

Addendum to “On the Generalized Linear Equivalence of Functions over Finite Fields”

Marco Macchetti

Politecnico di Milano, Milan, Italy
macchett@elet.polimi.it

Abstract. In this paper we discuss the example of APN permutation introduced in the paper “On the Generalized Linear Equivalence of Functions over Finite Fields” [1], presented at Asiacrypt 2004. We show that the permutation given in [1] is indeed classically linearly equivalent to a power monomial. More in general, we show that no new class of APN functions can be discovered starting from permutation polynomials of the type used in [1] applied on the APN monomial x^3 .

1 Introduction

The concept of generalized functional linear equivalence has been introduced in [1]; the idea is to define a geometric representation of function $f : F_p^m \rightarrow F_p^n$ with p prime and $m, n \geq 1$ onto the linear space F_p^{m+n} . Every function is associated with an implicit embedding, i.e. a set of vectors that contains the information of the function truth table. Two functions f, g are generally linearly equivalent if the embedding of g can be obtained from the embedding of f by means of an invertible linear transformation acting on the whole linear space.

In [1], Sect. 4, Example 2 contains the specification of an APN permutation obtained starting from the power monomial x^3 over $\text{GF}(2^3)$ which is claimed to be classically not equivalent to x^3 . In the next Section we show that all functions generated in this way are indeed classically affine equivalent to the inverse of the power monomial x^3 .

2 Revised Claim

Consider the APN power monomial $f(x) = x^3$ defined over $\text{GF}(2^n)$. The particular permutation polynomial $p(x)$ under discussion is of the form (1), where the conditions to be verified are that $b^2 = ac$, $2^n \bmod 3 = 2$ and $a, b, c, d \in \text{GF}(2^n)$.

$$p(x) = ax^3 + bx^2 + cx + d \quad (1)$$

This permutation polynomial can be re-written as (2), if x^3 is a power permutation.

$$p(x) = (ex + f)^3 + k = e^3x^3 + e^2fx^2 + ef^2x + f^3 + k \quad (2)$$

In fact, every choice of a in (1) implies a unique choice of e in (2) and every choice of c consequently implies a unique choice of f ; the condition $b^2 = ac$ is then a tautology since it is always true that $e^4 f^2 = e^3 e f^2$. The choice for d forces a unique choice of the constant k . The cases when x^3 is not a permutation are not of interest, since this implies that $\text{GCD}(3, 2^n - 1) \neq 1$, that in turn implies $2^n - 1 = 3m$ and finally $2^n \bmod 3 = 1$ and in this case (1) is not a permutation polynomial.

This said, every function obtained from x^3 by means of a generalized linear transformation and of the form (3), where M and N are arbitrarily chosen $n \times n$ binary matrices, can always be re-written as (4). This includes the function in [1], Example 2.

$$ax^3 + bx^2 + cx + d \rightarrow Mx + Nx^3 \quad (3)$$

$$(ex + f)^3 + k \rightarrow Mx + Nx^3 \quad (4)$$

Now, let us operate the substitution $y = (ex + f)^3 + k$, or $x = e^{-1}(y + k)^{\frac{1}{3}} + e^{-1}f$; if we re-write (4) in an explicit form using y we obtain (5) and then (6).

$$y \rightarrow M(e^{-1}(y + k)^{\frac{1}{3}} + e^{-1}f) + N(e^{-1}(y + k)^{\frac{1}{3}} + e^{-1}f)^3 \quad (5)$$

$$y \rightarrow M(e^{-1}(y + k)^{\frac{1}{3}} + e^{-1}f) + N(e^{-3}(y + k) + e^{-3}f^3 + e^{-3}f(y + k)^{\frac{2}{3}} + e^{-3}f^2(y + k)^{\frac{1}{3}}) \quad (6)$$

We can note that, by defining two opportune $n \times n$ binary matrices P and Q , and a constant $k' \in \text{GF}(2^n)$, (6) can be re-written¹ as (7), which is classically affine equivalent to the power monomial $y^{\frac{1}{3}}$, i.e. the inverse of y^3 , if and only if matrix Q is non-singular. The values of P and Q are given in (8) and (9), where the S matrix is associated with the squaring operation, and matrices E^i and F^i are associated with the constant multiplication times e^i and f^i .

$$y \rightarrow Py + Q(y + k)^{\frac{1}{3}} + k' \quad (7)$$

$$P = NE^{-3} \quad (8)$$

$$Q = ME^{-1} + N(E^{-3}FS + E^{-3}F^2) \quad (9)$$

Thus if $\det(Q)$ is null the function is not classically equivalent to $y^{\frac{1}{3}}$; exploiting the fact that the matrices E^i and F^i commute, and that S represents the squaring operation we can write:

$$\begin{aligned} Q &= ME^{-1} + N(FSE^{-3 \cdot 2^{n-1}} + E^{-3}F^2) = \\ &= ME^{-1} + N(FSE^{-2^{n-1}-1} + E^{-3}F^2) = \\ &= (M + N(FSE^{-2^{n-1}} + E^{-2}F^2))E^{-1} = \\ &= (M + N(E^{-1}FS + E^{-2}F^2))E^{-1} \end{aligned} \quad (10)$$

¹ This is possible since the squaring operation is always linear in finite fields with even characteristic.

However, the function is obtained with a generalized transformation and to preserve the APN property the determinant of matrix T associated with the generalized affine transformation must be positive. Matrix T is given by:

$$T = \left(\begin{array}{c|c} E^2FS + EF^2 & E^3 \\ \hline M & N \end{array} \right)$$

and its determinant is given by:

$$\det(T) = \det(E^3)\det(M + NE^{-3}(E^2FS + EF^2)) \quad (11)$$

Eventually, looking at (10) and (11) the two constraints to be satisfied are:

$$\det(M + N(E^{-1}FS + E^{-2}F^2)) = 0 \quad (12)$$

$$\det(M + N(E^{-1}FS + E^{-2}F^2)) \neq 0 \quad (13)$$

that always lead to contradiction. If the obtained function is generally equivalent to x^3 it is also classically equivalent to $x^{\frac{1}{3}}$. Thus, we can conclude that no non-trivial APN function can be produced starting from the given permutation polynomial class; this may be possible starting from other permutation polynomial classes, and/or other APN monomials.

References

1. Breveglieri, L., Cherubini, A., Macchetti, M.: On the Generalized Linear Equivalence of Functions over Finite Fields. Proceedings of ASIACRYPT 2004, 79–91, 2004.