Linearly Self-Equivalent APN Permutations in Small Dimension

Christof Beierle, Marcus Brinkmann, Gregor Leander

Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany

March 28, 2020

Abstract

All almost perfect nonlinear (APN) permutations that we know to date admit a special kind of linear self-equivalence, i.e., there exists a permutation G in their CCZ-class and two linear permutations A and B, such that $G \circ A = B \circ G$. After providing a survey on the known APN functions with a focus on the existence of self equivalences, we explicitly search for APN permutations in dimension 6, 7, and 8 that admit such a linear self equivalence. In dimension six, we were able to conduct an *exhaustive search* and obtain that there is only one such APN permutation up to CCZ-equivalence. In dimensions 7 and 8, we exhaustively searched through parts of the space and conclude that the linear self equivalences of such APN permutations must be of a special form. As one interesting result in dimension 7, we obtain that all APN permutation polynomials with coefficients in $\mathbb{F}_2$ must be (up to CCZ-equivalence) monomial functions.

Keywords: APN permutations, differential cryptanalysis, self equivalence, automorphism, CCZ equivalence, exhaustive search

1 Introduction

Differential cryptanalysis [3] certainly belongs to the most important attack vectors to consider when designing a new symmetric cryptographic primitive. The basic idea of this attack is that the adversary chooses an input difference a in the plaintext space and evaluates the encryption of pairs of values $(x, x + a)$ for a plaintext x and tries to predict the output difference of the two ciphertexts with a high probability. Vectorial Boolean functions (aka. *S-boxes*) that offer the best resistance against differential attacks are called *almost perfect nonlinear (APN)*. Precisely, a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called APN if, for every $b \in \mathbb{F}_2^m$ and non-zero $a \in \mathbb{F}_2^n$, the equation $F(x) + F(x + a) = b$ has at most two solutions. We know very few examples or constructions of APN functions and much less is known if we require F to be a permutation.

This work was funded by Deutsche Forschungsgemeinschaft (DFG); project number 411879806 and by DFG under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

For odd values of n, we know infinite families of APN permutations and in particular, they exist for every odd value of n. For even values of n, we only know one sporadic example up to CCZ-equivalence, i.e., for $n = 6$ (see [9]). Exhaustive search for APN permutations is only possible as long as n is small because the search space heavily increases. So far, an exhaustive search for APN permutations was only conducted up to $n = 5$ (see [8]). Since already for $n = 6$, the number of permutations in $\mathbb{F}_2^n$ is orders of magnitude higher ($64! \approx 2^{296}$ compared to $32! \approx 2^{117.7}$), the search space for finding new APN permutations has to be restricted in a meaningful way. Our idea is to restrict to the class of permutations that we conjecture to contain all possible cases. Namely, we restrict to the class of permutations that admit a non-trivial *linear self-equivalence*, i.e., those permutations F for which there exist non-trivial linear permutations A and B such that $F \circ A = B \circ F$.

1.1 Our Contribution

In the first part of this work, we provide a survey on all APN functions known from the literature and observe that they all admit a non-trivial automorphism. An *automorphism* of a vectorial Boolean function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an affine permutation in $\mathbb{F}_2^n \times \mathbb{F}_2^m$ that leaves the set $\{(x, F(x)) \mid x \in \mathbb{F}_2^n\}$ invariant. For all the known APN permutations $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, we show that there exists an automorphism of a special kind, i.e., there exists a permutation G which is CCZ-equivalent to F that admits a non-trivial linear self-equivalence. Since a linear self-equivalence is a special kind of automorphism, we also call it *LE-automorphism*. We conjecture the existence of a CCZ-equivalent permutation with a non-trivial LE-automorphism for any APN permutation (Conjecture 1).

Based on this conjecture, our goal is to conduct an exhaustive search for all such APN permutations in small dimension. To prepare, we first classify all possible LE-automorphisms that need to be considered in such a search. The most important observation here is that the number of tuples (A, B) can be reduced by only considering linear permutations up to similarity and identical cycle types for A and B. Surprisingly, we only need to consider a very low number of tuples, i.e., 17 for $n = 6$, 27 for $n = 7$, and 32 for $n = 8$. We stress that this reduction is valid for any kind of search within the permutations with non-trivial LE-automorphisms; it is not restricted to APN permutations.

We then use the above classification of LE-automorphism to explicitly search for APN permutations in dimension $n \in \{6, 7, 8\}$. By using the APN property, we can exclude some of the LE-automorphisms by theory (Propositions 4 and 5). For the others, we implemented a recursive tree search algorithm (Algorithm 1). For $n = 6$, we are able to *exhaustively* search for the APN permutations with non-trivial LE-automorphisms and conclude that only the CCZ-equivalence class of the only known APN permutation remains. In other words, if Conjecture 1 is true, this is the only APN permutation in dimension 6 up to CCZ-equivalence. For $n = 7$, we found all the APN monomial permutations, but no more CCZ classes. For $n = 8$, no APN permutations have been found. Since for $n \in \{7, 8\}$, we exhaustively searched through parts of the search space, we conclude that if new CCZ-classes of APN permutations with non-trivial LE-automorphisms exist, those automorphisms have to be of special forms (Theorem 3 and 4). Our *exhaustive search* for $n = 7$ covers the special case of *shift-invariant permutations*, which correspond to all permutation polynomials in $\mathbb{F}_{2^7}$ with coefficients in $\mathbb{F}_2$ (there are 20,851,424,802,623,573,443,244,703,744,000 of those, see [23] and OEIS sequence A326932 [36]). We obtain that the only shift-invariant APN permutations in dimension 7 are monomial functions.

2 Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ denote the field with two elements, let $\mathrm{GL}(n, \mathbb{F}_2)$ denote the group of invertible $n \times n$ matrices over $\mathbb{F}_2$ and let $\mathrm{AGL}(n, \mathbb{F}_2)$ denote the group of affine permutations on $\mathbb{F}_2^n$, i.e., the set of functions of the form $x \mapsto Lx + b$ for $L \in \mathrm{GL}(n, \mathbb{F}_2)$ and $b \in \mathbb{F}_2^n$. We denote by I_n the identity matrix in $\mathrm{GL}(n, \mathbb{F}_2)$. We denote a block-diagonal matrix consisting of blocks $M_1, M_2, \dots, M_k$ by $M_1 \oplus M_2 \oplus \cdots \oplus M_k$, where M_1 corresponds to the block in the upper left. For a matrix $M \in \mathrm{GL}(n, \mathbb{F}_2)$, we denote by $\mathrm{ord}(M)$ the *multiplicative order* of M, i.e., the smallest positive integer i such that $M^i = I_n$. Similarly, for a vector $x \in \mathbb{F}_2^n$, we denote by $\mathrm{ord}_M(x)$ the smallest positive integer i for which $M^i(x) = x$. It is well known that $\mathrm{ord}_M(x) \mid \mathrm{ord}(M)$.

For a polynomial $q = X^n + q_{n-1}X^{n-1} + \cdots + q_1X + q_0 \in \mathbb{F}_2[X]$ of degree n, the *companion matrix* of q is defined as the $n \times n$ matrix

$$\mathrm{Comp}(q) \coloneqq \begin{pmatrix} 0 & & & & q_0 \\ 1 & 0 & & & q_1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & q_{n-2} \\ & & & 1 & q_{n-1} \end{pmatrix} \in \mathrm{GL}(n, \mathbb{F}_2) .$$

Since this paper focuses on APN functions, we first recall the definition.

Definition 1. *[33] A vectorial Boolean function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called* almost perfect nonlinear *(APN) if, for every $a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^n$, the equation $F(x) + F(x + a) = b$ has at most 2 solutions for $x \in \mathbb{F}_2^n$.*

Let $F, G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be vectorial Boolean functions in dimension n. There are several well-known equivalence relations on vectorial Boolean functions. G is called *linear equivalent* to F if there exist $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$ such that $F \circ A = B \circ G$. If A and B are allowed to be in $\mathrm{AGL}(n, \mathbb{F}_2)$, G and F are called *affine equivalent*. Finally, we consider the notion of CCZ-equivalence. Let $\Gamma_F \coloneqq \{(x, F(x))^\top \mid x \in \mathbb{F}_2^n\}$ be the *graph* of F. The functions F and G are called *CCZ-equivalent* if there exist $\sigma \in \mathrm{AGL}(2n, \mathbb{F}_2)$ such that $\Gamma_G = \sigma(\Gamma_F)$. The above equivalence notions are ordered by strength with CCZ-equivalence being the strongest. In other words, two linear equivalent functions are also affine equivalent and two affine equivalent functions are also CCZ-equivalent.

The automorphism group of a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as

$$\mathsf{Aut}(F) \coloneqq \{\sigma \in \mathrm{AGL}(2n, \mathbb{F}_2) \mid \Gamma_F = \sigma(\Gamma_F)\} .$$

Analogously, we define the subgroups $\mathsf{Aut}_{\mathsf{AE}}$ and $\mathsf{Aut}_{\mathsf{LE}}$ as follows:

$$\mathsf{Aut}_{\mathsf{AE}}(F) := \left\{ \sigma \in \mathsf{Aut}(F) \mid \sigma = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \text{ for } A, B \in \mathrm{AGL}(n, \mathbb{F}_2) \right\}$$
$$\mathsf{Aut}_{\mathsf{LE}}(F) := \left\{ \sigma \in \mathsf{Aut}(F) \mid \sigma = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \text{ for } A, B \in \mathrm{GL}(n, \mathbb{F}_2) \right\}$$

It is $\{\mathrm{id}\} \subseteq \mathsf{Aut}_{\mathsf{LE}}(F) \subseteq \mathsf{Aut}_{\mathsf{AE}}(F) \subseteq \mathsf{Aut}(F) \subseteq \mathrm{AGL}(2n, \mathbb{F}_2)$. The automorphism group of F, resp., the subgroups $\mathsf{Aut}_{\mathsf{AE}}(F)$ and $\mathsf{Aut}_{\mathsf{LE}}(F)$ contain non-trivial elements if and only if F is self-equivalent with regard to the corresponding equivalence relation. For instance,

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \in \mathsf{Aut}(F) \quad \Leftrightarrow \quad F \circ A = B \circ F \;.$$

Self equivalences of vectorial Boolean functions in small dimension have already been considered in the PhD thesis [24]. Note that if F and G are CCZ-equivalent, resp., affine equivalent, resp., linear equivalent, it is $\mathsf{Aut}(F) \cong \mathsf{Aut}(G)$, resp., $\mathsf{Aut}_{\mathsf{AE}}(F) \cong \mathsf{Aut}_{\mathsf{AE}}(G)$, resp., $\mathsf{Aut}_{\mathsf{LE}}(F) \cong \mathsf{Aut}_{\mathsf{LE}}(G)$. Therefore, it is enough to consider only one single representative in each equivalence class when determining the automorphism groups. Throughout this paper, we are especially interested in APN permutations F with non trivial elements in $\mathsf{Aut}_{\mathsf{LE}}(F)$. If $|\mathsf{Aut}_{\mathsf{LE}}(F)| > 1$, we say that F has a non-trivial *LE-automorphism* (or a non-trivial *linear self equivalence*).

3 Automorphisms of Some (APN) Functions

It is well known (e.g., see [20, Section 5.1]) that the automorphism group of a function F can be computed by considering the associated linear code C_F for F with parity-check matrix

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_{2^n} \\ F(x_1) & F(x_2) & \dots & F(x_{2^n}) \end{bmatrix}$$

and computing its automorphism group, e.g., with the algorithm presented in [29]. However, in this part of the paper we are only interested in determining whether or not a non-trivial element in $\mathsf{Aut}(F)$, resp., $\mathsf{Aut}_{\mathsf{LE}}(F)$, exists, especially for the case of an APN function F. In the following, we study some interesting classes of functions and sporadic APN functions.

3.1 Quadratic Functions

Lots of function families studied in the literature are CCZ-quadratic, i.e., they are CCZ-equivalent to a function which coordinate functions only contain monomials of algebraic degree at most 2. Alternatively, if those functions are represented as mappings from the finite field $\mathbb{F}_{2^n}$ to itself, its polynomial representation only contains monomials of the form x^{2^i} or $x^{2^i+2^j}$ with non-zero coefficients. One reason that they are studied a lot in the literature is because they are much easier to handle. For instance, every first-order derivative is affine. The following is a well-known result (see, e.g., [7, Proposition 1] or [28, Theorem 4]).

Proposition 1. *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function. Then,* $|\mathsf{Aut}(F)| \geq 2^n$*.*

Proof. Let $\alpha \in \mathbb{F}_{2^n} \setminus \{0\}$. Since F is quadratic, $F(x) + F(x+\alpha) + F(\alpha)$ is linear. Let us denote this function by L_α. The function defined as

$$\sigma_\alpha\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}, \quad (x,y) \mapsto (x+\alpha, y + L_\alpha(x) + F(\alpha) + L_\alpha(\alpha))$$

is included in $\mathsf{Aut}(F)$. Indeed, it is easy to see that σ_α is an affine permutation. Further, it is

$$\begin{aligned} \sigma_\alpha(\Gamma_F) = \sigma_\alpha\{(x, F(x))\} &= \{(x+\alpha, F(x) + L_\alpha(x) + F(\alpha) + L_\alpha(\alpha))\} \\ &= \{(x, F(x+\alpha) + L_\alpha(x) + F(\alpha)) = \{(x, F(x))\} = \Gamma_F \ . \end{aligned}$$

This implies that $\mathsf{Aut}(F)$ contains $2^n - 1$ non-trivial elements. Since id is trivially contained in $\mathsf{Aut}(F)$, this concludes the proof. □

Many of the known APN functions are quadratic up to CCZ-equivalence, for instance the Gold functions $x \mapsto x^{2^i+1}$ for $\gcd(i,n) = 1$ (see [30, 32]), the two functions from $\mathbb{F}_{2^{10}}$ and $\mathbb{F}_{2^{12}}$ to itself defined in [27], and the classes defined in [5, 6, 11, 12, 13, 14, 15, 16, 18, 22, 40]. Indeed, to the best of our knowledge, at the time of writing only *a single* APN function is known which is not CCZ-equivalent to either a quadratic or a monomial function (see [28, 8]). We refer to [21, Sections 3.1.6–3.1.7] and Table 1.6 in the PhD thesis [1] for a recent summary of the known infinite classes of APN functions.

We leave it as an open question whether for a (quadratic) function F with a non-trivial automorphism in $\mathsf{Aut}(F)$ there always exists a representative G in the CCZ-class of F with a non-trivial automorphism in $\mathsf{Aut}_{\mathsf{LE}}(G)$. However, we will see in the following that in many cases, for APN functions, there exists such a representative of the CCZ-class.

3.2 Shift-Invariant Functions

The *shift-invariant* functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are exactly those for which

$$\begin{bmatrix} \mathrm{Comp}(X^n+1) & 0 \\ 0 & \mathrm{Comp}(X^n+1) \end{bmatrix} \in \mathsf{Aut}_{\mathsf{LE}}(F) \ .$$

If F is represented as a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ in the normal basis representation, this automorphism corresponds to squaring, i.e., for all $x \in \mathbb{F}_{2^n}$, $F(x^2) = F(x)^2$. Therefore, the shift-invariant functions correspond to the polynomials with coefficients in $\mathbb{F}_2$.

A lot of the known APN function families belong to the class of shift-invariant functions. Those include all the APN monomial functions $x \mapsto x^d$ and also the functions defined in [10, 15, 17]. For the latter, this is because $\mathrm{Tr}_m(x^2) = \mathrm{Tr}_m(x)^2$, where $\mathrm{Tr}_m(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{mi}}$ denotes the trace function from $\mathbb{F}_{2^n}$ to a subfield $\mathbb{F}_{2^m}$.

3.3 APN Binomial (and some Multinomial) Functions

For monomial functions, a non-trivial LE-automorphism can easily be given in terms of multiplication with finite field elements. In particular, if $x \in \mathbb{F}_{2^n}$, then, for any $\alpha \in \mathbb{F}_{2^n} \setminus \{0\}$, it is $(\alpha x)^d = \alpha^d x^d$.

The *binomial functions* $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are those which can be written as $F(x) = x^a + \omega x^b$, where $a, b \in \mathbb{Z}$ and $\omega \in \mathbb{F}_{2^n}$. For special choices of a and b, we can also easily give an LE-automorphism as follows.

Proposition 2. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, x \mapsto x^a + \omega x^b$ be a binomial function. Let $\alpha \in \mathbb{F}_{2^n}$ be an element of order d, where $d|(b-a)$. Then*

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^a \end{bmatrix} \in \mathsf{Aut}_{\mathsf{LE}}(F) \ .$$

Indeed, it is $(\alpha x)^a + \omega(\alpha x)^b = \alpha^a x^a + \omega \alpha^b x^b = \alpha^a(x^a + \omega \alpha^{b-a} x^b)$, and $\alpha^{b-a} = 1$ because $\mathrm{ord}(\alpha)|(b-a)$. Therefore, if $\gcd(b-a, 2^n-1) \neq 1$, we have a non-trivial element in $\mathsf{Aut}_{\mathsf{LE}}(F)$.

Example 1 (APN function[1] defined in Theorem 2 of [27]). Let $u \in \mathbb{F}_{2^{10}}^*$ be an element of order 3. The function $F\colon \mathbb{F}_{2^{10}} \to \mathbb{F}_{2^{10}}, x \mapsto x^3 + \omega x^{36}$ is APN if and only if $\omega \in \{u\mathbb{F}_{2^5}^*\} \cup \{u^2\mathbb{F}_{2^5}^*\}$.

Since $\gcd(36-3, 2^{10}-1) = 33$, a non-trivial automorphism in $\mathsf{Aut}_{\mathsf{LE}}(F)$ can be given by an element of order 33. □

Example 2 (APN functions defined in Theorem 1 of [14]). Let s and k be positive integers with $\gcd(s, 3k) = 1$ and let $t \in \{1, 2\}, i = 3-t$. Let further $a = 2^s+1$ and $b = 2^{ik}+2^{tk+s}$ and let $\omega = \alpha^{2^k-1}$ for a primitive element $\alpha \in \mathbb{F}_{2^{3k}}^*$. If $\gcd(2^{3k}-1, (b-a)/(2^k-1)) \neq \gcd(2^k-1, (b-a)/(2^k-1))$, the function $F\colon \mathbb{F}_{2^{3k}} \to \mathbb{F}_{2^{3k}}, x \mapsto x^a + \omega x^b$ is APN.

If $\gcd(2^{3k}-1, (b-a)/(2^k-1)) \neq 1$, the conditions of Proposition 2 are fulfilled and a non-trivial automorphism can be given by an element of order $\gcd(2^{3k}-1, (b-a))$. Otherwise, $\gcd(2^k-1, (b-a)/(2^k-1)) \neq 1$ by assumption and, since $(2^k-1)(2^k+2^{2k}+1) = 2^{3k}-1$, also $\gcd(2^{3k}-1, (b-a)) \neq 1$. Therefore, a non-trivial automorphism in $\mathsf{Aut}_{\mathsf{LE}}(F)$ always exists. □

Example 3 (APN functions defined in Theorem 2 of [14]). Let s and k be positive integers such that $s \leq 4k-1$, $\gcd(k, 2) = gcd(s, 2k) = 1$, and $i = sk \mod 4$, $t = 4-i$. Let further $a = 2^s+1$ and $b = 2^{ik}+2^{tk+s}$ and let $\omega = \alpha^{2^k-1}$ for a primitive element $\alpha \in \mathbb{F}_{2^{4k}}^*$. Then, the function $F\colon \mathbb{F}_{2^{4k}} \to \mathbb{F}_{2^{4k}}, x \mapsto x^a + \omega x^b$ is APN.

We will show that $b-a \mod 5 = 0$. Then, since $(2^4-1)|(2^{4k}-1)$, a non-trivial automorphism can be given. Indeed, the following equalities hold $\mod 5$:

$$\begin{aligned} b-a &= 2^{ik} + 2^{tk+s} - 2^s - 1 = 2^{(4m+sk)k} + 2^{tk+s} - 2^s - 1 \\ &= (2^{k^2})^s + 2^{tk+s} - 2^s - 1 = 2^{tk+s} - 1 \ , \end{aligned}$$

[1] recently classified into an infinite family, see [18]

where the last equality is fulfilled because k is odd and thus, $2^{k^2} = 2 \mod 5$. It is left to show that $2^s 2^{tk} = 1 \mod 5$. This can easily be obtained by considering the four different cases of $s \in \{1,3\} \mod 4$, $k \in \{1,3\} \mod 4$. □

Extension to Multinomial Functions. Proposition 2 can easily be generalized to multinomial functions as follows.

Proposition 3. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, x \mapsto \sum_{i=0}^{k-1} \omega_i x^{a_i}$. Let $\alpha \in \mathbb{F}_{2^n}$ be an element of order d, such that, for all $i \in \{0,\dots,k-1\}$, $d|(a_i - a_0)$. Then,*

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^a \end{bmatrix} \in \mathsf{Aut}_{\mathsf{LE}}(F) .$$

Example 4 (APN functions defined in Theorem 1 of [5]). Let k and s be odd integers with $\gcd(k,s) = 1$. Let $b \in \mathbb{F}_{2^{2k}}$ which is not a cube, $c \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$, and, for $i \in \{1,\dots,k-1\}$, let $r_i \in \mathbb{F}_{2^k}$. Then, the function

$$F\colon \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^{2k}}, \quad x \mapsto bx^{2^s+1} + b^{2^k} x^{2^{k+s}+2^k} + cx^{2^k+1} + \sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}$$

is APN.

Recall that $2^{2k} - 1 = 0 \mod 3$. To show that F admits a non-trivial automorphism according to Proposition 3, we see that

(i) $2^{k+s} + 2^k - 2^s - 1 = 0 \mod 3$, and

(ii) $\forall i \in \{0,1,\dots,k-1\}, 2^{i+k} + 2^i - 2^s - 1 = 0 \mod 3$. □

Example 5 (APN functions defined in Theorem 2.1 of [6]). Let k and s be positive integers such that $k + s = 0 \mod 3$ and $gcd(s,3k) = \gcd(3,k) = 1$. Let further $u \in \mathbb{F}^*_{2^{3k}}$ be primitive and let $v, w \in \mathbb{F}_{2^k}$ with $vw \neq 1$. Then, the function

$$F\colon \mathbb{F}_{2^{3k}} \to \mathbb{F}_{2^{3k}}, \quad x \mapsto ux^{2^s+1} + u^{2^k} x^{2^{2k}+2^{k+s}} + vx^{2^{2k}+1} + wu^{2^k+1} x^{2^{k+s}+2^s}$$

is APN.

Recall that $2^{3k} - 1 = 0 \mod 7$. To show that F admits a non-trivial automorphism according to Proposition 3, we show that

1. $2^{2k} + 2^{k+s} - 2^s - 1 = 0 \mod 7$, and
2. $2^{2k} + 1 - 2^s - 1 = (2^k)^2 - 2^s = 0 \mod 7$, and
3. $2^{k+s} + 2^s - 2^s - 1 = 2^{k+s} - 1 = 0 \mod 7$.

Case (iii) holds because $k + s = 0 \mod 3$ and thus, $2^{k+s} = 1 \mod 7$. Case (ii) can be deduced by considering the two cases of $k = 1 \mod 3$ and $k = 2 \mod 3$ separately. Case (i) immediately follows from (ii) and (iii). □

3.4 Generalized Butterflies

It was shown in [35] that the sporadic APN permutation in dimension six found in [9] (aka., the "Dillon" permutation) can be decomposed into a special structure.

Definition 2 (Generalized Butterfly [19])**.** *Let $n \in \mathbb{N}$ be odd and let $\alpha, \beta \in \mathbb{F}_{2^n}, \beta \neq 0$. An* open generalized butterfly *is defined as a permutation*

$$\mathsf{H}_{\alpha,\beta} \colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \quad (x,y) \mapsto \big(R(y, R^{-1}(x,y)), R^{-1}(x,y)\big) \ ,$$

where $R(x,y) = (x + \alpha y)^3 + \beta y^3$.

The APN permutation found in [9] is affine equivalent to $\mathsf{H}_{\alpha,\beta}$ for $n = 3, \beta = 1$ and $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 0$. More generally, open generalized butterflies are APN for $n = 3, \alpha \neq 0$ with $\mathrm{Tr}(\alpha) = 0$ and $\beta \in \{\alpha^3 + \alpha, (\alpha^3 + 1)\alpha^{-1}\}$.

Let ζ denote a non-zero element of the finite field $\mathbb{F}_{2^n}$. For

$$A = \begin{pmatrix} \zeta^3 & \\ & \zeta \end{pmatrix} \ ,$$

we have $\mathsf{H}_{\alpha,\beta} \circ A = A \circ \mathsf{H}_{\alpha,\beta}$ for any $\alpha, \beta \in \mathbb{F}_{2^n}, \beta \neq 0$. Thus, there always exists a non-trivial element in $\mathsf{Aut}_{\mathsf{LE}}(\mathsf{H}_{\alpha,\beta})$.

For $n = 3$, it is easy to verify that all matrices A of the structure above for $\zeta \neq 1$ are similar to $\mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$.

3.5 Known APN Functions in Small Dimension

Up to dimension $n = 5$, all APN functions are CCZ-equivalent to monomial functions, see [8].

In [28], for dimensions $n \in \{6, 7, 8\}$, Edel and Pott constructed new APN functions up to CCZ-equivalence from the APN functions known so far (see [25]) by the so-called "switching construction". In particular, they listed 14 CCZ-inequivalent APN functions in dimension six, 19 in dimension seven, and 23 in dimension eight. All but one of them (see [28, Theorem 11]) are either monomial functions or quadratic. For this special case, the authors computed the order of the automorphism group, which is 8. Note that this is the only known example of an APN function which is not CCZ-equivalent to either a monomial function or a quadratic function. This function was discovered independently by Brinkmann and Leander in [8]. Note that in the recent works [11, 12], the authors have found a new class of quadratic APN permutations which lead to new APN functions in dimension 8 and 9. In [11], it was shown that some of the APN functions from [28] can be classified into an infinite class.

In [39], the authors found more than 471 new CCZ-classes of APN functions in dimension seven, and more than 2252 new CCZ-classes in dimension eight. All of them contain a quadratic function, so they admit non-trivial automorphisms. In the PhD thesis [37, Table 23], five new quadratic CCZ-classes of APN functions in dimension 11 were found.

Those are the only known sporadic APN functions we are aware of.

3.6 APN Permutations

An interesting case to consider are APN functions that are at the same time permutations. Note that the property of being a permutation is not invariant under CCZ-equivalence. Actually, not many examples of APN permutations are known. To the best of our knowledge, the known APN permutations fall in either of the following three cases, where the first two cases define infinite families of functions, and the third one a sporadic example which is not classified into an infinite family yet.[2]

1. The APN monomial functions for n odd.
2. The quadratic functions $F\colon \mathbb{F}_{2^{3k}} \mapsto \mathbb{F}_{2^{3k}}, x \mapsto x^{2^s+1} + \omega x^{2^{ik}+2^{tk+s}}$, where s and k are positive integers with k odd, $\gcd(k,3) = \gcd(s,3k) = 1$, $i = sk \mod 3$, $t = 3-i$, and $\omega \in \mathbb{F}_{2^{3k}}^*$ with order $2^{2k} + 2^k + 1$ (Corollary 1 of [14]).
3. The quadratic function $F\colon \mathbb{F}_{2^6} \mapsto \mathbb{F}_{2^6}, x \mapsto x^3 + \alpha x^{24} + x^{10}$, where α is primitive in $\mathbb{F}_{2^6}^*$ (i.e., the CCZ-class of the "Dillon permutation" [9])

The authors of [14] showed that the functions in Class 2 are CCZ-inequivalent to Gold functions when $k \geq 4$. In [38], Yoshiara proved that if a quadratic APN function is CCZ-equivalent to a monomial function, it must be EA-equivalent to a Gold function. Therefore, the functions in Class 2 are CCZ-inequivalent to any monomial function when $k \geq 4$.

For each of the different CCZ-classes coming from the above cases, one can give a representative which is a permutation and admits a non-trivial LE-automorphism. Indeed, the monomial functions are shift-invariant and an LE-automorphism can be given as described in Section 3.2. Class 2 defines a special case of Theorem 1 in [14], which was covered in Example 2 above. Finally, Class 3 is covered by the generalized butterfly structure, described in Section 3.4.

A Conjecture on the Automorphisms of APN Functions and Permutations. For all of the APN functions covered in this section, the automorphism group is non-trivial (remember that the only known non-quadratic function up to CCZ-equivalence has an automorphism group of order 8). Moreover, if it is known that those APN functions are CCZ-equivalent to a permutation, a CCZ-equivalent permutation G can be given with $|\mathsf{Aut}_{\mathsf{LE}}(G)| > 1$. Therefore, we raise the following conjecture.

Conjecture 1. *For an APN function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, it is $|\mathsf{Aut}(F)| > 1$. Moreover, if F is an APN permutation, there exists a CCZ-equivalent permutation G with $|\mathsf{Aut}_{\mathsf{LE}}(G)| > 1$.*

[2] In the GitHub repository [34], Perrin implements an algorithm that checks whether an APN function is CCZ equivalent to a permutation. We tested all cases of APN functions that come from infinite classes in dimension 7 and 9 (see the list in [37] and the new class from [11] and [12]) and all the cases for dimension 7 listed in [28]. Besides the monomial functions, none of them are CCZ-equivalent to a permutation.

In the spirit of this conjecture, we are going to explicitly search for APN permutations with non-trivial LE-automorphisms in small dimensions. In the remainder of this paper, we describe our method for doing this search.

Remark 1. The size of the group of LE-automorphisms is invariant under linear equivalence, but not under affine equivalence. In particular if $|\mathsf{Aut}_{\mathsf{LE}}(F)| > 1$ for a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, then there might exist a constant $c \in \mathbb{F}_2^n$ such that $\mathsf{Aut}_{\mathsf{LE}}(F+c)$ is trivial. For example, this is the case for the 6-bit APN permutation found by Algorithm 1 (see Section 5.1).

More precisely, if $F(0) = 0$, one can show that $\mathsf{Aut}_{\mathsf{LE}}(F+c)$ is a subgroup of $\mathsf{Aut}_{\mathsf{LE}}(F)$ given by

$$\mathsf{Aut}_{\mathsf{LE}}(F+c) = \left\{ \sigma = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \mid \sigma \in \mathsf{Aut}_{\mathsf{LE}}(F) \text{ and } Bc = c \right\} .$$

Remark 2. One can further ask whether for any APN *function*, there exists a representative in its CCZ-class which admits a non-trivial LE-automorphism. We checked that this is the case for any APN function in dimension $n \leq 5$.

4 Equivalences for Permutations with Non-Trivial LE-Automorphisms

If we want to classify all n-bit permutations F (up to CCZ-equivalence) with non-trivial elements

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \in \mathsf{Aut}_{\mathsf{LE}}(F) ,$$

we can significantly reduce the number of tuples (B, A) to consider. The observations in this section result in Corollary 1, which states that for $n \in \{6, 7, 8\}$, we only need to consider $17, 27$, and 32 tuples (B, A), respectively. Note that this classification holds for *any* permutation with a non trivial LE-automorphism, not only for APN permutations.

Let in the following $F \circ A = B \circ F$ for a *function* $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$. For a permutation P on $\mathbb{F}_2^n$, we define $\mathrm{Ord}(P, i) \coloneqq \{x \in \mathbb{F}_2^n \mid P^i(x) = x\}$, which is a subspace of $\mathbb{F}_2^n$.

Lemma 1. *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let A, B be permutations on $\mathbb{F}_2^n$ such that $F \circ A = B \circ F$. Then, for all $i \in \mathbb{N}$,*

$$x \in \mathrm{Ord}(A, i) \quad \Rightarrow \quad F(x) \in \mathrm{Ord}(B, i) .$$

Moreover, if F is a permutation, the converse of the above implication holds.

Proof. Observe that, for all $i \in \mathbb{N}$, $F \circ A^i = B^i \circ F$. If $x \in \mathrm{Ord}(A, i)$, then $F(x) = B^i(F(x))$, thus $F(x) \in \mathrm{Ord}(B, i)$. Let on the other hand $F(x) \in \mathrm{Ord}(B, i)$. Then, $F(x) = F(A^i x)$. Thus, $x = A^i x$ if F is a permutation. □

We only need to consider A and B of prime order, as shown in the following.

Lemma 2. *Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ for which there exists a non-trivial automorphism in $\mathsf{Aut}_{\mathsf{LE}}(F)$. Then, $F \circ A = B \circ F$ with $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$ such that either*

1. $\mathrm{ord}(A) = \mathrm{ord}(B) = p$ *for p prime, or*

2. $A = I_n$ *and* $\mathrm{ord}(B) = p$ *for p prime,or*

3. $B = I_n$ *and* $\mathrm{ord}(A) = p$ *for p prime.*

If F is a permutation, the first of the above conditions must hold.

Proof. Let $g \in \mathsf{Aut}_{\mathsf{LE}}(F)$, $g \neq I_n$. We consider the cyclic subgroup $\langle g \rangle \subseteq \mathsf{Aut}_{\mathsf{LE}}(F)$. From the fundamental theorem of cyclic groups, it contains a cyclic subgroup of prime order. Let this subgroup be generated by

$$h = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

The result follows since $\mathrm{ord}(h) = \mathrm{lcm}(\mathrm{ord}(A), \mathrm{ord}(B))$. If F is a permutation, then $\mathrm{ord}(A) = \mathrm{ord}(B)$ because of Lemma 1. □

Two matrices $M, M' \in \mathrm{GL}(n, \mathbb{F}_2)$ are called *similar*, denoted $M \sim M'$, if there exists a matrix $P \in \mathrm{GL}(n, \mathbb{F}_2)$ such that $M' = P^{-1}MP$. It is well known that similarity defines an equivalence relation. Moreover, we can provide a representative of each equivalence class as follows.

Lemma 3. *(Rational Canonical Form)[26, Page 476] Every matrix $M \in \mathrm{GL}(n, \mathbb{F}_2)$ is similar to a unique matrix $M' \in \mathrm{GL}(n, \mathbb{F}_2)$ of the form*

$$\begin{pmatrix} \mathrm{Comp}(q_r) & & & \\ & \mathrm{Comp}(q_{r-1}) & & \\ & & \ddots & \\ & & & \mathrm{Comp}(q_1) \end{pmatrix}$$

for polynomials q_i such that $q_r \mid q_{r-1} \mid \cdots \mid q_1$. The matrix M' in the form above is called the rational canonical form *of M, denoted* $\mathrm{RCF}(M)$.

If $A' \sim A$ and $B' \sim B$, then there exists a function G which is linear equivalent to F, for which $G \circ A' = B' \circ G$. Therefore, if we are only interested in F up to linear equivalence, it is sufficient to consider A and B in rational canonical form.

We can reduce the search space further if we use the fact that all powers of automorphisms are also automorphisms. Based on this fact, we consider the following equivalence classes for matrices of prime order.

Definition 3. *Let $A, B, C, D \in \mathrm{GL}(n, \mathbb{F}_2)$ be of order p for p prime. The tuple (A, B) is said to be* power similar *to the tuple (C, D), denoted $(A, B) \sim_p (C, D)$, if there exists $i \in \mathbb{N}$ such that $A \sim C^i$ and $B \sim D^i$. The tuple (A, B) is said to be* extended-power similar *to (C, D), denoted $(A, B) \sim_{Ep} (C, D)$, if one of the two following conditions hold:*

1. $(A, B) \sim_p (C, D)$

2. $(A^{-1}, B^{-1}) \sim_p (D, C)$.

Power similarity and extended power similarity defines an equivalence relation on the tuples of matrices in $\mathrm{GL}(n, \mathbb{F}_2^n)$ of the same prime order. Therefore, we can deduce the following lemma.

Lemma 4. *Let $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ with an automorphism*

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \in \mathsf{Aut}_{\mathsf{LE}}(F)$$

for $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$ being of prime order p. For every $(\widetilde{B}, \widetilde{A})$ power similar to (B, A), there is a function G linear equivalent to F such that

$$\begin{bmatrix} \mathrm{RCF}(\widetilde{A}) & 0 \\ 0 & \mathrm{RCF}(\widetilde{B}) \end{bmatrix} \in \mathsf{Aut}_{\mathsf{LE}}(G) \ . \tag{1}$$

Moreover, if F is a permutation, then for every tuple $(\widetilde{B}, \widetilde{A})$ extended-power similar to (B, A), there is such a function G fulfilling Equation 1 and being linear equivalent to either F or F^{-1}.

Proof. Let $A = P^{-1}\widetilde{A}^i P$ and let $B = Q^{-1}\widetilde{B}^i Q$. We have that

$$F \circ A = B \circ F \quad \Leftrightarrow \quad F \circ P^{-1}\widetilde{A}^i P = Q^{-1}\widetilde{B}^i Q \circ F$$

and, thus, for $G \coloneqq Q \circ F \circ P^{-1}$, it is $G \circ \widetilde{A}^i = \widetilde{B}^i \circ G$. Let $k = i^{-1} \mod p$. We have

$$G \circ \widetilde{A}^{ik} = \widetilde{B}^{ik} \circ G \quad \Leftrightarrow \quad G \circ \widetilde{A} = \widetilde{B} \circ G \ .$$

Without loss of generality, $\widetilde{A}$ and $\widetilde{B}$ can be chosen up to similarity. If we chose them in rational canonical form, we obtain the first part of the lemma.

The second part can be obtained by the same argument and using the fact that, for a permutation F, we have $F^{-1} \circ B^{-1} = F^{-1} \circ A^{-1}$. □

Thus, if we want to consider all permutations with a non-trivial linear self equivalence up to CCZ-equivalence (since F is CCZ-equivalent to F^{-1}), we can restrict to tuples (B, A) up to extended-power similarity.

Therefore, combining all the lemmas established in this section, we can enumerate the tuples we need to consider for $n \in \{6, 7, 8\}$ as follows. The code for generating all those tuples can be found at `https://github.com/cbe90/self_equivalent_apn`.

Corollary 1. *Let $n \in \{6, 7, 8\}$. All linear-equivalence classes of permutations $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ or F^{-1} with a non-trivial automorphism*

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \in \mathsf{Aut}_{\mathsf{LE}}(F)$$

can be obtained by considering the following classes for tuples (B, A):

For $n = 6$, we have the 17 classes

1. $B = \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = \mathrm{Comp}(X^6 + X^3 + X^2 + 1)$
2. $B = \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = \mathrm{Comp}(X^6 + X^5 + X^3 + X^2 + X + 1)$
3. $B = \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = \mathrm{Comp}(X^6 + X^5 + X^4 + 1)$
4. $B = A = \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1)$
5. $B = A = \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$
6. $B = A = I_1 \oplus \mathrm{Comp}(X^5 + 1)$
7. $B = I_2 \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \quad A = I_2 \oplus \mathrm{Comp}(X^4 + X^2 + X + 1)$
8. $B = A = I_2 \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1)$
9. $B = A = \mathrm{Comp}(X^3 + 1) \oplus \mathrm{Comp}(X^3 + 1)$
10. $B = \mathrm{Comp}(X^3 + X^2 + 1) \oplus \mathrm{Comp}(X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$
11. $B = \mathrm{Comp}(X^3 + X^2 + 1) \oplus \mathrm{Comp}(X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^3 + X + 1) \oplus \mathrm{Comp}(X^3 + X + 1)$
12. $B = A = \mathrm{Comp}(X^3 + X^2 + 1) \oplus \mathrm{Comp}(X^3 + X^2 + 1)$
13. $B = A = I_3 \oplus \mathrm{Comp}(X^3 + 1)$
14. $B = A = \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$
15. $B = A = \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^2 + X + 1)$
16. $B = A = I_2 \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$
17. $B = A = I_4 \oplus \mathrm{Comp}(X^2 + 1)$.

For $n = 7$, we have the 27 classes

1. $B = A = \mathrm{Comp}(X^7 + 1)$
2. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^3 + 1)$
3. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^5 + X^3 + X + 1)$
4. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^5 + X^4 + X^3 + X^2 + X + 1)$
5. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^6 + 1)$
6. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^6 + X^4 + X + 1)$
7. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^6 + X^5 + X^2 + 1)$

8. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^6 + X^5 + X^3 + X^2 + X + 1)$

9. $B = \mathrm{Comp}(X^7+X^6+X^5+X^4+X^3+X^2+1) \quad A = \mathrm{Comp}(X^7+X^6+X^5+X^4+1)$

10. $B = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^2 + X + 1)$

11. $B = A = \mathrm{Comp}(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1)$

12. $B = I_1 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = I_1 \oplus \mathrm{Comp}(X^6 + X^3 + X^2 + 1)$

13. $B = I_1 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = I_1 \oplus \mathrm{Comp}(X^6 + X^5 + X^3 + X^2 + X + 1)$

14. $B = I_1 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = I_1 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + 1)$

15. $B = A = I_1 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1)$

16. $B = A = I_2 \oplus \mathrm{Comp}(X^5 + 1)$

17. $B = \mathrm{Comp}(X^3 + X + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^7 + 1)$

18. $B = \mathrm{Comp}(X^3 + X + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^3 + X^2 + 1) \oplus \mathrm{Comp}(X^4 + X^2 + X + 1)$

19. $B = A = \mathrm{Comp}(X^3 + X + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1)$

20. $B = I_3 \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \quad A = I_3 \oplus \mathrm{Comp}(X^4 + X^2 + X + 1)$

21. $B = A = I_3 \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1)$

22. $B = A = I_1 \oplus \mathrm{Comp}(X^3 + 1) \oplus \mathrm{Comp}(X^3 + 1)$

23. $B = A = \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^3 + 1)$

24. $B = A = I_4 \oplus \mathrm{Comp}(X^3 + 1)$

25. $B = A = I_1 \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$

26. $B = A = I_3 \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$

27. $B = A = I_5 \oplus \mathrm{Comp}(X^2 + 1)$.

For $n = 8$, we have the 32 classes

1. $B = \mathrm{Comp}(X^8+X^7+X^6+X^4+X^2+X+1) \quad A = \mathrm{Comp}(X^8+X^5+X^4+X^3+1)$

2. $B = A = \mathrm{Comp}(X^8 + X^7 + X^6 + X^4 + X^2 + X + 1)$

3. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^6 + X^4 + X^3 + X^2 + 1)$

4. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^6 + X^5 + X^4 + X^2 + 1)$

5. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$

6. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^7 + X^4 + X^3 + X + 1)$

7. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^7 + X^5 + X^2 + X + 1)$

8. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^7 + X^5 + X^4 + X + 1)$

9. $B = \mathrm{Comp}(X^8+X^7+X^6+X^5+X^4+X^3+X^2+1) \quad A = \mathrm{Comp}(X^8+X^7+X^6+1)$

10. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^7 + X^6 + X^3 + X + 1)$

11. $B = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^3 + 1)$

12. $B = A = \mathrm{Comp}(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + 1)$

13. $B = A = I_1 \oplus \mathrm{Comp}(X^7 + 1)$

14. $B = I_2 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = I_2 \oplus \mathrm{Comp}(X^6 + X^3 + X^2 + 1)$

15. $B = I_2 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = I_2 \oplus \mathrm{Comp}(X^6 + X^5 + X^3 + X^2 + X + 1)$

16. $B = I_2 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1) \quad A = I_2 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + 1)$

17. $B = A = I_2 \oplus \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X + 1)$

18. $B = A = I_3 \oplus \mathrm{Comp}(X^5 + 1)$

19. $B = \mathrm{Comp}(X^4+X^3+X^2+1) \oplus \mathrm{Comp}(X^4+X^3+X^2+1) \quad A = I_1 \oplus \mathrm{Comp}(X^7+1)$

20. $B = \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \quad A = \mathrm{Comp}(X^4 + X^2 + X + 1) \oplus \mathrm{Comp}(X^4 + X^2 + X + 1)$

21. $B = A = \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1)$

22. $B = A = \mathrm{Comp}(X^4 + X^3 + X^2 + X + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + X + 1)$

23. $B = I_4 \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1) \quad A = I_4 \oplus \mathrm{Comp}(X^4 + X^2 + X + 1)$

24. $B = A = I_4 \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + 1)$

25. $B = A = \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^3 + 1) \oplus \mathrm{Comp}(X^3 + 1)$

26. $B = A = I_2 \oplus \mathrm{Comp}(X^3 + 1) \oplus \mathrm{Comp}(X^3 + 1)$

27. $B = A = I_5 \oplus \mathrm{Comp}(X^3 + 1)$

28. $B = A = \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$

29. $B = A = \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^2 + X + 1)$

30. $B = A = I_2 \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$

31. $B = A = I_4 \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$

32. $B = A = I_6 \oplus \mathrm{Comp}(X^2 + 1)$.

Note that, when searching for permutations in one of the above classes, we can reduce the search space further by filtering candidates up to affine equivalence as follows. For a matrix $M \in \mathrm{GL}(n, \mathbb{F}_2)$, let $\mathrm{Comm}(M)$ denote the subgroup of $\mathrm{GL}(n, \mathbb{F}_2)$ of all matrices that commute with M.

Lemma 5. *Let $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$ such that $F \circ A = B \circ F$. Then, $G \circ A = B \circ G$ for any $G = C_B \circ F \circ C_A$ with $C_A \in \mathrm{Comm}(A)$ and $C_B \in \mathrm{Comm}(B)$.*

This allows us to only consider one representative within the class of $\mathrm{Comm}(B) \circ F \circ \mathrm{Comm}(A)$.

5 Searching for APN Permutations with Non-Trivial LE-Automorphisms

We now use the classification of tuples from Corollary 1 to explicitly search for APN permutations with non-trivial linear self-equivalences in dimensions $n \in \{6, 7, 8\}$. First, we observe that not all of the tuples (B, A) obtained in Corollary 1 have to be considered in the search.

Definition 4. *Let $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$. A tuple (B, A) is* admissible *if there exists an APN permutation $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $F \circ A = B \circ F$.*

The following two propositions imply necessary conditions for a tuple to be admissible.

Proposition 4. *Let $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation that is APN. Let $A_1, A_2 \subseteq \mathbb{F}_2^n$ be two affine spaces such that $F(A_1) = A_2$. Then, $\dim A_i \notin \{2, 4, n-1\}$.*

Proof. Let $d = \dim A_1 = \dim A_2$. Without loss of generality, we can choose $A_1 = A_2 = \mathbb{F}_2^d \times \{0\}^{n-d}$ by considering an affine equivalent permutation F' of F. Because F' is APN, the property $F'(A_1) = A_2$ implies the existence of an APN permutation in dimension d. This cannot happen for $d = 2$ and $d = 4$, see [31]. The case of $d = n - 1$ was shown in [31, Proposition 2.1]. □

Therefore, if $(B, A) \in \mathrm{GL}(n, \mathbb{F}_2) \times \mathrm{GL}(n, \mathbb{F}_2)$ is an admissible tuple, we have that $\dim \mathrm{Ord}(A, i) = \dim \mathrm{Ord}(B, i) \notin \{2, 4, n-1\}$ for all $i \in \mathbb{N}$.

Proposition 5. *Let $(B, A) \in \mathrm{GL}(n, \mathbb{F}_2) \times \mathrm{GL}(n, \mathbb{F}_2)$ be an admissible tuple with $\mathrm{ord}(A) = \mathrm{ord}(B) = k$ for k prime. Then, there exists no 4-nomial in $\mathbb{F}_2[X]/(X^k - 1)$ which is a multiple of both the minimal polynomial of A and the minimal polynomial of B.*

Proof. Suppose there is such a 4-nomial $p = X^a + X^b + X^c + 1$. Then, both $A^a + A^b = A^c + 1$ and $B^a + B^b = B^c + 1$ hold. Let $g \in \mathbb{F}_2$ be an element with $\mathrm{ord}_A(g) = k$ and let F be a permutation that fulfills the self-equivalence for (B, A). We have

$$\begin{aligned} F(A^a g) + F(A^b g) = B^a F(g) + B^b F(g) &= (B^a + B^b) F(g) \\ &= (B^c + 1) F(g) = F(A^c g) + F(g) \ , \end{aligned}$$

which implies that F cannot be APN. □

The following statement is a variant of the above proposition for monomial functions.

Proposition 6. *Let $F(x) = x^d$ be a permutation over $\mathbb{F}_{2^n}$. Then, F is APN if and only if there exists no 4-nomial $p \in \mathbb{F}_2[X]/(X^{2^n-1} + 1)$ such that both p and p^d are multiples of the same primitive polynomial $f \in \mathbb{F}_2[x]/(X^{2^n-1} + 1)$.*

Depth-First Tree Search Algorithm. Using the above propositions, for some of the tuples given in Corollary 1 we can directly say that they are not admissible. For the other tuples, we can check their admissibility by the recursive depth-first tree search described in Algorithm 1 at the end of the paper.

It gets as input two matrices $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$ and constructs the look-up tables of all n-bit APN permutations F with $F \circ A = B \circ F$ up to linear equivalence. To reduce the search space according to Lemma 5, we provide a subset of $C_A \subseteq \mathrm{Comm}(A)$ and a subset $C_B \subseteq \mathrm{Comm}(B)$ as additional inputs. The idea is that the algorithm should output only the *smallest* representative of an APN permutation up to conjugation with elements in C_A, resp. C_B, where the term *smallest* refers to some lexicographic ordering of the look-up table.[3]

At the beginning of the search, the look-up table is initialized to $\perp$ at each point, where $\perp$ indicates that the respective point is not yet defined. At the beginning of each iteration of the recursive NextVal procedure, it is checked whether the look-up table is completely defined, i.e., whether it contains no more $\perp$. If it is completely defined, the look-up table will be appended to the list of solutions and the procedure returns. Otherwise, it chooses the next undefined point x in the look-up table (according to some previously defined ordering) and sets it to the next value y (also according to some previously defined ordering) which does not yet occur in the look-up table and for which $\mathrm{ord}_A(x) = \mathrm{ord}_B(y)$. Besides fixing $F(x) := y$, the algorithm further fixes

[3] The check for being the smallest representative is omitted if the depth exceeds some threshold t, because at some depth it is faster to just traverse the remaining tree. Therefore, it might happen that the algorithm outputs more representatives than just the smallest.

all $F(A^i(x)) := B^i(y)$ according to the self-equivalence. For each point that is fixed, it will be checked whether the partially-defined function can still be APN (procedure IsAPN). In case that there is already a contradiction with the property of being APN, the corresponding branch is pruned and the point x is set to the next possible value y. In case that the partially-defined function can still be APN, the algorithm iterates to the next depth.

APN Check. The description of Alg. 1 is a bit simplified. Instead of checking for each new fixing of a point whether the partially-defined function can still be APN (for example by constructing the difference distribution table (DDT) partially), we use a global two-dimensional array of size $2^n \times 2^n$ that dynamically stores the partial DDT. After each point of F is fixed, we update the partial DDT according to the new set point and check whether it contains values larger than 2 (in that case, F cannot be APN). If a point is reset to $\perp$ (line 32), the DDT array has to be updated accordingly.

For a further speed-up, note that we do not have to consider the whole DDT for the APN check. As it was shown in [2, Theorem 4], only those DDT entries corresponding to input differences with even Hamming Weight have to be computed.

5.1 Results for $n = 6$

By Propositions 4 and 5, we directly obtain that 8 out of the 17 tuples given in Corollary 1 are not admissible (see Table 1). We *exhaustively* searched the remaining 9 tuples using Algorithm 1. The case of

$$B = A = \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \tag{2}$$

(Class 14) was the most difficult one. A, resp., B is an involution and therefore only consists of cycles of length 1 and 2, which causes Alg. 1 to be less efficient. However, since A, resp. B has 8 fixed points, we can w.l.o.g. set F on the fixed points of A to the only existing APN permutation on 3-bit up to affine equivalence. This trick allowed us to finish this case within roughly 8 core hours on a standard CPU. Only for the case

$$B = A = \mathrm{Comp}(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1) \tag{3}$$

(Class 5), APN permutations exist and they are all CCZ-equivalent to Dillon's permutation. To conclude, we have shown the following.

Theorem 1. *Up to CCZ-equivalence, there is only one APN permutation F in dimension 6 with $|\mathsf{Aut}_{\mathsf{LE}}(F)| > 1$.*

5.2 Results for $n = 7$

By Propositions 4 and 5, we directly obtain that 13 out of the 27 tuples given in Corollary 1 are not admissible. We exhaustively searched through 11 of the remaining 14 tuples using Algorithm 1.

Algorithm 1 APNsearch

Require: Matrices $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$, $C_A \subseteq \mathrm{Comm}(A), C_B \subseteq \mathrm{Comm}(B)$. Global array sbox of size 2^n, initialized to $\mathrm{sbox}[i] = \perp$, for all $i \in \{0, \ldots, 2^n - 1\}$

Ensure: All n-bit APN permutations F s.t. $FA = BF$ up to linear equivalence.

```
 1: $L \leftarrow \{\}, \quad \mathrm{sbox}[0] \leftarrow 0$
 2: nextVal(0)
 3: return $L$

 4: function nextVal(depth)
 5:     if isComplete(sbox) then
 6:         $L \leftarrow L \cup \{\mathrm{sbox}\}$
 7:         return
 8:     end if
 9:     $x \leftarrow$ nextFreePosition()
10:     for $y \in \mathbb{F}_2^n$ do
11:         if isNotTaken($y$) and $\mathrm{ord}_A(x) = \mathrm{ord}_B(y)$ then
12:             $xS \leftarrow x, \quad xY \leftarrow y$
13:             for $i = 0$ to $\mathrm{ord}_A(x) - 2$ do
14:                 $\mathrm{sbox}[xS] \leftarrow yS$
15:                 if not isAPN(sbox) then
16:                     go to 31
17:                 end if
18:                 $xS \leftarrow A(xS), \quad yS \leftarrow B(yS)$
19:             end for
20:             $\mathrm{sbox}[xS] \leftarrow yS$
21:             if not isAPN(sbox) then
22:                 go to 31
23:             end if
24:             if depth $\leq t$ then
25:                 if isSmallest(sbox) then
26:                     nextVal(depth + 1)
27:                 end if
28:             else
29:                 nextVal(depth + 1)
30:             end if
31:             repeat
32:                 $\mathrm{sbox}[xS] \leftarrow \perp$
33:                 $xS \leftarrow A^{-1}(xS)$
34:             until $xS = A^{-1}(x)$
35:         end if
36:     end for
37: end function
```

Table 1: Analysis of the tuples (B, A) given in Corollary 1. "No." corresponds to the number of the tuple in Corollary 1. The column "admissible" indicates whether there exists an n-bit APN permutation F for which $F \circ A = B \circ F$. In case that it does, we list *all* the solutions for the CCZ classes of such F. The "?" indicates that we were not able to either exclude the tuple by Prop. 4 or 5, or to finish the exhaustive search for F.

$n = 6$			$n = 7$			$n = 8$	
No.	admissible	solutions	No.	admissible	solutions	No.	admissible
1	no (Alg. 1)		1	yes	$x \mapsto x^5$ $x \mapsto x^9$ $x \mapsto x^{63}$ $x \mapsto x^{78}$ $x \mapsto x^{85}$ $x \mapsto x^{88}$	1	no (Alg. 1)
2	no (Alg. 1)		2	no (Prop. 5)		2	no (Alg. 1)
3	no (Alg. 1)		3	no (Prop. 5)		3	no (Prop. 5)
4	no (Prop. 5)		4	yes	$x \mapsto x^{63}$	4	no (Alg. 1)
5	yes	"Dillon" [9]	5	yes	$x \mapsto x^9$	5	no (Alg. 1)
6	no (Prop. 4)		6	no (Prop. 5)		6	no (Alg. 1)
7	no (Alg. 1)		7	yes	$x \mapsto x^5$	7	no (Prop. 5)
8	no (Prop. 5)		8	yes	$x \mapsto x^{78}$	8	no (Alg. 1)
9	no (Prop. 4)		9	yes	$x \mapsto x^{85}$	9	no (Alg. 1)
10	no (Alg. 1)		10	yes	$x \mapsto x^{88}$	10	no (Alg. 1)
11	no (Alg. 1)		11	no (Prop. 5)		11	no (Prop. 5)
12	no (Prop. 5)		12	no (Prop. 4)		12	no (Prop. 5)
13	no (Prop. 4)		13	no (Prop. 4)		13	no (Prop. 4)
14	no (Alg. 1)		14	no (Prop. 4)		14	no (Alg. 1)
15	no (Alg. 1)		15	no (Prop. 4)		15	no (Alg. 1)
16	no (Prop. 4)		16	?		16	no (Alg. 1)
17	no (Prop. 4)		17	no (Alg. 1)		17	no (Prop. 5)
			18	no (Alg. 1)		18	no (Prop. 4)
			19	no (Prop. 5)		19	no (Prop. 4)
			20	no (Prop. 4)		20	no (Prop. 4)
			21	no (Prop. 4)		21	no (Prop. 4)
			22	?		22	?
			23	?		23	no (Alg. 1)
			24	no (Alg. 1)		24	no (Prop. 5)
			25	no (Prop. 4)		25	no (Prop. 4)
			26	no (Alg. 1)		26	no (Prop. 4)
			27	no (Prop. 4)		27	no (Alg. 1)
						28	no (Prop. 4)
						29	no (Alg. 1)
						30	no (Alg. 1)
						31	no (Alg. 1)
						32	no (Prop. 4)

Class 1 corresponds to the shift-invariant permutations, which obviously contains all the monomial permutations. By letting Alg. 1 run for several days on a cluster with 256 cores, we were able to finish the search for APN permutations in this class. We obtained that the APN monomial permutations are the *only* shift-invariant APN permutations.

Theorem 2. *Up to CCZ-equivalence, a shift-invariant APN permutation in dimension 7 must be a monomial function.*

The 6 APN monomial permutations in dimension 7 are also contained in Classes 4, 5, 7, 8, 9, and 10, respectively. Those classes correspond to tuples (B, A), where A and B correspond to multiplications by elements in the finite field $\mathbb{F}_{2^7}$. No more APN permutation have been found. This leads us to state the following theorem.

Theorem 3. *Let F be an APN permutation in dimension 7 with $|\mathsf{Aut}_{\mathsf{LE}}(F)| > 1$ and which is not CCZ-equivalent to a monomial function. Then, F is CCZ-equivalent to a permutation G for which $G \circ A = B \circ G$ with*

1. $B = A = I_2 \oplus \mathrm{Comp}(X^5 + 1)$ *or*
2. $B = A = I_1 \oplus \mathrm{Comp}(X^3 + 1) \oplus \mathrm{Comp}(X^3 + 1)$ *or*
3. $B = A = \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^2 + X + 1) \oplus \mathrm{Comp}(X^3 + 1)$.

5.3 Results for $n = 8$

By Propositions 4 and 5, we directly obtain that 15 out of the 32 tuples given in Corollary 1 are not admissible. We exhaustively searched through 16 of the remaining 17 tuples using Algorithm 1. No APN permutation have been found. To complete the search for Class 30, similarly to Class 14 in the 6-bit case, we set F on the 32 fixed points of A (resp. B) to an APN permutation on 5-bit. Since there are exactly five 5-bit APN permutations up to affine equivalence [8], this has to repeated 5 times. To conclude, we state the following theorem.

Theorem 4. *Let F be an APN permutation in dimension 8 with $|\mathsf{Aut}_{\mathsf{LE}}(F)| > 1$. Then, F is CCZ-equivalent to a permutation G for which $G \circ A = B \circ G$ with*

$$B = A = \mathrm{Comp}(X^4 + X^3 + X^2 + X + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + X + 1) .$$

Table 1 summarizes our results. The source code of our implementation of Alg. 1 can be found at `https://github.com/cbe90/self_equivalent_apn`. For checking whether a found solution is CCZ-equivalent to an already known APN permutation, we used the equivalent condition on code equivalence as explained in [9]. Practically, we used the code equivalence algorithm of the computer algebra system Magma [4], which for $n = 7$ takes a few seconds on a standard PC.

5.4 Randomized Search

In case that the search space for a tuple (B, A) is too large such that Alg. 1 is not going to terminate in reasonable time, we can randomly search for APN permutations F for which $F \circ A = B \circ F$. Indeed, it is straightforward to implement a randomized version of Algorithm 1. For that, before the initial call of NextVal, we randomly shuffle the order in which the values for y are iterated in line 10. We abort the search after a previously-defined amount of time and repeat with a new initial shuffling. Further, since we are not aiming for an *exhaustive* search, we omit the check for the smallest representative, i.e., set t to -1.

We applied the randomized search for the 4 tuples for which we were not able to finish the exhaustive search, i.e., Classes 16, 22, and 23 for $n = 7$, and Class 22 for $n = 8$. No APN permutations have been found by letting the algorithm run for one week on 32 cores for each of those cases.

6 Conclusion and Open Questions

We observed that all APN permutations known from the literature contain a permutation in their CCZ-class that admit a non-trivial linear self equivalence. We performed an exhaustive search for 6-bit APN permutations with such non-trivial linear self equivalences and a partial search in dimension 7 and 8. Although we did not find any new APN permutations, we think that our work contributes to the knowledge of APN permutations in small dimensions.

We expect that there are no more APN permutations with non-trivial linear self-equivalences in dimension 7 and 8. As open problems, it would be interesting to settle the cases described in Theorem 3 and 4, i.e., to show that those cases contain no APN permutations. Another (very ambitious) open problem is to prove or disprove Conjecture 1. This would certainly be considered a major breakthrough in the theory of APN functions.

Acknowledgment

We thank Anne Canteaut, Yann Rotella and Cihangir Tezcan for fruitful discussions at an early stage of this project.

References

[1] R. Arshad. *Contributions to the theory of almost perfect nonlinear functions.* PhD thesis, Otto-von-Guericke-Universität Magdeburg, 2018.

[2] T. Beth and C. Ding. On almost perfect nonlinear permutations. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 65–76. Springer, 1993.

[3] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] C. Bracken, E. Byrne, N. Markin, and G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.

[6] C. Bracken, E. Byrne, N. Markin, and G. McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[7] C. Bracken, E. Byrne, G. McGuire, and G. Nebe. On the equivalence of quadratic APN functions. *Des. Codes Cryptogr.*, 61(3):261–272, 2011.

[8] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptogr.*, 49(1-3):273–288, 2008.

[9] K. Browning, J. Dillon, M. McQuistan, and A. Wolfe. An APN permutation in dimension six. *Finite Fields: theory and applications*, 518:33–42, 2010.

[10] L. Budaghyan. The simplest method for constructing APN polynomials EA-inequivalent to power functions. In C. Carlet and B. Sunar, editors, *Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings*, volume 4547 of *Lecture Notes in Computer Science*, pages 177–188. Springer, 2007.

[11] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa. Generalized isotopic shift construction for APN functions. Cryptology ePrint Archive, Report 2020/295, 2020. https://eprint.iacr.org/2020/295.

[12] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, and I. Villa. Constructing APN functions through isotopic shifts. *IEEE Trans. Information Theory*, 2020. Advance online publication.

[13] L. Budaghyan and C. Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Trans. Information Theory*, 54(5):2354–2357, 2008.

[14] L. Budaghyan, C. Carlet, and G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Trans. Information Theory*, 54(9):4218–4229, 2008.

[15] L. Budaghyan, C. Carlet, and G. Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[16] L. Budaghyan, C. Carlet, and G. Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378, Oct 2009.

[17] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Trans. Information Theory*, 52(3):1141–1152, 2006.

[18] L. Budaghyan, T. Helleseth, and N. S. Kaleyski. A new family of APN quadrinomials. Cryptology ePrint Archive, Report 2019/994, 2019. `https://eprint.iacr.org/2019/994`.

[19] A. Canteaut, S. Duval, and L. Perrin. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. *IEEE Trans. Information Theory*, 63(11):7575–7591, 2017.

[20] A. Canteaut and L. Perrin. On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields and Their Applications*, 56:209–246, 2019.

[21] C. Carlet. Vectorial Boolean functions for cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469, 2010.

[22] C. Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Des. Codes Cryptogr.*, 59(1-3):89–109, 2011.

[23] L. Carlitz and D. Hayes. Permutations with coefficients in a subfield. *Acta Arithmetica*, 21(1):131–135, 1972.

[24] C. De Cannière. *Analysis and design of symmetric encryption algorithms.* PhD thesis, KULeuven, 2007.

[25] J. F. Dillon. APN polynomials and related codes. Banff International Research Station workshop on Polynomials over Finite Fields and Applications, 2006.

[26] D. S. Dummit and R. M. Foote. *Abstract algebra.* John Wiley and Sons, Inc., 2004.

[27] Y. Edel, G. M. M. Kyureghyan, and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Information Theory*, 52(2):744–747, 2006.

[28] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. in Math. of Comm.*, 3(1):59–81, 2009.

[29] T. Feulner. The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes. *Adv. in Math. of Comm.*, 3(4):363–383, 2009.

[30] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Information Theory*, 14(1):154–156, 1968.

[31] X. Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Discrete Applied Mathematics*, 154(2):313–325, 2006.

[32] K. Nyberg. Differentially uniform mappings for cryptography. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1993.

[33] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In E. F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 566–574. Springer, 1992.

[34] L. Perrin. sboxU. *GitHub repository*, 2017. Availabe via `https://github.com/lpp-crypto/sboxU`, commit fb8941790ce6850d9fbdee3334ca2e2d381fb24c.

[35] L. Perrin, A. Udovenko, and A. Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In M. Robshaw and J. Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 93–122. Springer, 2016.

[36] N. J. A. Sloane (editor). The on-line encyclopedia of integer sequences. Sequence A326932, published electronically at `https://oeis.org`, 2019.

[37] B. Sun. *On Classification and Some Properties of APN Functions*. PhD thesis, University of Bergen, 2018.

[38] S. Yoshiara. Equivalences of power APN functions with power or quadratic APN functions. *Journal of Algebraic Combinatorics*, 44(3):561–585, Nov 2016.

[39] Y. Yu, M. Wang, and Y. Li. A matrix approach for constructing quadratic APN functions. *Des. Codes Cryptogr.*, 73(2):587–600, 2014.

[40] Y. Zhou and A. Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43 – 60, 2013.