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, although the method used to derive the function is correct, the permutation given in [1] is classically linearly equivalent to a power monomial. We therefore use the same method here to generate other APN permutations that are generally, but not classically, linearly equivalent to power monomials.

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 GF(2^3) which is claimed to be classically not equivalent to x^3. The claim is false. However, in the next Section we show that the same method can be used to build previously unknown APN permutations over different finite fields.

2 Revised Examples

Consider the power monomial $f(x) = x^3$ defined over GF(2^5). Let S represent the matrix over $\{0, 1\}$ which governs the squaring operation[1] in GF(2^5). The implicit embedding of function g is obtained starting from that of f by applying the following transformation:

$$\begin{pmatrix} y \\ g(y) \end{pmatrix} = \left(\begin{array}{c|c} I+S & I \\ \hline I & 0 \end{array}\right) \bullet \begin{pmatrix} x \\ x^3 \end{pmatrix}$$

[1] The squaring operation is always linear in finite fields with even characteristic.

The guarantee that the derived implicit embedding actually represents a function comes from the fact that $x^3 + x^2 + x$ is a permutation polynomial over GF(2^n) with n odd. The truth table of function g is defined by the following relation:

$$x^3 + x^2 + x \quad \rightarrow \quad x \tag{1}$$

Lagrange interpolation leads to the conventional form:

$$g(x) = x^{21} + x^{20} + x^{17} + x^{16} + x^5 + x^4 + x \tag{2}$$

This permutation is generally linearly equivalent to x^3 and thus is APN, but cannot be classically obtained from x^3, because some of the monomials inside (2) belong to different cyclotomic cosets. Table 1 contains a list of the cyclotomic cosets of power monomials over GF(2^5); exponents present in (2) are shown in bold.

Table 1. The cyclotomic cosets of GF(2^5).

Coset leader	Exponents
0	0
1	**1**, 2, **4**, 8, **16**
3	3, 6, 12, 24, **17**
5	**5**, 10, **20**, 9, 18
7	7, 14, 28, 25, 19
11	11, 22, 13, 26, **21**
15	15, 30, 29, 27, 23

The same construction can be applied to GF(2^7); in this case Lagrange interpolation of (1) gives the following APN permutation:

$$\begin{aligned} g(x) = {} & x^{85} + x^{84} + x^{81} + x^{80} + x^{69} + x^{68} + x^{65} + x^{64} + \\ & + x^{21} + x^{20} + x^{17} + x^{16} + x^5 + x^4 + x \end{aligned} \tag{3}$$

which again is not classically equivalent to x^3. However, when the construction is applied to GF(2^3), the function $g(x) = x^5 + x^4 + x$ is obtained, which is classically linearly equivalent to x^3 since exponents 5 and 3 are in the same coset and $x^4 + x$ is a linear function of x. We think this is a peculiar characteristic of GF(2^3), due to the small number of elements in this field; we conjecture that all functions obtained with (1) on GF(2^n), n odd and $n > 3$, are APN permutations which are not classically equivalent to any power monomial. A formal proof, however, will be required to settle the result.

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.