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

August 13, 2021

Abstract

We found 5412 new quadratic APN functions on $\mathbb{F}_{2^8}$ by modifying the last two columns of a given QAM, 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 complete list (to the best of our knowledge) of known quadratic APN functions, including our new ones, has been added to `sboxU` for ease of study by others.

In this paper, we recall how to construct new QAMs from a known one. Based on these results and on others on smaller fields, we make two conjectures: that the total number of CCZ-inequivalent APN functions on $\mathbb{F}_{2^8}$ may exceed 50000, and that the full list of quadratic APN functions could be obtained by modifying only a small number of entries of the QAM (provided enormous computing power).

1 Introduction

Browning and Dillon [4] found the first APN permutation in dimension 6. Their idea was to check the CCZ-equivalence [6] class of a quadratic APN function: indeed, if an APN function is CCZ-equivalent to a permutation, then that permutation has to be APN. Browning and Dillon then provided a method to find APN permutations. Their idea was to construct new APN functions and to check whether they are equivalent to permutations. In this paper, we focus on how to construct quadratic APN functions in small dimensions, especially in dimension 8. Edel and Pott [8] listed 23 CCZ-inequivalent APN functions on $\mathbb{F}_{2^8}$. Weng et al.[11] and Yu et al.[13] 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. In total, 21113 CCZ-inequivalent quadratic APN functions were known before this paper. We present another 5412 new quadratic APN functions. Thus, the number of CCZ-inequivalent quadratic APN functions in dimension 8 increases to 26525.

We will recall how to modify a QAM to get some new QAMs in the sequel. The related theory and algorithm can be found in [13]. A discussion of our results on 8 bits, including conjectures about 8-bit APN functions, are presented in Section 3.

2 Notation

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

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

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** (quadratic functions without linear and constant terms), 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 $1 \le i \le n$.

$\delta(F)$: $\delta(F) = \max_{a \in \mathbb{F}_{2^n}^\star, b \in \mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} : F(x+a) - F(x) = b\}|$ denotes the differential uniformity of F.

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 $1 \le u, i \le n$. The transpose of M_α is denoted by M_α^t. 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 zero main diagonal. 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 $\gamma = g^{11}$ on $\mathbb{F}_{2^8}$, where g is the default primitive element in Magma [3].

Our method for generating QAMs relies on the following concept from [13].

Definition 2.1 ([13]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 correspondence between quadratic homogeneous APN functions and a subset of such matrices, as explained by the following theorem from the same paper.

Theorem 2.2 (Theorem 1 of [13]) *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) describes a one to one correspondence between quadratic homogeneous APN functions and QAMs.

3 New 8-bit Quadratic APN Functions

3.1 Our Results

Using the search algorithm from [13], 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. These do not all correspond to new CCZ-classes. In order to partition this set into CCZ-classes, we used a classical method based on CCZ-class invariants. Those we considered are listed in Section 3.2, the main one being based on the ortho-derivative [5].

In total, we have obtained 5412 new classes of quadratic APN functions operating on 8 bits. These functions have been added to `sboxU`[1]: 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 along with all other known quadratic APN functions in this dimension.

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

3.2 Using Class Invariants

In order to sort our functions into distinct EA-equivalence classes (and thus distinct CCZ-classes)[2] , we used the approach based on ortho-derivative introduced in [5]. First let us recall the definition of the ortho-derivative.

Definition 3.1 *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 $x \in \mathbb{F}_{2^n}$.

The crucial fact behind the sorting approach presented in [5] is that if two functions are EA-equivalent, then their ortho-derivatives are affine-equivalent. As a consequence, they need to have identical differential and extended Walsh spectra. Thus, two functions for which these spectra do not match cannot be EA-equivalent, and as a consequence cannot be CCZ-equivalent [12]. For each function F, we computed its *ortho-derivative* π_F. Then, we sorted all functions F according to the extended Walsh and differential spectra of their ortho-derivatives, keeping only one function when several had the same spectra. Here are some observations about these 6794 functions that we found.

- There are repetitions: there is a pair of spectra shared by 3 different functions, and 245 pairs that are each shared by 2 different functions. 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 a pair of spectra that was already present in the set identified by Beierle and Leander [2]; and 1133 had already been found using the QAM method [13]. The intersections are distinct: there was no function among the ones that we found that was in either the data set of Beierle and Leander or the previous QAM one.

In the end, we can conclude that we found 5412 new EA-equivalence classes of quadratic APN functions.

Unfortunately, none of our new functions yield a new Walsh spectrum. More precisely, if we let N_i denote the number of pairs $(a, b) \in \mathbb{F}_{2^8}$ with $b \neq 0$ such that $|\sum_{x \in \mathbb{F}_{2^8}} (-1)^{a \cdot x + b \cdot F(x)}| = i$, then we observe the following spectra:

$$\begin{aligned}
\mathcal{W}_1 &= \{N_0 = 16320, N_{16} = 43520, N_{32} = 5440\} \\
\mathcal{W}_2 &= \{N_0 = 15600, N_{16} = 44544, N_{32} = 5120, N_{64} = 16\} \\
\mathcal{W}_3 &= \{N_0 = 14880, N_{16} = 45568, N_{32} = 4800, N_{64} = 32\},
\end{aligned}$$

where $\mathcal{W}_1$ occurs 5084 times, $\mathcal{W}_2$ 324 times, and $\mathcal{W}_3$ only 4 times.

The Δ- and Γ-ranks are well known CCZ-class invariants defined as follows. First, let S be any subset of $\mathbb{F}_{2^n}$. We denote by $\mathsf{r}(S)$ the rank of the binary matrix $M(S)$ of dimension $2^n \times 2^n$ which is such that $M_{x,y} = 1$ if and only if $x + y \in S$. Then, we have that the Γ-rank of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is equal to

$$\Gamma_F \;=\; \mathsf{r}\left(\left\{(x, F(x)) : x \in \mathbb{F}_{2^n}\right\}\right),$$

and that its Δ-rank is

$$\Delta_F \;=\; \mathsf{r}\left(\left\{(a, b) \in (\mathbb{F}_{2^n})^2 : F(x+a) + F(x) = b \text{ has at least 1 solution}\right\}\right).$$

However, their computation relies on evaluating the rank of a binary matrix of dimension $2^{16} \times 2^{16}$, a task of significant computational complexity. Our best implementation could only compute

[2] As recalled before, two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [12].

57 of these in a week of computations[3]. Furthermore, the pairs formed by Δ-rank and Γ-rank of these 57 functions are one of only five distinct values in

$$\{(14044, 454), (14046, 452), (14046, 454), (14048, 454), (14050, 454)\}.$$

As a consequence, we can see that these invariants are of little interest when sorting quadratic APN functions for $n \geq 8$: they are slow to compute, and do not provide much differentiation.

We have also computed the multisets $\Sigma_4^F(0)$ for each F in our set of functions, where this quantity is the multiset defined as follows [9]:

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

and is an EA-class invariant. Evaluating this invariant on our full set of function is quite practical, and 4655 distinct values were found. This invariant is thus far more useful than the Δ- and Γ-rank: it can be computed much faster, and provides much more differentiation. It also has the significant advantage over the ortho-derivative that it does not require the function investigated to be both quadratic and APN.

3.3 Some Conjectures

Up to now, the total number of CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$ is more than 26000. However, we believe that this number is still far from complete. We give a conjecture to estimate the lower bound of the total number.

Conjecture 1 *The total number of CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$ is more than 50000.*

We list some facts to support Conjecture 1 that correspond to the experiments we made by looping through all the QAMs with a given structure for a given n.

(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.

The following conjecture may provide a method to construct the complete list of quadratic APN functions in dimension 8.

Conjecture 2 *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*

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

[3]For comparison, computing the extended Walsh and differential spectra of all our new functions takes 21 seconds on the same machine.

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

The first 6×6 submatrix of H_8 is the same as the corresponding QAM of x^3, and all known QAM-based APN functions are constructed by modifying the last two columns (and rows) of the matrix H_8. However, we have only traversed less than 1% elements of the last two columns (and rows), and there is an about 79% probability that the next QAM-based APN function is new compared to all known ones.

We had to generate more than 200 (about 16×13) and more than 3000 (about 8×488) quadratic APN functions using the QAM method in order to obtain the complete list of quadratic APN functions in dimension 6 and dimension 7, respectively. Therefore, we may need to generate more than 200000 (4×50000) quadratic APN functions in order to get the complete list in dimension 8 using a QAM-based approach. Thus, there is a high probability that we can get the full list after traversing x_1, x_2, ..., x_{12} and x_{13}, since using this method we can construct at least 2000000 quadratic APN functions. This would require substantial computations corresponding to centuries of CPU time.

Acknowledgements

We would like to thank the anonymous referees for their detailed and helpful suggestions.

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] 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).

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

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

[6] 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).

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

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

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

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

[11] 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).

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

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