\}$$

is a normal basis on $\mathbb{F}_{2^n}$. Then we have $M_\alpha[i,u] = \gamma^{2^{i+u-2}}$ for $1 \le u, i \le n$. Specifically, we let $\gamma = g^{11}, g^{13}, g^{11}$ on $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$, respectively, where g is the default primitive element in Magma.

Our generating method relies on the following concept from [11].

Definition 2.1 ([11]QAM) *Let $H = (h_{u,v})_{n\times n}$ be an $n\times n$ matrix defined on $\mathbb{F}_{2^n}$. The matrix H is called a* Quadratic APN Matrix (QAM) *if:*

1. *H is symmetric and the elements in its main diagonal are all zeros, and*
2. *every nonzero linear combination of the n rows of H has rank $n-1$.*

Crucially, there is a one-to-one correspondance between quadratic homogenous APN functions and a subset of such matrices, as explained by the following theorem from the same reference.

Theorem 2.2 (Theorem 1 of [11]) *Let $F(x) = \sum_{1\le t<i\le n} c_{i,t}x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$, C_F and M_α be defined as above. Let*

$$H = M_\alpha^t C_F M_\alpha. \tag{1}$$

Then, $\delta(F) = 2^k$ if and only if any nonzero linear combination of the n rows of H has rank at least $n-k$. In particular, F is APN on $\mathbb{F}_{2^n}$ if and only if H is a QAM. In fact, Equation (1) builds a one to one correspondence between quadratic APN functions and QAMs.

3 On the Completeness of the QAM-based Approach

Full classifications of CCZ-equivalence classes of quadratic APN functions are known for 6- and 7-bit functions. All those CCZ-classes could be obtained efficiently using a QAM-based approach.

3.1 13 Quadratic APN functions on $\mathbb{F}_{2^6}$

Edel [6] proved that the total number of CCZ-inequivalent quadratic APN functions is 13. We can get 13 CCZ-inequivalent quadratic APN functions with the following method.

$$H_6 = \begin{pmatrix} 0 & g^4 & g^{41} & 1 & g^{26} & g^2 \\ g^4 & 0 & g^8 & g^{19} & 1 & \mathbf{x_4} \\ g^{41} & g^8 & 0 & g^{16} & g^{38} & \mathbf{x_3} \\ 1 & g^{19} & g^{16} & 0 & g^{32} & \mathbf{x_2} \\ g^{26} & 1 & g^{38} & g^{32} & 0 & \mathbf{x_1} \\ g^2 & \mathbf{x_4} & \mathbf{x_3} & \mathbf{x_2} & \mathbf{x_1} & 0 \end{pmatrix}.$$

Proposition 3.1 *Let $C_F = M_\alpha^{-1} H_6 (M_\alpha^t)^{-1}$ be the coefficient matrix of $F(x) \in \mathbb{F}_{2^6}[x]$. All (13) CCZ-inequivalent classes quadratic APN functions on $\mathbb{F}_{2^6}$ can be obtained by letting x_1, x_2, x_3 and x_4 traverse $\mathbb{F}_{2^6}$.*

3.2 488 Quadratic APN functions on $\mathbb{F}_{2^7}$

Kalgin and Idrisova [8] proved that the complete classification of quadratic APN functions up to CCZ-equivalence in dimension 7 contains 488 classes. We can get 488 CCZ-inequivalent quadratic APN functions as follows.

$$H_7 = \begin{pmatrix} 0 & g^{107} & g^{51} & g^{73} & g^{25} & g^{108} & \mathbf{x_6} \\ g^{107} & 0 & g^{87} & g^{102} & g^{19} & g^{50} & \mathbf{x_5} \\ g^{51} & g^{87} & 0 & g^{47} & g^{77} & \mathbf{x_9} & \mathbf{x_4} \\ g^{73} & g^{102} & g^{47} & 0 & g^{94} & \mathbf{x_8} & \mathbf{x_3} \\ g^{25} & g^{19} & g^{77} & g^{94} & 0 & \mathbf{x_7} & \mathbf{x_2} \\ g^{108} & g^{50} & \mathbf{x_9} & \mathbf{x_8} & \mathbf{x_7} & 0 & \mathbf{x_1} \\ \mathbf{x_6} & \mathbf{x_5} & \mathbf{x_4} & \mathbf{x_3} & \mathbf{x_2} & \mathbf{x_1} & 0 \end{pmatrix}.$$

Proposition 3.2 *Let $C_F = M_\alpha^{-1} H_7 (M_\alpha^t)^{-1}$ be the coefficient matrix of $F(x) \in \mathbb{F}_{2^7}[x]$. All (488) CCZ-inequivalent classes quadratic APN functions on $\mathbb{F}_{2^7}$ can be obtained by letting x_1, x_2, $\cdots$, x_8 and x_9 traverse $\mathbb{F}_{2^7}$.*

4 New 8-bit Quadratic APN Functions

4.1 Our Results

Using the search algorithm from [11], we could obtain 6794 functions. These do not all correspond to new CCZ-classes. To figure it out, we used the ortho-derivative based approach described in [4]: for each function F, we compute its *ortho-derivative* π_F. Then, the differential and extended Walsh spectra of π_F serve as a label for a bucket. The crucial fact behind this approach is that two functions with different bucket labels cannot be EA-equivalent, and thus cannot be CCZ-equivalent.[1] Here are some observations about these 6794 functions.

- There are repetitions: 1 bucket contains 3 different functions, and 245 contain 2. As a consequence, we can only prove that there are at least 6547 distinct CCZ-classes in the set we generated.
- Among these 6547 functions, only 2 had already been found by Beierle and Leander [2]; and 1133 had already been found using the QAM method [11]. The intersections are distinct.

In total, we have 5412 new classes of quadratic APN function operating on 8 bits. These functions have been added to `sboxU`:[2] the function

```
sboxU.known_functions.eightBitAPN.second_QAMs()
```

returns a list containing their look-up tables. The function

```
sboxU.known_functions.eightBitAPN.all_quadratics()
```

now also returns them.

4.2 Some Conjectures

First, in light of the results on 6- and 7-bit functions, we make the following conjecture.

[1] As recalled before, two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [10].

[2] `https://github.com/lpp-crypto/sboxU`

Conjecture 1 *Let $C_F = M_\alpha^{-1} H_8 (M_\alpha^t)^{-1}$ be the coefficient matrix of $F(x) \in \mathbb{F}_{2^8}[x]$, where H_8 is such that*

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

All CCZ-inequivalent classes of quadratic APN functions on $\mathbb{F}_{2^8}$ can be obtained by letting x_1, x_2, $\cdots$, x_{12} and x_{13} traverse $\mathbb{F}_{2^8}$.

Up to now, the total number of CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$ has increased up to 26514. However, this number is still far from complete. We give a conjecture to estimate the lower bound of the total number.

Conjecture 2 *The total number of CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$ is more than 50000.*

This conjecture comes from our experimental results. When we found 2282 quadratic APN functions on $\mathbb{F}_{2^8}$, 2252 are new compared to the 12 known ones. That is, more than 98.6% are new. When we found 6794 quadratic APN functions on $\mathbb{F}_{2^8}$, 5412 are new compared to the 21102 known ones. That is, 79.6% are new. And we have only traversed less than 1% elements of the last two columns of the matrix H_8. Thus, we can still find a large number of quadratic APN functions with the QAM method. According to our experimence in dimension 6 and 7, only when the proportion of the APN functions constructed by the QAM method are new compared to the known ones becomes very low, the list of CCZ-inequivalent quadratic APN is close to be complete. Therefore, much work waiting to be done on $\mathbb{F}_{2^8}$.

References

[1] C. Beierle, M. Brinkmann, G. Leander, Linearly Self-Equivalent APN Permutations in Small Dimension. https://arxiv.org/abs/2003.12006?context=cs.IT (26 Mar 2020).

[2] C. Beierle, G. Leander, New Instances of Quadratic APN Functions. https://arxiv.org/abs/2009.07204.

[3] K. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe, An APN permutation in dimension six, Contemaray Mathematics 58, p.33-42, (2010).

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

[5] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev, Codes, bent functions and permutations suitable for des-like cryptosystems. Des. Codes Cryptogr., 15(2):125–156, 1998.

[6] Y. Edel, Quadratic APN functions as subspaces of alternating bilinear forms. In: Proceedings of the Contact Forum Coding Theory and Cryptography III, Belgium 2009, pp. 11–24 (2011).

[7] Y. Edel, A. Pott, A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun., 3(1):59–81, 2009.

[8] K. Kalgin, V. Idrisova, The classification of quadratic APN functions in 7 variables, https://eprint.iacr.org/2020/1515.

[9] G. Weng, Y. Tan, G. Gong, On quadratic almost perfect nonlinear functions and their related algebraic object. In Workshop on Coding and Cryptography, WCC., 2013.

[10] S. Yoshiara, Equivalences of quadratic APN functions. Journal of Algebraic Combinatorics, 35:461-475, September 2011.

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

Appendix 1

These information may be help to understand the QAM method and Proposition 1, Proposition 2 and Conjecture 1.

g is the default primitive element in Magma. The corresponding QAM of x^3 on $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ are in the following. Modifying the bold elements can generate new QAMs. There is one to one correspondence between QAMs and homogeneous quadratic APN functions, thus, we can find all CCZ-inequivalent quadratic APN functions by constructing enough new QAMs.

$$H_6' = \begin{pmatrix} 0 & g^{4} & g^{41} & 1 & g^{26} & g^{2} \\ g^{4} & 0 & g^{8} & g^{19} & 1 & \mathbf{g}^{\mathbf{52}} \\ g^{41} & g^{8} & 0 & g^{16} & g^{38} & \mathbf{1} \\ 1 & g^{19} & g^{16} & 0 & g^{32} & \mathbf{g}^{\mathbf{13}} \\ g^{26} & 1 & g^{38} & g^{32} & 0 & \mathbf{g} \\ g^{2} & \mathbf{g}^{\mathbf{52}} & \mathbf{1} & \mathbf{g}^{\mathbf{13}} & \mathbf{g} & 0 \end{pmatrix}.$$

$$H_7' = \begin{pmatrix} 0 & g^{107} & g^{51} & g^{73} & g^{25} & g^{108} & \mathbf{g}^{\mathbf{117}} \\ g^{107} & 0 & g^{87} & g^{102} & g^{19} & g^{50} & \mathbf{g}^{\mathbf{89}} \\ g^{51} & g^{87} & 0 & g^{47} & g^{77} & \mathbf{g}^{\mathbf{38}} & \mathbf{g}^{\mathbf{100}} \\ g^{73} & g^{102} & g^{47} & 0 & g^{94} & \mathbf{g}^{\mathbf{27}} & \mathbf{g}^{\mathbf{76}} \\ g^{25} & g^{19} & g^{77} & g^{94} & 0 & \mathbf{g}^{\mathbf{61}} & \mathbf{g}^{\mathbf{54}} \\ g^{108} & g^{50} & \mathbf{g}^{\mathbf{38}} & \mathbf{g}^{\mathbf{27}} & \mathbf{g}^{\mathbf{61}} & 0 & \mathbf{g}^{\mathbf{122}} \\ \mathbf{g}^{\mathbf{117}} & \mathbf{g}^{\mathbf{89}} & \mathbf{g}^{\mathbf{100}} & \mathbf{g}^{\mathbf{76}} & \mathbf{g}^{\mathbf{54}} & \mathbf{g}^{\mathbf{122}} & 0 \end{pmatrix}.$$

$$H_8' = \begin{pmatrix} 0 & g^{34} & g^{81} & g^{83} & g^{170} & g^{106} & \mathbf{g}^{\mathbf{84}} & \mathbf{g}^{\mathbf{17}} \\ g^{34} & 0 & g^{68} & g^{162} & g^{166} & g^{85} & \mathbf{g}^{\mathbf{212}} & \mathbf{g}^{\mathbf{168}} \\ g^{81} & g^{68} & 0 & g^{136} & g^{69} & g^{77} & \mathbf{g}^{\mathbf{170}} & \mathbf{g}^{\mathbf{169}} \\ g^{83} & g^{162} & g^{136} & 0 & g^{17} & g^{138} & \mathbf{g}^{\mathbf{154}} & \mathbf{g}^{\mathbf{85}} \\ g^{170} & g^{166} & g^{69} & g^{17} & 0 & g^{34} & \mathbf{g}^{\mathbf{21}} & \mathbf{g}^{\mathbf{53}} \\ g^{106} & g^{85} & g^{77} & g^{138} & g^{34} & 0 & \mathbf{g}^{\mathbf{68}} & \mathbf{g}^{\mathbf{42}} \\ \mathbf{g}^{\mathbf{84}} & \mathbf{g}^{\mathbf{212}} & \mathbf{g}^{\mathbf{170}} & \mathbf{g}^{\mathbf{154}} & \mathbf{g}^{\mathbf{21}} & \mathbf{g}^{\mathbf{68}} & 0 & \mathbf{g}^{\mathbf{136}} \\ \mathbf{g}^{\mathbf{17}} & \mathbf{g}^{\mathbf{168}} & \mathbf{g}^{\mathbf{169}} & \mathbf{g}^{\mathbf{85}} & \mathbf{g}^{\mathbf{53}} & \mathbf{g}^{\mathbf{42}} & \mathbf{g}^{\mathbf{136}} & 0 \end{pmatrix}.$$