Des. Codes Cryptogr.
DOI 10.1007/s10623-010-9365-0

Some results concerning cryptographically significant mappings over GF(2^n)

E. Pasalic · P. Charpin

Received: 17 August 2009 / Revised: 6 November 2009 / Accepted: 15 January 2010

Abstract In this paper we investigate the existence of permutation polynomials of the form $F(x) = x^d + L(x)$ over GF(2^n), L being a linear polynomial. The results we derive have a certain impact on the long-term open problem on the nonexistence of APN permutations over GF(2^n), when n is even. It is shown that certain choices of exponent d cannot yield APN permutations for even n. When n is odd, an infinite class of APN permutations may be derived from Gold mapping x^3 in a recursive manner, that is starting with a specific APN permutation on GF(2^k), k odd, APN permutations are derived over GF(2^{k+2i}) for any $i \geq 1$. But it is demonstrated that these classes of functions are simply affine permutations of the inverse coset of the Gold mapping x^3. This essentially excludes the possibility of deriving new EA-inequivalent classes of APN functions by applying the method of Berveglieri et al. (approach proposed at Asiacrypt 2004, see [3]) to arbitrary APN functions.

Keywords Permutation polynomials · Power mappings · APN functions · S-box · EA-equivalence · CCZ-equivalence

Mathematics Subject Classification (2000): 94A60

Communicated by Daniel Panario.

This is an extended and modified version of the manuscript presented at WAIFI 08, International Conference on the Arithmetic of Finite Fields, Siena, Italy, July 6-9, 2008.

E. Pasalic (✉)
IMFM Ljubljana & University of Primorska, Koper, Slovenia
e-mail: enespasalic@yahoo.se

P. Charpin
INRIA, projet SECRET, Domaine de Voluceau, Rocquencourt, BP 105, Le Chesnay Cedex 78153, France
e-mail: Pascale.Charpin@inria.fr

Published online: 06 February 2010

1 Introduction

Differential cryptanalysis introduced in [2], together with linear cryptanalysis [24] are considered as the most efficient cryptanalyst tools for block ciphers. Commonly, the security of modern block ciphers substantially relies on the cryptographic properties of its substitution boxes (S-boxes), which are in most of the cases the only source of nonlinearity. These S-boxes are most often constructed by means of certain well-known power mappings that have relatively good cryptographic properties such as high nonlinearity, high algebraic degree and good differential characteristics.

To satisfy the diverse cryptographic criteria, a cryptographically strong S-box can be taken from the class of almost perfect nonlinear (APN) permutations. In addition it should have good algebraic properties, so that low degree input/output (I/O) relations do not exist. However, almost all families of APN functions have been derived from power polynomials, that is $F(x) = x^d$ over the field GF(2^n) for a suitably chosen d. Unfortunately, when n is even, it has been a long-term open problem to prove the nonexistence of APN permutations over GF(2^n).

One of the major achievements in this context is the result of Hou [19] showing that an APN function F, $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, cannot be a permutation if $a_i \in \mathbb{F}_{2^{n/2}}$ and n is even. Quite recently, Dillon [15] succeeded in finding a first instance of APN permutation polynomial over GF(64). This result, though of outstanding theoretical importance, does not solve the question related to efficient construction or finding new classes of APN permutations when n is even. Indeed, until today no further examples of APN permutations have been exhibited.

Our idea is to investigate the conditions for $F_d(x) = x^d + L(x)$ to be a permutation. Then, showing that F_d cannot be a permutation for some d we also exclude the possibility of turning a non-permuting APN function x^d into permutation by adding a linear function to it. An instance of this problem was recently studied in [12]. Also the case of permutations F such that $x \mapsto F(x) + x$ remains a permutation was already studied. These permutations are called *complete* permutations [25].

To preserve good differential and linear properties, we may attempt to find instances (or classes) of polynomials derived from power monomials that have better algebraic properties than power monomials. It is well-known that the differential and linear properties of the power permutation $F(x) = x^d$ are the same as for $x^{2d}, x^{4d}, \dots, x^{2^{n-1}d}$. The same is true for the inverse cyclotomic coset $x^{2/d}, x^{4/d}, \dots, x^{2^{n-1}/d}$ if x^d is a bijection, see e.g. [17]. Of course, the exponents of these mappings are reduced mod $2^n - 1$. While $x^{2^i d}$ is of the same algebraic degree as x^d, this is not the case for the inverse cyclotomic coset as $x^{2^i/d}$ has in general different algebraic degree than x^d.

The linear transformation is embedded in the so-called *extended affine equivalence* (EA-equivalence) so that F and F' are EA-equivalent if $F' = A_1 \circ F \circ A_2 + A$ for some affine permutations A_1, A_2 and affine function A. A more general equivalence that we term just equivalence (following the terminology in [7]) also includes the inverse coset by replacing F with F^{-1}. Nevertheless, the EA-equivalence in general does not apply to the inverse cyclotomic coset. This means that transforming F into F' by means of the existence of A, A_1, A_2 does not necessarily imply that we can retrieve F from F^{-1} by applying the above affine transformation for some $\tilde{A}, \tilde{A}_1, \tilde{A}_2$.

A more general framework was first introduced in [8], where the transformation is applied rather to the graph of functions. Then $F, F' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called CCZ-equivalent, terminology introduced in [5], if the sets $G_F = \{(x, F(x)) | x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) | x \in \mathbb{F}_{2^n}\}$

are affine equivalent. It was shown in [8] that EA-equivalence is a particular case of CCZ-equivalence, and both equivalence relations preserve (up to permutation) the differential table and the extended Walsh spectra. Furthermore, the strength to algebraic cryptanalysis (admittance of low degree I/O equations) is invariant to both equivalence relations. Nevertheless, certain classes of AB (APN) functions derived by applying the CCZ transformation cannot be obtained via classical EA-equivalence [4].

The research on the classification of functions with respect to the above equivalence classes has received a lot of attention, see e.g. [4,5,18]. At Asiacrypt 2004, Breveglieri et al. in the paper "On generalized linear equivalence of functions over finite fields" introduced a new class of APN permutations derived from Gold mapping $F(x) = x^3$ for which the conjecture was made that this class was EA-inequivalent to any power mapping. Later this statement was corrected not to hold over $\mathbb{F}_{2^3}$ due to the small size of the field (first revision), and eventually the statement was completely withdrawn by the authors in the second revision [23]. Using an approach based on matrix theory it was shown that the class of functions introduced in [3] is EA-equivalent to the inverse mapping of x^3. Here we give a simplified proof of this fact at the same time specifying the particular affine transformation. More importantly, the possibility of constructing APN permutations in a recursive manner, that was only verified by computer in [26], is formally proved here using the number theory. To the best of our knowledge we are not aware of any other examples of constructing APN permutations recursively, that is starting with an APN permutation over GF(2^{2k-1}) one may define an APN permutation over a field GF($2^{2k+2i-1}$) for any $i > 0$ using a simple recursive formulae.

The rest of the paper is organized as follows.[1] Section 2 introduces basic definitions and concepts. The nonexistence of certain classes of permutations and the implication of this result to the APN conjecture is treated in Sect. 3. In Sect. 4, we disprove the statement of Breveglieri et al. [23] on the possibility of deriving new classes of functions EA-nonequivalent to power monomials. The recursive property of APN permutations derived from the Gold mapping x^3 is explained. Section 5 concludes the paper.

2 Preliminaries

In the sequel $\mathbb{F}_{2^n}$ will denote the Galois field of 2^n elements.

The *polynomial degree*, denoted by deg_p, associated to $P(x) = \sum_i a_i x^i$ is defined as the largest i for which a_i is nonzero. Any mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be viewed as a mapping $F' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by fixing the isomorphism between the vector space $\mathbb{F}_2^n$ and the field $\mathbb{F}_{2^n}$. If we represent the function F as a function on the vector space $\mathbb{F}_2^n$, then we may consider this function as being a collection of n Boolean functions $f_1, \ldots, f_n$, that is, $F' = (f_1, \ldots, f_n)$, where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$. The algebraic degree of F' when defined as a global degree of F' implies the following definition.

Definition 1 The algebraic degree of F' is defined as,

$$deg(F') = \max_j deg(f_j(x)), \tag{1}$$

where $deg(f)$ denotes the usual algebraic degree of a Boolean function f, that is, the highest length of the terms that appear in the algebraic normal form of f.

[1] In the manuscript published in conference proceedings of WAIFI 08 [26], there is a section that contains a polynomial time algorithm for finding low degree input/output relations for sparse polynomials over finite fields. The interested reader is therefore referred to the manuscript in the conference proceedings [26] for the details regarding this algorithm.

A related notion that even better captures the cryptographic properties of F' is so-called *minimum degree*.

Definition 2 The minimum degree of F' is defined as,

$$deg(F') = \min_{\tau \in \mathbb{F}_2^{n*}} deg\left(\sum_{j=1}^{n} \tau_j f_j(x)\right). \tag{2}$$

In most of the cryptographic applications the minimum degree of high order is an essential criterion, as otherwise it might be the case that certain linear combinations of the inputs induce simple (low degree) input/output relations.

The algebraic degree may also be deduced from the polynomial representation. That is, for a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ represented as $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, the algebraic degree is given by

$$deg(F) = \max_i \{wt(i); a_i \neq 0\}, \tag{3}$$

where $wt(i)$ denotes the Hamming weight (number of ones) in a binary representation of integer i. Also for a function $F(x, y) : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, where $F(x, y) = \sum_{i,j=0}^{2^n-1} a_{i,j} x^i y^j$, the algebraic degree is defined as,

$$deg(F) = \max_{i,j} \{wt(i) + wt(j); a_{i,j} \neq 0\}, \tag{4}$$

The differential properties of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are visualized through so-called differential table that for each $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$ consists of the number of solutions to the following equation,

$$F(x + a) + F(x) = b \quad a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}. \tag{5}$$

Then, a function F is called *almost perfect nonlinear* (APN) if each equation (5) has at most two solutions in $\mathbb{F}_{2^n}$ and such a function has a highest resistance to differential cryptanalysis. The differential properties of F are then comprised through the differential table,

$$\{\delta_F(a, b)\} = \{|\{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}|; a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}.$$

The nonlinearity of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and hereby the resistance to linear cryptanalysis of Matsui [24] is measured through extended Walsh transform defined as,

$$W_F(\lambda, \gamma) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\gamma F(x) + \lambda x)}, \ \lambda \in \mathbb{F}_{2^n}, \gamma \in \mathbb{F}_{2^n}^*, \tag{6}$$

where Tr denotes the trace mapping, i.e. $Tr(x) = x + x^{2^1} + \cdots + x^{2^{n-1}}$. Then, defining the linearity as

$$\mathcal{L}(F) = \max\{|W_F(\lambda, \gamma)| : \lambda \in \mathbb{F}_{2^n}, \gamma \in \mathbb{F}_{2^n}^*\},$$

the goal is to find mappings with minimum possible value for $\mathcal{L}(F)$.

Those F, that achieve the minimum possible value for $\mathcal{L}(F)$ are called AB (*almost bent*) or *maximally nonlinear*, and these functions have the maximum resistance against linear cryptanalysis. For odd $n = 2m + 1$ this value is known to be 2^{m+1} [9]. For even n it is still open problem to determine the minimum for $\mathcal{L}(F)$. It was shown in [1, Theorem 4] that $\mathcal{L}(F) \geq 2^{n/2+1}$ for any APN power function, n even. In the Boolean case, when considering $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the situation is somewhat similar. Here, when n is even the functions achieving the maximum possible nonlinearity are known as *bent functions* [6,14,27]. These functions are not balanced and they have a uniform Walsh spectra, that is $W_f(\lambda) = 2^{n/2}$ for any $\lambda \in \mathbb{F}_2^n$.

3 Nonexistence of certain classes of permutations

Let x^d be a power monomial over $\mathbb{F}_{2^n}$, and $L(x)$ be a linear function. Our goal in this section is to answer the question when $x^d + L(x)$ is a permutation. In general, it is an open problem when an arbitrary (non)permuting function G becomes (remains) a permutation when a linear polynomial is added to G. Note that there exist integers d and s such that taking a nonpermutation binomial $G(x) = x^d + x^s$ where d, s are not 2-power ($d, s \neq 2^i$ for some $i \geq 0$), we can find permutation polynomials of the form $P(x) = G(x) + L(x)$. One example can be found in [17], where it was proved that for $n = 2m + 1$ the polynomial $P(x) = x^{2^{m+1}+1} + x^3 + x$ is a permutation polynomial on $\mathbb{F}_{2^n}$. When n is even, the permutation property of $x^d + L(x)$ is also related to open problem of the existence of APN permutations.

3.1 On permutations of the form $x^d + L(x)$ for even n

For the rest of the paper we denote

$$F_d(x) = x^d + L(x),\ L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}, \quad a_i \in \mathbb{F}_{2^n}. \tag{7}$$

Also for a linear function L on $\mathbb{F}_{2^n}$:

$$L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}, \quad a_i \in \mathbb{F}_{2^n},$$

we call *adjoint mapping of* L the linear function:

$$L^*(x) = \sum_{j=1}^{n} a_{n-j}^{2^j} x^{2^j}. \tag{8}$$

Lemma 1 *Let L be a linear function on $\mathbb{F}_{2^n}$. Then L is a permutation if and only if L^* is a permutation.*

Proof For any linear function $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$, the image set of L is a linear space, say V. Furthermore, L is a permutation if and only if $Ker(L) = \{0\}$. An element β is in the dual of V if and only if

$$Tr(\beta L(x)) = 0, \quad \text{for all} x \in \mathbb{F}_{2^n}.$$

But

$$Tr\left(\beta \sum_{i=0}^{n-1} a_i x^{2^i}\right) = Tr\left(x\left(\sum_{i=0}^{n-1} (a_i \beta)^{2^{n-i}}\right)\right) = Tr\left(x\left(\sum_{j=1}^{n} (a_{n-j}\beta)^{2^j}\right)\right)$$
$$= Tr(xL^*(\beta)).$$

Thus, $\beta \in V^\perp$ if and only if $L^*(\beta) = 0$. If L is a permutation then $V^\perp = \{0\}$ so that it is impossible to have $L^*(\beta) = 0$ unless $\beta = 0$, *i.e.,* L^* is a permutation. Conversely, if L^* is a permutation then $V^\perp = \{0\}$ implying that L is a permutation. □

Theorem 1 *The functions F_d are defined by (7). Let $n = 2m$ and d be any nonzero integer. If there is $\lambda \in \mathbb{F}_{2^n}^*$ such that the function $x \mapsto Tr(\lambda x^d)$ is bent then F_d is not a permutation, for any choice of L.*

Proof It is well-known that any function F over $\mathbb{F}_{2^n}$ is a permutation if and only if all its component functions are balanced, that is

$$\sum_{x \in \mathbb{F}} (-1)^{Tr(\lambda F(x))} = 0 \text{ for all } \lambda \in \mathbb{F}_{2^n}^*. \tag{9}$$

(see for instance [22, Theorem 7.7]). In other words, any function $Tr(\lambda F(x))$ has weight 2^{n-1}. So, F_d is a permutation if and only if any function

$$f_\lambda : x \mapsto Tr\left(\lambda\left(x^d + \sum_{i=0}^{n-1} a_i x^{2^i}\right)\right) = Tr\left(\lambda x^d + x\left(\sum_{i=0}^{n-1} (a_i \lambda)^{2^{n-i}}\right)\right), \tag{10}$$

is balanced. If λ is such that $x \mapsto Tr(\lambda x^d)$ is bent then any function $x \mapsto Tr(\lambda x^d + ax)$ is not balanced. In particular f_λ is not balanced, completing the proof. □

Note that Theorem 1 holds if we replace the power function $x \mapsto x^d$ by any function F. We now apply Theorem 1 to some important classes of power functions. Moreover, Theorem 1 is applicable to any bent function of the form $x \mapsto Tr(ax^d)$. The reader can see a recent list in [11].

Corollary 1 *Let $n = 2m$. The functions F_d are not permutations, for any choice of L, when d is as follows:*

(i) $d = 2^r + 2^s$ *with* $0 \le s < r \le n - 1$ *and* $\gcd(2^{r-s} + 1, 2^n - 1) \ne 1$*;*
(ii) $d = s(2^m - 1)$ *where s is coprime to* $2^m + 1$ *(with $n = 2m$);*
(iii) $d = 2^{2t} - 2^t + 1$ *with* $\gcd(t, n) = 1$ *where n is coprime to 3.*

Proof In all cases, we have to prove that there are some $\lambda \in \mathbb{F}_{2^n}^*$ such that the function $x \mapsto Tr(\lambda x^d)$ is bent.

Note that $Tr(ax^{2^r+2^s}) = Tr(a^{2^{n-s}} x^{2^{r-s}+1})$. But the function $x \mapsto Tr(\lambda x^{2^t+1})$ is bent if and only if $\lambda \notin \{y^{2^t+1} | y \in \mathbb{F}_{2^n}\}$ (see the proof in [21, Theorem 2]). Thus, a bent function exists as soon as $2^{r-s} + 1$ is not coprime to $2^n - 1$, proving (i).

In the case (ii), $x \mapsto Tr(\lambda x^d)$, with $\lambda \in \mathbb{F}_{2^m}$, is bent whenever the Kloosterman sum in point λ on $\mathbb{F}_{2^m}$ is zero (see explanations in [21] and [10]).

The case (iii) was treated by Dillon and Dobbertin [13, Theorem 11]. They proved that the function $x \mapsto Tr(\lambda x^d)$ is bent if and only if $\lambda \notin \{y^3 | y \in \mathbb{F}_{2^n}\}$. □

3.2 On APN permutations of the form $x^d + L(x)$, n even

Theorem 1 applies to a great majority of power monomials for which the spectrum is known. In particular, item (iii) in Corollary 1 refers to the Kasami exponent for which it was proved that $x^{2^{2t}-2^t+1}$ is APN [17]. On the other hand item (i) covers a broad class of functions with or without APN property depending on the choice of r, s. For instance, taking $s = 0, r = 1$ implies that $x^3 + L(x)$ is never a permutation, thus an APN function x^3 cannot be turned into permutation by adding a linear function. Note that the coefficients of $L(x)$ are in $\mathbb{F}_{2^n}$, hence this result is not covered by the result of Hou [19].

Remark 1 One might be tempted to assert a conjecture that any power function has bent components when n is even. This is in general not true, a counterexample is the Dobbertin exponent $d = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$, for even $n = 5g$. This function is APN [16], but its sum-of-square indicator takes such values so that the function cannot have bent components for $n \in \{10, 20\}$, for more details see [1, Example 5].

Now we consider APN mappings in a more general framework in connection to the open problem of the existence of APN permutation when n is even. Recall that if a function F is APN then $F + L$ is also APN. Recent results on this problem are summarized in [1, Theorem 3]. Notably, it was proved that if all component functions of F are plateaued then F cannot be a permutation. But, if F has all its components plateaued, this property holds for $F + L$ too. The property of being plateaued refers to the spectral characterization of Boolean functions, and the class of plateaued functions includes both bent and partially bent functions [28]. In addition, this superclass also contains functions that are not bent and do not have nonzero linear structures (the main property of the partial-bent class), therefore making them more suitable for cryptographic use. The above discussion yields the following general result:

Proposition 1 *Let $n = 2m$. Let F be an APN function on $\mathbb{F}_{2^n}$ which has all its components functions plateaued. Then $F + L$ cannot be a permutation, for any L. This is true, in particular, when F is quadratic.*

The main question we try to answer is: Can F_d be a permutation for some L when $x \mapsto x^d$ is APN ? We first give a more general result in this context.

Lemma 2 *Let d be such that $\gcd(2^n - 1, d) = s$ with $s > 1$. If F_d is a permutation for some L then L is a permutation too. In particular this holds for even n when $x \mapsto x^d$ is APN.*

Proof Assume that $\gcd(2^n - 1, d) = s$ with $s > 1$. Then any Boolean function

$$g_\lambda : x \in \mathbb{F}_{2^n} \longmapsto Tr(\lambda x^d)$$

has a weight divisible by s so that its weight cannot be 2^{n-1}. This means that g_λ cannot be balanced, for any λ. Now let $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$. So F_d is a permutation if and only if any function f_λ is balanced, with

$$f_\lambda(x) = Tr\left(\lambda x^d + x\left(\sum_{i=0}^{n-1} (a_i\lambda)^{2^{n-i}}\right)\right) = Tr\left(\lambda x^d + xL^*(\lambda)\right).$$

(see (9) and (10)). If L is not a permutation then L^* is not a permutation, from Lemma 1. Then there is $\alpha \neq 0$ such that $L^*(\alpha) = 0$ and further

$$f_\alpha(x) = Tr(\alpha x^d) = g_\alpha(x),$$

which is not balanced.

If $n = 2m$, we know that for any power APN function $x \mapsto x^d$ we have $\gcd(d, 2^n - 1) = 3$ (see [1], Section C). In this case g_α has a weight divisible by 3. □

Remark 2 A method to construct linear permutations was introduced in [20]. Let $(a_1, \ldots, a_{n-1})$ be $n - 1$ elements of $\mathbb{F}_{2^n}$ and consider

$$P(x) = \sum_{i=1}^{n-1} a_i x^{2^i} = x\left(\sum_{i=1}^{n-1} a_i x^{2^i - 1}\right) = xQ(x).$$

It is known that Q cannot be a permutation unless it has the form $ax + x^{2^i-1}, i > 1$ and $a \in \mathbb{F}_{2^n}^*$. Hence one can choose a_0 which is not in the image set of Q. Then

$$L(x) = x(a_0 + Q(x)) = \sum_{i=0}^{n-1} a_i x^{2^i},$$

is a permutation.

Theorem 2 *There are no permutations of the form* $x^d + \sum_{i=0}^{n-1} a_i x^{2^i}$, *where* $\gcd(d, 2^n - 1) = s > 1$ *and* $a_i \in \mathbb{F}_2$.

Proof We first note that if F_d is to be a permutation, then $\sum_{i=0}^{n-1} a_i x^{2^i}, a_i \in \mathbb{F}_2$, cannot be a permutation as we would have $\{0, 1\} \overset{F_d}{\mapsto} 0$. But by Lemma 2, $\sum_{i=0}^{n-1} a_i x^{2^i}$ must be a permutation, therefore result. □

In particular the result of Theorem 2 applies to those d for which x^d is APN function.

Corollary 2 *There do not exist APN permutations on* $\mathbb{F}_{2^n}$ *of the form,*

$$x^d + L(x),$$

where $\gcd(2^n - 1, d) > 1$, *and* $L(x) = \sum_{k=0}^{n-1} a_k x^{2^k}$, $a_k \in \mathbb{F}_2$.

Remark though, as these polynomials have binary coefficients, this result is just a special case of Hou's result [19].

Theorem 2 cannot be extended to nonbinary coefficients without further restrictions on F and/or parity of n. For instance, when n is even, the polynomial $F(x) = x^{171} + \alpha^5 x$ over $\mathbb{F}_{2^8}$ is a permutation for a primitive element α. F is obtained by adding a linear function with nonbinary coefficient to nonpermutation polynomial x^d, and furthermore $\gcd(d, 2^n - 1) = 3$ for $d = 171$ and $n = 8$; therefore the conditions of Theorem 2 are satisfied. Notice that extension of Theorem 2 to the case of nonbinary coefficients of L, n odd, would formally disprove the conjecture stated in [8]. This conjecture claims that given any AB function F there exist a linear function L such that $F + L$ is a permutation. A counterexample for this conjecture has already been found [5], for a certain AB function over $\mathbb{F}_{2^5}$.

Finally, we have the following result for APN power functions (but also applicable to any power mapping).

Proposition 2 *Let* F_d *be defined by* (7) *such that* $x \mapsto x^d$ *is APN and* L *is any linear permutation.*

Then F_d *is a permutation, for such* L *and* d, *if and only if*

$$z^d + (z+1)^d \neq \frac{L(e)}{e^d}, \quad \text{for all } z \in \mathbb{F}_{2^n} \text{ and } e \in \mathbb{F}_{2^n}^*.$$

Proof Assume that F_d is a permutation for some choice of permutation L. This is equivalent to say that there is no pair (x, y) such that $F_d(x) = F_d(y)$ with $x \neq y$. In other terms, it is impossible to have a pair (x, e) such that $F_d(x) + F_d(x + e) = 0$, which is

$$x^d + (x + e)^d + L(e) = 0.$$

Taking $z = x/e$, the equality above becomes

$$e^d \left(z^d + (z+1)^d\right) = L(e).$$

□

4 Recursive APN permutations from Gold mapping x^3

In Asiacrypt 2004 paper "On the generalized linear equivalence of functions over finite fields" [3], Breveglieri et al. conjectured that all functions obtained from an implicitly defined mapping,

$$x^3 + x^2 + x \to x$$

are not EA-equivalent to any power monomial over the field $\mathbb{F}_{2^n}$, for odd $n \geq 3$. Later this statement was corrected not to hold over $\mathbb{F}_{2^3}$ due to the small size of the field (first revision), and eventually completely withdrawn by the authors in the second revision [23].

Using a matrix-based approach it was shown that the above implicit mapping can be represented as affine transformation of the inverse coset of x^3, therefore the two representations are equivalent in the sense discussed in the introduction (EA-equivalent with respect to the inverse coset). Yet the authors in [23] claim that the possibility of deriving EA-inequivalent classes of APN functions by applying their approach to other APN monomials instead of applying it to x^3.

In the sequel we specify this affine transformation and furthermore give a formal proof of the recursive property of this transformation (this property was only justified through computer simulations in the conference version of this manuscript [26]). To give an exact description of the affine transformation let us define $F(x) = x^3$ and consider $g : x^3 + x^2 + x \to x$ over $\mathbb{F}_{2^5}$. Then the explicit form of g is given by,

$$g(x) = x^{21} + x^{20} + x^{17} + x^{16} + x^5 + x^4 + x \text{ over } \mathbb{F}_{2^5},$$

where $g \circ f(x) = x \pmod{x^{32} + x}$, for $f(x) = x^3 + x^2 + x$. Then from $F(x) \circ F^{-1}(x) \equiv x \pmod{x^{32} + x}$ we would get $F^{-1}(x) = x^{21}$ so that,

$$F^{-1}(x+1) + 1 = (x+1)^{21} + 1 = x^{21} + x^{20} + x^{17} + x^{16} + x^5 + x^4 + x = g(x).$$

Thus, the implicit mapping $x^3 + x^2 + x \to x$ corresponds to $g(x) = F^{-1} \circ A_2 + A$, where $F^{-1}(x)$ is a compositional inverse of $F(x) = x^3$, $A_2(x) = x + 1$ is affine permutation, and $A(x) = 1$ is a constant function. The very same transformation applies to arbitrary field sizes. The true essence of the Breveglieri et al. method [3] is therefore an affine transformation of the inverse coset of the Gold mapping. Applying the same approach to arbitrary APN functions would only give the functions that belong to the inverse coset of the initial APN function used.

In the conference version of this manuscript [26] a simple recursive method of constructing APN permutations was derived using the result in [3]. The method was based on the following observation. The Lagrange interpolation for the mapping $x^3 + x^2 + x \to x$ over $\mathbb{F}_{2^3}$ gives the function $g'(x) = x^5 + x^4 + x$, the same explicit form over $\mathbb{F}_{2^5}$ is then,

$$g(x) = x^{21} + x^{20} + x^{17} + x^{16} + x^5 + x^4 + x, \tag{11}$$

from which it was deduced that

$$g(x) = x^{16}(g'(x) + 1) + g'(x)$$

holds. This, however, gives a general recursion, that was verified by computer in [26] for finite fields of relatively small sizes, that relates the function $g' : x^3 + x^2 + x \to x$ on $\mathbb{F}_{2^{2k-1}}$ to the function $g : x^3 + x^2 + x \to x$ on $\mathbb{F}_{2^{2k+1}}$, $k \geq 2$, through

$$g(x) = x^{2^{2k}}(g'(x) + 1) + g'(x). \tag{12}$$

This interesting feature seems only to be valid for the Gold mapping $F(x) = x^3$. Below, we formally prove that recursion is true for any odd n. The following lemma will be needed.

Lemma 1 *Let $F(x) = x^3$ and $F^{-1}(x) = x^u$ for some $u > 0$, so that $(F \circ F^{-1})(x) \equiv x \pmod{x^{2^{2k-1}} + x}$ over $\mathbb{F}_{2^{2k-1}}$, $k \geq 2$. Then the compositional inverse of $F(x) = x^3$ over $\mathbb{F}_{2^{2k+1}}$ is computed as,*

$$F^{-1}(x) = x^{2^{2k}+u}.$$

Proof We have assumed that $(x^3)^u \equiv x \pmod{x^{2^{2k-1}} + x}$, that is,

$$3u \equiv 1 \pmod{2^{2k-1} - 1}.$$

Then we can write $3u = 1 + d(2^{2k-1} - 1)$ for some $d > 0$. But as $1 < u < 2^{2k-1} - 1$ then $0 < d < 3$, and we must necessarily have $d = 2$. That is, $3u = 1 + 2(2^{2k-1} - 1)$. To show that $F^{-1}(x) = x^{2^{2k}+u}$ over $\mathbb{F}_{2^{2k+1}}$ it suffices to show that,

$$3(2^{2k} + u) \equiv 1 \pmod{2^{2k+1} - 1}.$$

We have,

$$3(2^{2k} + u) = 3 \cdot 2^{2k} + 1 + 2(2^{2k-1} - 1) = 2^{2k+2} - 1 \equiv 1 \pmod{2^{2k+1} - 1}.$$

This concludes the proof. □

We are now ready to prove the recursive property of the APN permutations of the form $g'(x) = F^{-1}(x + 1) + 1$, where F^{-1} is the compositional inverse of $F(x) = x^3$.

Proposition 3 *Let F'^{-1} and F^{-1} denote the compositional inverses of $F(x) = x^3$ over $\mathbb{F}_{2^{2k-1}}$ and $\mathbb{F}_{2^{2k+1}}$, respectively. Given the APN permutation $g'(x) = F'^{-1}(x + 1) + 1$ over $\mathbb{F}_{2^{2k-1}}$, the function $g(x) = F^{-1}(x + 1) + 1$ over $\mathbb{F}_{2^{2k+1}}$ is given by,*

$$g(x) = x^{2^{2k}}(g'(x) + 1) + g'(x).$$

Proof Let $g'(x) = F'^{-1}(x + 1) + 1 = (x + 1)^{u'} + 1$, where $x^{u'}$ is a compositional inverse of x^3 over $\mathbb{F}_{2^{2k-1}}$. Then,

$$\begin{aligned} g(x) &= (x + 1)^u + 1 \overset{\text{Lem. 1}}{=} (x + 1)^{2^{2k}+u'} + 1 = (x^{2^{2k}} + 1)(x + 1)^{u'} + 1 = \\ &= x^{2^{2k}}(x + 1)^{u'} + g'(x) = x^{2^{2k}}(g'(x) + 1) + g'(x). \end{aligned} \tag{13}$$

□

Remarkably the recursion is more delicate when considering the inverse mapping of $x^3 + x^2 + x$ over $\mathbb{F}_{2^3}$. In other words, instead of considering $x^3 + x^2 + x \rightarrow x$ whose explicit polynomial form over $\mathbb{F}_{2^3}$ is $g(x) = x^5 + x^4 + x$, we may start with the implicit mapping $x^5 + x^4 + x \rightarrow x$ over $\mathbb{F}_{2^3}$ and then try to deduce a recursion similar to the one valid for $x^3 + x^2 + x \rightarrow x$. The Lagrange interpolation of $g : x^5 + x^4 + x \rightarrow x$ gives the following explicit forms,

$$\begin{aligned} &x^3 + x^2 + x, \quad \text{over } \mathbb{F}_{2^3} \\ &x^{25} + x^{24} + x^{17} + x^{16} + x^9 + x^8 + x, \quad \text{over } \mathbb{F}_{2^5} \\ &x^{51} + x^{50} + x^{49} + x^{48} + x^{35} + x^{34} + x^{33} + x^{32} + x^{19} + x^{18} + x^{17} + x^{16} \\ &\quad + x^3 + x^2 + x, \quad \text{over } \mathbb{F}_{2^7} \end{aligned}$$

$$x^{409}+x^{408}+x^{401}+x^{400}+x^{393}+x^{392}+x^{385}+x^{384}+x^{281}+x^{280}+x^{273}$$
$$+x^{272}+x^{265}++x^{264}+x^{257}+x^{256}+x^{153}+x^{152}+x^{145}+x^{144}+x^{137}+x^{136}$$
$$+x^{129}+x^{128}+x^{25}+x^{24}++x^{17}+x^{16}+x^{9}+x^{8}+x \text{ over } \mathbb{F}_{2^9}.$$

All these functions are clearly APN permutations but in difference to $x^3+x^2+x \to x$ the recursive relation that defines APN permutation over $\mathbb{F}_{2^{2k+1}}$ refers to a smaller field $\mathbb{F}_{2^{2k-3}}$ rather than to $\mathbb{F}_{2^{2k-1}}$. When $2k+1=5$, i.e. $k=2$, a general recursion given below does not apply as the binary field $\mathbb{F}_2$ would be then used. The recursion, valid for $\mathbb{F}_{2^{2k+1}}$ and $k>2$, is given by

$$g(x)=\begin{cases}(x^{2^{2k-2}}+x^{2^{2k-1}}+x^{2^{2k-1}+2^{2k-2}})(g_1(x)+1)+g_1(x), & k \text{ odd};\\ (x^{2^{2k-1}}+x^{2^{2k}}+x^{2^{2k}+2^{2k-1}})(g_1(x)+1)+g_1(x), & k \text{ even};\end{cases}$$

where g_1 and g denote the explicit mappings of $x^5+x^4+x \to x$ over $\mathbb{F}_{2^{2k-3}}$ and $\mathbb{F}_{2^{2k11}}$ respectively. Nevertheless, the affine transformation applied to the compositional inverse is expectedly the same one as for $x^3+x^2+x \to x$. That is, the explicit form of the mapping $g: x^5+x^4+x \to x$ is given by $g(x)=F^{-1}(x+1)+1$, where $F^{-1}(x)$ is a compositional inverse of $F(x)=x^5$. For instance, over $\mathbb{F}_{2^5}$ it is readily checked that using $F^{-1}(x)=x^{25}$ for $F(x)=x^5$ the above expression is retrieved.

Lemma 2 *Let $F(x)=x^5$ and $F^{-1}(x)=x^u$ for some $u>0$, so that $(F\circ F^{-1})(x)\equiv x$ (mod $x^{2^{2k-1}}+x$) over $\mathbb{F}_{2^{2k-3}}$, $k>2$. Then the compositional inverse of $F(x)=x^5$ over $\mathbb{F}_{2^{2k+1}}$ is computed as,*

$$F^{-1}(x)=\begin{cases}x^{2^{2k-1}+2^{2k-2}+u}, & k \ \text{odd};\\ x^{2^{2k}+2^{2k-1}+u}, & k \ \text{even};\end{cases}$$

Proof We have assumed that $(x^5)^u \equiv x \pmod{x^{2^{2k-3}}+x}$, that is,

$$5u \equiv 1 \pmod{2^{2k-3}-1}.$$

Then we can write $5u = 1 + d(2^{2k-3}-1)$ for some $d>0$. But as $1<u<2^{2k-3}-1$ then $0<d<5$, and then $d\in\{2,4\}$. The case $d=2$ holds for odd k, and $d=4$ when k is even.

To show that $F^{-1}(x)=x^{2^{2k-1}+2^{2k-2}+u}$ over $\mathbb{F}_{2^{2k+1}}$ for odd k and $d=2$, it suffices to show that,

$$5(2^{2k-1}+2^{2k-2}+u)\equiv 1 \pmod{2^{2k+1}-1},$$

where the multiplicative inverse u over the field $\mathbb{F}_{2^{2k-3}}$ satisfies $5u=1+2\cdot(2^{2k-3}-1)$. Then,

$$\begin{aligned}5\cdot(2^{2k-1}+2^{2k-2}+u) &= 5\cdot(2^{2k-1}+2^{2k-2})+1+2\cdot(2^{2k-3}-1)\\ &= 2^{2k+2}-1\equiv 1 \pmod{2^{2k+1}-1}.\end{aligned}$$

When k is even, that is $d=4$, then $5u=1+4(2^{2k-3}-1)$ so that,

$$\begin{aligned}5\cdot(2^{2k}+2^{2k-1}+u) &= 5\cdot(2^{2k}+2^{2k-1})+1+4\cdot(2^{2k-3}-1)\\ &= 2^{2k+3}-3\equiv 1 \pmod{2^{2k+1}-1}.\end{aligned}$$

This concludes the proof. □

Proposition 4 *Let F'^{-1} and F^{-1} denote the compositional inverses of $F(x) = x^5$ over $\mathbb{F}_{2^{2k-3}}$ and $\mathbb{F}_{2^{2k+1}}$, respectively. Given the APN permutation $g_1(x) = F'^{-1}(x+1)+1$ over $\mathbb{F}_{2^{2k-3}}$, the function $g(x) = F^{-1}(x+1)+1$ over $\mathbb{F}_{2^{2k+1}}$ is given by,*

$$g(x) = \begin{cases} (x^{2^{2k-2}} + x^{2^{2k-1}} + x^{2^{2k-1}+2^{2k-2}})(g_1(x)+1) + g_1(x), & k \text{ odd;} \\ (x^{2^{2k-1}} + x^{2^{2k}} + x^{2^{2k}+2^{2k-1}})(g_1(x)+1) + g_1(x), & k \text{ even;} \end{cases}$$

Proof We only prove the case k odd, the proof for k even is similar. Let $g_1(x) = F'^{-1}(x+1)+1 = (x+1)^{u'}+1$, where x^{u^Prime} is a compositional inverse of x^5 over $\mathbb{F}_{2^{2k-3}}$. Then,

$$\begin{aligned} g(x) &= (x+1)^u + 1 \overset{\text{Lem. 2}}{=} (x+1)^{2^{2k-1}+2^{2k-2}+u'} + 1 \\ &= (x^{2^{2k-1}}+1)(x^{2^{2k-2}}+1)(x+1)^{u'}+1 \\ &= (x^{2^{2k-1}} + x^{2^{2k-2}} + x^{2^{2k-1}+2^{2k-2}})(x+1)^{u'} + (x+1)^{u'} + 1 \\ &= (x^{2^{2k-1}} + x^{2^{2k-2}} + x^{2^{2k-1}+2^{2k-2}})(g_1(x)+1) + g_1(x). \end{aligned}$$ □

Remark 3 The authors are not aware of similar examples of APN functions with such a recursive property. The recursion resembles the properties of the Welch exponent $d = 2^m + 3$ over $\mathbb{F}_{2^n}$, $n = 2m+1$, (known to be an APN (AB) permutation [17]) which relates the exponent of x^{2^m+3} to the field size. The recursion in this case is given by $F_d(x) = x^{2^m} F'_d(x)$ where F'_d and F_d define the APN permutations over $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^{n+2}}$ respectively, $n = 2m+1$. Note that the algebraic degree is always equal to 3 in this case whereas the recursion in (12) increases the degree in each step of iteration. Furthermore, there is no obvious relation between the inverse coset exponents.

The iterative property of the Gold function cannot in general be extended to polynomials with nonbinary coefficients. It remains an open problem to find other examples of recursions for polynomials with nonbinary coefficients in the subfield of all considered larger fields in the sequence. For instance, starting with an initial polynomial in $\mathbb{F}_{2^3}[x]$ with the coefficients in $\mathbb{F}_{2^3}$ one may try to construct polynomials (that preserve the permutation and APN property) over $\mathbb{F}_{2^6}, \mathbb{F}_{2^9}, \mathbb{F}_{2^{12}}$, etc. in an iterative manner.

5 Conclusions

In this paper we have developed several ideas useful in analysis of cryptographically significant mappings over finite fields. Though, we could not treat all the cases of interest for particular class of polynomials given by $x^d + L(x)$, the results presented here will hopefully impact the subsequent research in this field.

Acknowledgments The authors would like to thank to Sumanta Sarkar and Srimanta Bhattacharya for providing the example of binomial permutation $x^{171} + \alpha^5 x$, and for drawing our attention to the mapping $x^5 + x^4 + x \to x$.

References

1. Berger T.P., Canteaut A., Charpin P., Laigle-Chapuy, Y.: On almost perfect nonlinear functions over $GF(2^n)$. IEEE Trans. Inform. Theory **IT-52**(9), 4160–4170 (2006).
2. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991).

3. Breveglieri L., Cherubini A., Macchetti M.: On the generalized linear equivalence of functions over finite fields. In: Advances in Cryptology—ASIACRYPT 2004. Lecture Notes in Computer Science, LNCS vol. 3329, pp. 79–91. Springer-Verlag, Berlin (2004).
4. Budaghyan L.: The simplest method for constructing APN polynomials EA-inequivalent to power functions. In: Arithmetic of Finite Fields, WAIFI 2007. LNCS, vol. 4547, pp. 177–188. Springer-Verlag, Berlin (2007).
5. Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory **IT-52**(3), 1141–1152 (2006).
6. Carlet, C.: A Construction Of Bent Functions. Finite Fields and Applications, London Mathematical Society Lecture Notes Series 233, pp. 47–58. Cambridge University Press, Cambridge (1996)
7. Carlet C.: Vectorial Boolean functions for cryptography. In: Crama E.Y., Hammer P. (eds.) Boolean Methods and Models. Cambridge University Press, Cambridge (2009).
8. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998).
9. Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. In: Advances in Cryptology—EUROCRYPT'94. LNCS, vol. 950, pp. 356–365. Springer-Verlag, New York (1994).
10. Charpin P., Gong G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. IEEE Trans. Inform. Theory **IT-54**(9), 4230–4238 (2008)
11. Charpin P., Kyureghyan G.: Cubic monomial bent functions: a subclass of $\mathcal{M}$. SIAM J. Discrete Math. **22**(2), 650–665 (2008).
12. Charpin P., Kyureghyan G.: On a class of permutation polynomials over F_{2^n}. In: Sequences and Their Applications-SETA 2008. LNCS, vol. 5203, pp. 368–376. Springer-Verlag, Berlin (2008).
13. Dillon J., Dobbertin H.: New cyclic difference sets with singer parameters. Finite Fields Appl. **10**, 342–389 (2004).
14. Dillon J.F.: Elementary Haddamard difference sets. Ph. D. thesis, University of Maryland, USA (1974).
15. Dillon J.F.: APN polynomials: An Update. To be published in proceedings of: The 9th Conference on Finite Fields and Applications FQ9, Dublin, Ireland (2009).
16. Dobbertin H.: Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. In: Jungnickel D., Niederreiter H., (eds.) proceedings of: The fifth Conference on Finite Fields and Applications FQ5, pp. 113–121. Springer-Verlag (1999).
17. Dobbertin H.: Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case. IEEE Trans. Inform. Theory **IT-45**(4), 1271–1275 (1999).
18. Edel Y., Kyureghyan G., Pott A.: A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory **IT-45**(4), 1237–1243 (1999).
19. Hou X.D.: Affinity of permutations of $\mathbb{F}_{2^n}$. Discrete Appl. Math. **154**(2), 313–325 (2006).
20. Laigle-Chapuy Y.: A note on a class of quadratic permutations over F_{2^n}. In Proceedings of the 17th Symposium on Applied algebra, Algebraic algorithms, and Error Correcting Codes AAECC 17. LNCS, vol. 4851, pp. 130–137. Springer-Verlag (2007).
21. Leander N.G.: Monomial bent functions. IEEE Trans. Inform. Theory **IT-52**(2), 738–743 (2006).
22. Lidl R., Niederreiter, R.E.: Finite fields. Cambridge University Press, Cambridge (1997).
23. Macchetti M.: Addendum to "On the generalized linear equivalence of functions over finite fields". Cryptology ePrint Archive, Report 2004/347, (2004) http://eprint.iacr.org/.
24. Matsui M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology—EUROCRYPT'93. LNCS, vol. 765, pp. 386–397. Springer-Verlag, Berlin (1993).
25. Niederreiter H., Robinson K.H.: Complete mappings of finite fields. J. Aust. Math. Soc. Ser. A **33**, 197–212 (1982).
26. Pasalic E.: On cryptographically significant mappings over GF (2^n). In Proceedings of Arithmetics of Finite Fields, Second International Conference, WAIFI 2008. LNCS, vol. 5130, pp. 189–204. Springer-Verlag, Berlin (2008).
27. Rothaus O.S.: On bent functions. J. Combin. Theory Ser. A **20**, 300–305 (1976).
28. Zheng Y., Zheng X.-M.: On plateaued functions. IEEE Trans. Inform. Theory **IT-47**(3), 1215–1223 (2001).