Some More Functions That Are Not APN Infinitely Often

François Rodier

Abstract

We give new functions which cannot be APN over an infinity of field extensions.

Keywords: vector Boolean functions, almost perfect nonlinear functions, algebraic surface.

1 Introduction

The vector Boolean functions are used in cryptography to construct block ciphers and an important criterion on these functions is highly resistance to differential cryptanalysis.

Let $q = 2^n$ for some positive integer n. A function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is said to be *almost perfect nonlinear* (APN) on $\mathbb{F}_q$ if the number of solutions in $\mathbb{F}_q$ of the equation

$$f(x + a) + f(x) = b$$

is at most 2, for all $a, b \in \mathbb{F}_q$, $a \neq 0$. Because $\mathbb{F}_q$ has characteristic 2, the number of solutions to the above equation must be an even number, for any function f on $\mathbb{F}_q$. This kind of function has a good resistance to differential cryptanalysis as was proved by Nyberg in [11].

So far, the study of APN functions has focused on power functions. Recently it was generalized to other functions, particularly polynomials (Carlet, Pott and al. [3, 7, 8]) or polynomials on small fields (Dillon [6]). On the other hand, several authors (Berger, Canteaut, Charpin, Laigle-Chapuy [2], Byrne and McGuire [4] or Jedlicka [10]) showed that APN functions did not exist in certain cases.

Thus, towards a full classification of all APN functions, one approach that already proved to be successful is to show that certain polynomials are not APN for infinitely many extensions of $\mathbb{F}_2$. So here one first fixes a

finite field $\mathbb{F}_q$ and a function $f : \mathbb{F}_q \to \mathbb{F}_q$ given as a polynomial in $\mathbb{F}_q[x]$ and asks the question whether this function can be APN on infinitely many extensions of $\mathbb{F}_q$. There is a variety of classes of functions for which it can be shown that each function is APN at most for a finite number of extensions.

Hernando and McGuire [9] showed a result on the classification of APN monomials which has been conjectured for 40 years: the only exponents such that the monomial x^d are APN over infinitely many extension of $\mathbb{F}_2$ are of the form $2^i + 1$ or $4^i - 2^i + 1$. One calls these exponents *exceptional exponents*. Then it is natural to formulate for polynomial functions the following conjecture.

Conjecture: (Aubry, McGuire and Rodier) a polynomial can be APN for an infinity of ground fields $\mathbb{F}_q$ only if it is CCZ equivalent (as was defined by Carlet, Charpin and Zinoviev in [5]) to a monomial x^t where t is an exceptional exponent.

One mean to prove this conjecture is to remark that the APN property is equivalent to the fact that the rational points of a certain algebraic surface $S(f)$ in a 3-dimensional space linked with the polynomial f defining the Boolean function are all in a surface V made of 3 planes and independent of f. We define the surface $S(f)$ in the three dimensional affine space $\mathbb{A}^3$ by

$$\phi(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(x + z)(y + z)}$$

which is a polynomial in $\mathbb{F}_q[x, y, z]$.

When this surface is irreducible (or when it has an irreducible component defined over the field of definition of f), a Weil's type bound may be used to approximate the number of rational points of this surface. When it is too large the surface is too big to be contained in the surface V, and the function f cannot be APN. A relation between the degree and the number of variables on a large number of Boolean function was obtained by this mean by the author [12]. This enabled him, with Aubry and McGuire to prove the conjecture in a number of cases.

2 The State of the Art

The best known examples of APN functions are the Gold functions x^{2^k+1} and the Kasami-Welch functions $x^{4^k-2^k+1}$. These functions are defined over $\mathbb{F}_2$, and are APN on any field $\mathbb{F}_{2^m}$ where $gcd(k, m) = 1$.

Theorem 2.1 (Aubry, McGuire and Rodier, [1]) *If the degree of the*

polynomial function f is odd and not a Gold or a Kasami-Welch number then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

In the even degree case, we can state the result when half of the degree is odd, with an extra minor condition.

Theorem 2.2 (Aubry, McGuire and Rodier, [1]) *If the degree of the polynomial function f is $2e$ with e odd, and if f contains a term of odd degree, then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.*

We have some results on the polynomials of Gold degree $d = 2^k + 1$.

Theorem 2.3 (Aubry, McGuire and Rodier, [1]) *Suppose $f(x) = x^d + g(x)$ where $\deg(g) \leq 2^{k-1}+1$. Let $g(x) = \sum_{j=0}^{2^{k-1}+1} a_j x^j$. Suppose moreover that there exists a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible (where $\phi_i(x, y, z)$ denote the polynomial $\phi(x, y, z)$ associated to x^i). Then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.*

3 New results

3.1 Functions of degree $4e$ where e is odd

We have been interested in the degrees of the form $4e$, where e is an odd number. This case is far more intricate than the previous cases, because there are some polynomials which are CCZ equivalent to monomials.

Here are some partial results.

Theorem 3.1 *If the degree of the polynomial function f is even such that $\deg(f) = 4e$ with $e \equiv 3 \pmod 4$ and $e \geq 7$, then f is not APN over $\mathbb{F}_{q^n}$ for n large.*

Sketch of proof. We have in this case:

$$\phi_d(x, y, z) = \phi_e(x, y, z)^4((x + y)(x + z)(y + z))^3$$

where ϕ_d is the ϕ function associated to the monomial x^d. Hence X_∞ is not reduced where $X_\infty = H_\infty \cap \overline{S}(f)$, H_∞ is the plane at infinity of the space $\mathbb{A}^3$ and $\overline{S}(f)$ is the projective closure of $S(f)$.

Let X_0 a reduced absolutely irreducible component of $\overline{S}(f)$ which contains the line $x + y = 0$ in H_∞. By studying the various cases which may happen, one is reduced to the case where there are three components X_0,

X_1 and X_2 which contain this line, they are defined over the field $\mathbb{F}_{q^3}$, where $\mathbb{F}_q$ is the field of definition of f and the Galois group of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$ acts by cyclic permutations of X_0, X_1 and X_2. By studying the irreducibility of X_0, one is again reduced to the case where X_0, X_1 and X_2 are of degree 3 of the form $((x+y)(x+z)(y+z))^3 + P$ where P is a polynomial of degree at most 2. Because of the symmetry of the function ϕ associated to f in the variables x, y and z, one is reduced to the cases where the polynomial P is of the form

$$P(x,y,z) = c_1(x^2+y^2+z^2) + c_4(xy+xz+zy) + b_1(x+y+z) + d$$

Investigating these polynomials, one prove that it is impossible that they divide ϕ.

We have some other results when the degree e is a Gold degree.

Theorem 3.2 *If the degree of the polynomial f is 12, then either f is not APN over $\mathbb{F}_{q^m}$ for m large or f is CCZ equivalent to the Gold function x^3.*

Let $d \in \mathbb{F}_{q^3}$ such that $d + d^q + d^{q^2} = 0$. The polynomials CCZ equivalent to the Gold function x^3 are the polynomial functions

$$f(x) = L(x^3) \quad \text{or} \quad f(x) = L(x)^3$$

with

$$L(x) = x^4 + (d^{1+q} + d^{1+q^2} + d^{q+q^2})x^2 + d^{1+q+q^2}x$$

and the polynomials composed with f and an affine permutation.

3.2 Functions of Kasami degree

We can prove that a function $f(x) = x^d + g(x)$ where $d = 2^{2k} - 2^k + 1$ and $\deg(g)$ small enough and such that there exists a nonzero coefficient a_j of g such that $\phi_j(x,y,z)$ is absolutely irreducible. Then $\phi(x,y,z)$ is absolutely irreducible and f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

This is proved by the same way than the case of polynomials of Gold degree in [1].

References

[1] Y. Aubry, G. McGuire, F. Rodier, *A few more functions that are not APN infinitely often*, to be published with the proceedings of the conference Fq9, Dublin, 2009. Contemporary Mathematics Series.

[2] T. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy *On almost perfect nonlinear functions over* F_2^n. IEEE Trans. Inform. Theory 52 (2006), no. 9, 4160–4170.

[3] L. Budaghyan and C. Carlet and P. Felke and G. Leander *An infinite class of quadratic APN functions which are not equivalent to power mappings,* Cryptology ePrint Archive, n° 2005/359

[4] Byrne E. and McGuire G., *On the Non-Existence of Quadratic APN and Crooked Functions on Finite Fields*, prepublication. http://www.maths.may.ie/sta/gmg/APNniceWeilEBGMG.pdf.

[5] C. Carlet, P. Charpin and V. Zinoviev. *Codes, bent functions and permutations suitable for DES-like cryptosystems.* Designs, Codes and Cryptography, 15(2), pp. 125-156, 1998.

[6] J. Dillon, *APN Polynomials: An Update.* Fq9, International Conference on Finite Fields and their Applications July 2009

[7] Y. Edel, G. Kyureghyan and A. Pott. *A new APN function which is not equivalent to a power mapping.* IEEE Trans. Inform. Theory 52 (2006), no. 2, 744–747.

[8] Y. Edel, A. Pott. *A new almost perfect nonlinear function which is not quadratic* Adv. Math. Commun. 3 (2009), no. 1, 59–81.

[9] F. Hernando and G. McGuire, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, arXiv:0903.2016v3* [cs.IT], 2009.

[10] Jedlicka, D., *APN monomials over* GF(2^n) *for infinitely many* n, Finite Fields Appl. 13 (2007), no. 4, 1006–1028.

[11] K. Nyberg, *Differentially uniform mappings for cryptography, Advances in cryptology—Eurocrypt '93* (Lofthus, 1993), 55–64, Lecture Notes in Comput. Sci., Vol. 765, Springer, Berlin, 1994.

[12] F. Rodier, *Bornes sur le degré des polynômes presque parfaitement non-linéaires,* in Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M.Tsfasman editors, Contemporary Math. no 487, AMS, Providence (RI), USA, pp. 169-181, 2009. *arXiv:math/0605232v3* [math.AG].