Algebraic geometry and symmetric cryptography

Y. Aubry[1] G. McGuire[2] F. Rodier[1]

[1]IML – Marseille
[2]University College Dublin

Outline

APN functions.

- Vectorial Boolean functions are useful in private key cryptography for designing block ciphers.
- Two main attacks on these ciphers are differential attacks and linear attacks.
  An important criterion on Boolean functions is a high resistance to the differential cryptanalysis.
- Kaisa Nyberg has introduced the notion of almost perfect nonlinearity (APN) to characterize those functions which have the better resistance to differential attacks.

APN functions

Let us consider a vectorial Boolean function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$.

If we use the function f in a S-box of a cryptosystem, the efficiency of differential cryptanalysis is measured by the maximum of the cardinality of the set of elements x in $\mathbb{F}_2^m$ such that

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

where a and b are elements in $\mathbb{F}_2^m$ and $a \neq 0$.

Definition

The function f is said to be APN (almost perfect nonlinear) if for every $a \neq 0$ in $\mathbb{F}_2^m$ and $b \in \mathbb{F}_2^m$, there exists at most 2 elements x of $\mathbb{F}_2^m$ such that

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

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).
- $d = 2^{2h} - 2^h + 1$ where $\gcd(h, m) = 1$ (Kasami functions).

- and other functions with exponent d depending on m
  - $d = 2^{(m-1)/2} + 3$ with m odd (Welch functions).
  - $d = 2^{(m-1)/2} + 2^{(m-1)/4} - 1$, where $m \equiv 1 \pmod 4$, $d = 2^{(m-1)/2} + 2^{(3m-1)/4} - 1$, where $m \equiv 3 \pmod 4$ (Niho functions).
  - $d = 2^m - 2$, for m odd; (inverse function)
  - $d = 2^{4m/5} + 2^{3m/5} + 2^{2m/5} + 2^{m/5} - 1$, where m is divisible by 5 (Dobbertin functions).

One conjectured for a long time that the Gold and Kasami functions are the only ones where d is independent from m and which give APN functions for an infinity of values of m.

APN power functions

Janwa, McGuire, Wilson, Jedlicka worked on this conjecture.

Fernando Hernando and Gary McGuire proved recently the following theorem:

Theorem

The Gold and Kasami functions are the only monomials where d is odd and which give APN functions for an infinity of values of m.

Other APN functions

In 2005, Edel, Kyureghyan and Alexander Pott have proved that the function

$$\begin{array}{ccc} \mathbb{F}_{2^{10}} & \longrightarrow & \mathbb{F}_{2^{10}} \\ x & \longmapsto & x^3 + ux^{36} \end{array}$$

where u is a suitable element in the multiplicative group $\mathbb{F}_{2^{10}}^*$ was APN and not equivalent to power functions.

A number of people (Budaghyan, Carlet, Felke, Leander, Bracken, Byrne, Markin, McGuire, Dillon. . .) showed that certain quadratic polynomials were APN and not equivalent to known power functions.

New Conjecture

G. McGuire proposed the following conjecture.

Conjecture

The Gold and Kasami functions are the only APN functions which are APN on infinitely many extensions of their field of definition.

We will give some results toward this conjecture.

Toward the classification of APN functions

Some results toward the classification of APN functions given by polynomials have been proved by

- Berger, Canteaut, Charpin, Laigle-Chapuy,
- Byrne and McGuire,
- Brinkman and Leander,
- Voloch . . .

They prove results mainly on quadratic functions or binomials.

We will give here some bound on the degree of a Boolean polynomial not to be almost perfect nonlinear.

Result on monomials

To solve the problem of APN monomials Janwa and Wilson studied the following curve:

$$\frac{x^d + y^d + 1 + (x + y + 1)^d}{(x + y)(x + 1)(y + 1)} = 0$$

Proposition (Anne Canteaut)

Suppose that this curve is absolutely irreducible over $\mathbb{F}_2$. The mapping $x \longmapsto x^d$ is not APN over $\mathbb{F}_q$, $q \geq 32$, if

$$d \leq q^{1/4} + 4.5$$

Equivalent polynomials

A *q*-affine polynomial is a polynomial whose monomials are of degree 0 or a power of 2.

Proposition

The class of APN functions is invariant by addition of a q-affine polynomial.

We choose for f a polynomial mapping from $\mathbb{F}_{2^m}$ in itself

- which has no term of degree a power of 2
- and with no constant term.

Characterization of APN polynomials

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself. We can rephrase the definition of an APN function.

Proposition

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ *is APN if and only if the surface*

$$f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2) = 0$$

has all of its rational points contained in the surface

$$(x_0 + x_1)(x_2 + x_1)(x_0 + x_2) = 0.$$

A first bound for the degree of an APN polynomial

Theorem

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, d its degree.

Suppose that the surface X with affine equation

$$\frac{f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)}{(x_0+x_1)(x_2+x_1)(x_0+x_2)}=0$$

is absolutely irreducible.

Then, if $9 \leq d < 0.45q^{1/4}+0.5$, f is not APN.

Sketch of proof

- The number of rational points on the surface X is bounded. From an improvement of Lang-Weil's bound by Ghorpade-Lachaud, we deduce

$$|\#\overline{X}(\mathbb{F}_q) - q^2 - q - 1| \leq (d-4)(d-5)q^{3/2} + 18d^4q.$$

- If f is APN and d too large, then the surface X has too many rational points to be contained in the surface $(x_0 + x_1)(x_2 + x_1)(x_0 + x_2) = 0$.

Irreducibility of X

Criterion for the surface X to be irreducible.

Proposition

Let f be a polynomial of $\mathbb{F}_q$ to itself, d its degree. Let us suppose that the curve X_∞ with homogeneous equation

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is absolutely irreducible. Then the surface X of affine equation

$$\frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is absolutely irreducible.

The curve X_∞ is the intersection of the surface X with the plane at infinity.

Irreducibility of X_∞

F. Hernando and G. McGuire have studied the curve X_∞.

Proposition

The curve X_∞ of degree d is absolutely irreducible for

- *d odd of the form $d = 2^i\ell + 1$ with ℓ odd;*
- *ℓ does not divides $2^i - 1$;*

Proposition

The curve X_∞ of degree d has an irreducible component defined over $\mathbb{F}_2$ for

- *$d = 2^j(2^i\ell + 1)$ with ℓ odd;*
- *where $\ell \neq 1$ or $2^i - 1$;*

We conjecture that the bound for f to be APN is also true in this case.

A second bound

We can improve the bound for some cases.

Theorem

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, d its degree.
Let us suppose that d is not a power of 2 and that the surface X

$$\frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

has only a finite number of singular points.
Then if $10 \leq d < q^{1/4} + 4$, f is not APN.

The number of rational points on the surface X is bounded from an improvement of a theorem of Deligne on Weil's conjectures by Ghorpade-Lachaud.

Singular points on X

Proposition

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, d its degree. Let us suppose that the curve X_∞ of equation

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is smooth.
Then the surface X has only a finite number of singular points.

Janwa and Wilson have studied the curve X_∞ and have deduced a certain number of cases where it is nonsingular.

In particular the condition is satisfied if $d = 2l + 1$ and l is a prime number congruent to ± 3 modulo 8.

Some perspective – The conjecture on APN function

We have shown that many polynomials cannot be APN

if their degrees are too large with respect to the number of variables

It is a consequence of bounds of the Weil type on some surfaces on finite fields.

To prove the conjecture on APN function we have

- to prove the bound for several classes of degrees not Gold or Kasami;
- to study polynomials of Gold or Kasami degree.

For small degrees, it works.

Some perspective – Differentially 4-uniform functions

Let δ be the maximum of the cardinality of the set of elements x in $\mathbb{F}_2^m$ such that

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

where a and b are elements in $\mathbb{F}_2^m$ and $a \neq 0$.

To study Boolean functions with $\delta = 4,\ 6 \ldots$

Some perspective – Differentially 4-uniform function

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is differentially 4-uniform if and only if the set of points (x, y, z, t) such that

$$S \quad \begin{cases} f(x) + f(y) + f(z) + f(x + y + z) = 0 \\ f(x) + f(y) + f(t) + f(x + y + t) = 0 \end{cases}$$

is contained in the hypersurface
$(x + y)(x + z)(x + t)(y + z)(y + t)(z + t)(x + y + z + t) = 0.$

The surface S is reducible.
Can one get a nice bound?

THANK YOU