A New Step Toward Classification Of APN Functions

Florian Caullery

Modern private key cryptosystems, such as AES, are block cipher. The security of such systems relies on what is called the S-box. This is simply a Boolean function $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ where n is the size of the blocks. It is the only non linear operation in the algorithm. One of the best known attack on these systems is differential cryptanalysis. Nyberg proved that the S-boxes with the best resistance to such attacks are the one who are said to be Almost Perfectly Non-linear (APN).

Let $q=2^n$. A function $f:\mathbb{F}_q\to\mathbb{F}_q$ is said 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 $a,b\in\mathbb{F}_q$, $a\neq 0$. The fact that $\mathbb{F}_q$ has charecteristic 2 implies that the number of solutions is even for any function f on $\mathbb{F}_q$.

The study of APN functions has focused on power functions and it was recently generalized to other functions, particularly polynomials or polynomials on small fields. On the other hand, several authors showed that APN functions did not exist in certain cases. Some also studied the notion of being APN on other fields than $\mathbb{F}_{2^n}$.

Toward a full classification of all APN functions, an approach is to show that certain polynomials are not APN for an infinity of extension of $\mathbb{F}_2$. Hernando and McGuire showed a result on classification of APN functions which was conjectured for 40 years : the only exponents such that the monomial x^d is APN over an infinity of extension of $\mathbb{F}_2$ are of the form 2^i+1 or 4^i-2^i+1. Those exponents are called *exceptional exponents*. It lead Aubry, McGuire and Rodier to formulate the following conjecture:

Conjecture: (Aubry, McGuire and Rodier) a polynomial can be APN for an infinity of ground fields $\mathbb{F}_q$ if and only if it is CCZ-equivalent (as defined by Carlet, Charpin and Zinoviev in [3]) to a monomial x^d where d is exceptional exponent.

A way to prove this conjecture is to remark that being APN is equivalent to the fact that the rational points of a certain algebraic surface X in a 3-dimensional space linked to the polynomial f defining the Boolean function are all in a surface V made of 3 planes and independant of f. We define the surface X in the 3-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 the surface is irreducible or 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 it means the surface is too big to be contained in the surface V and the function f cannot be APN.

This way enabled Rodier to prove in [2] that when the degree of f is equal to $4e$ with $e\equiv 3\,(\mathrm{mod}\,4)$ and ϕ is not dividable by a certain form of polynomial then f is not APN for an infinity of extension of $\mathbb{F}_q$. He also found all the APN function of degree 12 and proved they are all CCZ-equivalent to x^3.

To continue in this way, let's get interested in the APN functions of degree 20 which were the next ones on the list. The main difference in this case is that $e\equiv 1\,(\mathrm{mod}\,4)$. We got inspired by the proof of Rodier in [2] but we had an other approach using divisors of the surface $\bar{X}$. This was due to the fact that some of the components of $\bar{X}$ are no longer irreducible in our case.

Then we were able to obtain all the APN functions of degree 20 by calculation. The conditions of divisibility by the polynomials we obtained made the first part of our work, we had to work on the quotient after to obtain the final forms of the functions. The second part was to prove that all were CCZ-equivalent to x^5.

This work has been done with François Rodier as adviser.