Fonctions booléennes cryptographiquement robustes

Yves Aubry[1] Gregor Leander[2] Gary McGuire[4]
François Rodier[3]

[1] Imath – Toulon
[2] Technical University of Danemark
[4] Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography
[3] IML – Marseille

Outline

Boolean 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 in 1993 the notion of differential uniformity and 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 $a \neq 0$.
Since this number is obviously even and is nonzero, its least value is 2.

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.

- The function x^d is APN if and only if the equation

$$x^d + y^d + z^d + (x + y + z)^d = 0$$

has only solutions such that $(x + y)(x + z)(y + z) = 0$.

- If the curve

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

is irreductible, Weil's inequality shows that it has too many rational points if the field $\mathbb{F}_{q^n}$ is too big.

- To show that it is irreducible, one studies singular points.
- In fact we show that if d is not a Gold or Kasami exponent, this curve has an absolutely irreducible factor defined on $\mathbb{F}_2$, which is enough.

CCZ equivalence

Carlet, Charpin and Zinoviev have defined an equivalence relation between Boolean functions.

For a function f of $\mathbb{F}_2^m$ in itself we denote by G_f the graph of the function f:

$$G_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^m\}.$$

Definition

The functions $f, f' : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ are equivalent in the sense of Carlet-Charpin-Zinoviev (CCZ equivalence) if there exist a linear permutation $L : \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2^{2m}$ such that $L(G_f) = G_{f'}$.

Proposition

If f and f' are CCZ equivalent, then f is APN if and only if f' is.

APN function not equivalent to a power function

First example:

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

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

where ω is a primitive cube root of unity in $\mathbb{F}_{2^{10}}^*$ was APN and not CCZ equivalent to a power function.

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

Dillon found an APN polynomial on $\mathbb{F}_{2^6}$ which was a permutation.
First APN permutation on an even number of variables.
Not CCZ equivalent to a power function.

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
    They prove that a large class of quadratic functions cannot be APN.
  - by Byrne and McGuire
    Many quadratic functions, are not APN functions over an extension of the base field.
  - by Brinkman and Leander,
    APN functions with at most 5 variables are equivalent to power functions.
  - by Voloch
    Many binomials are not APN functions over an extension of the base field.
  - ...
- We will give here some bound on the degree of a Boolean polynomial not to be APN.

Equivalent polynomials

An affine 2-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 an affine 2-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*

$$f(x) + f(y) + f(z) + f(x + y + z) = 0$$

has all of its rational points contained in the surface

$$(x + y)(z + y)(x + z) = 0.$$

A first bound for the degree of an APN polynomial

Lemma

Let us suppose that the degree d of f is not a power of 2 and $d \geq 5$. If f is APN and if the affine surface X

$$\frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$

is absolutely irreducible, then the corresponding projective surface has at most $4((d-3)q+1)$ rational points.

$X: \quad \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$

Proof –

The intersection of the surface $\overline{X}$ with the plane $x + y = 0$ is a curve of degree $d - 3$.

This curve has at most $(d-3)q+1$ rational points from Serre's bound.

The same for the plane at infinity.

If f is APN, the surface $\overline{X}$ has no other rational points than those in the union of the plane $x + y = 0$, $z + y = 0$ and $x + z = 0$ or the plane at infinity.

So it has an most $4((d-3)q+1)$ rational points.

A first bound for the degree of an APN polynomial

We have the following result:

Theorem (FR)

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

$$\frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(z+y)(x+z)}=0$$

is absolutely irreducible.

Then if

$$9 \leq d < 0.45q^{1/4}+0.5$$

f is not APN.

Skech of proof

- The surface X has a number of rational points bounded by a bound à la Weil.

  More exactly, thanks to an improvement of Lang-Weil's bound by Ghorpade-Lachaud, one 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 q too big, then the surface X has too many rational points to be contained in the surface $(x+y)(z+y)(x+z) = 0$.

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 d is not a power of 2 and that the curve X_∞ with homogeneous equation

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

is absolutely irreducible.

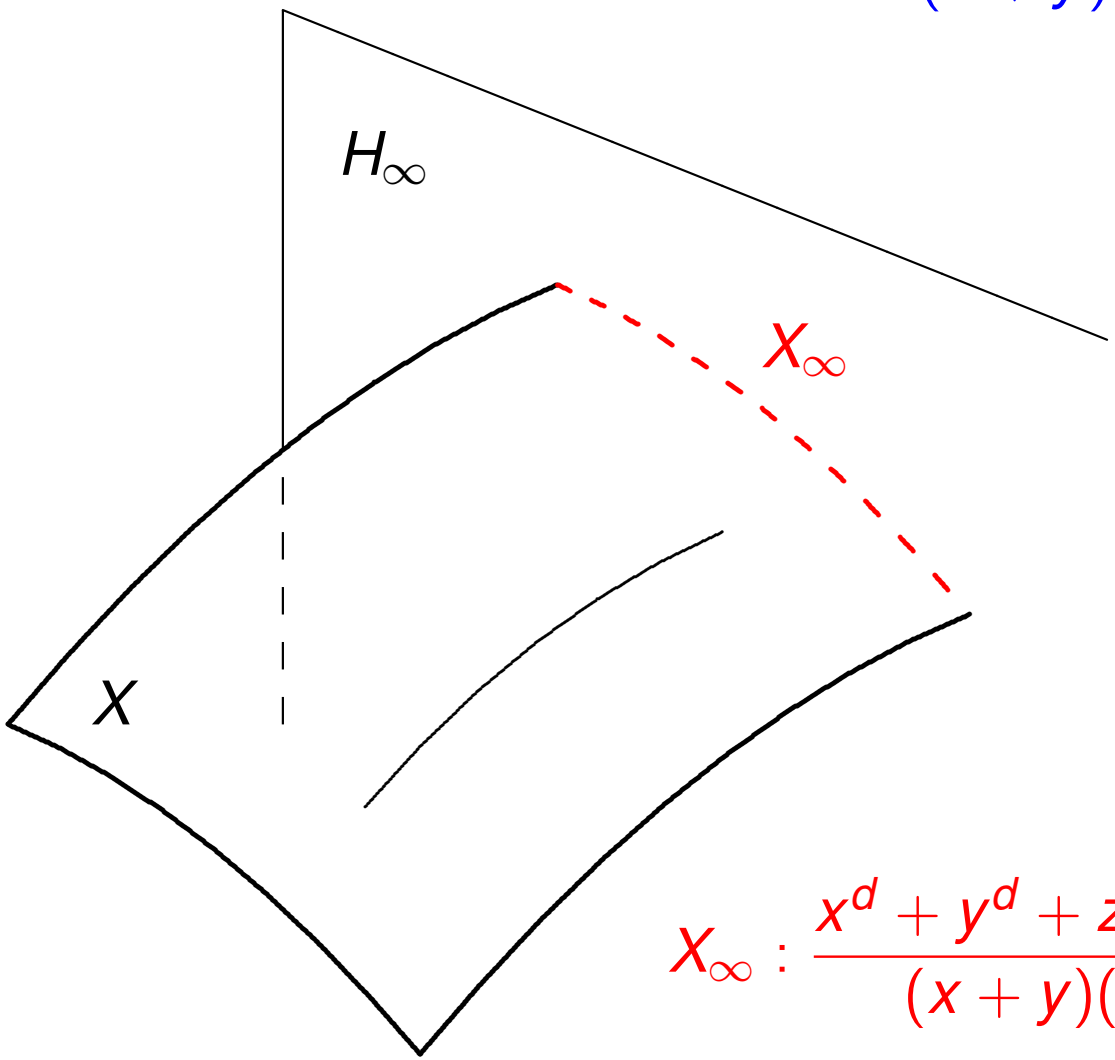
Then the surface X of affine equation

$$\frac{f(x) + f(y) + f(z) + f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$

is absolutely irreducible.

Irreducibility of X

$$X : \frac{f(x) + f(y) + f(z) + f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$



$$X_\infty : \frac{x^d + y^d + z^d + (x+y+z)^d}{(x+y)(z+y)(x+z)} = 0$$

Proposition

X_∞ *absolutely irreducible* $\Rightarrow X$ *absolutely irreducible*

Irreducibility of X_∞

Janwa, McGuire and Wilson have studied the curve X_∞ and have deduced a certain number of cases where it is absolutely irreducible.

Proposition

The curve X_∞ is absolutely irreducible for

$$d \equiv 3 \pmod 4$$

or

$$d \equiv 5 \pmod 8 \quad \textit{and} \quad d > 13.$$

The conjecture on APN functions

Irreducibility of X_∞

Let $\mathbb{F}_q$ the field of definition of f.
If the surface X is absolutely irreducible,has an irreducible component defined over $\mathbb{F}_q$
then the polynomial function f can be APN only for a finite number of extensions.

Proposition

If X_∞ has an irreducible component defined over $\mathbb{F}_2$ then X has an irreducible component defined over $\mathbb{F}_q$

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

Proposition

The curve X_∞ of degree d has an irreducible component defined over $\mathbb{F}_2$ for d odd, not equal to Gold or Kasami exponent.

The conjecture on APN functions

Polynomials of odd degree d

Theorem (Aubry, McGuire, Rodier)

If the degree of the polynomial function f is d with d odd, not equal to Gold or Kasami exponent, then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

The conjecture on APN functions

Polynomials of degree $d = 2e$

Theorem (Aubry, McGuire, Rodier)

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.

Let

$$\phi_r = \frac{x^r + y^r + z^r + (x+y+z)^r}{(x+y)(z+y)(x+z)}.$$

The equation of X_∞ is

$$\phi_{2e}(x,y,z) = \phi_e^2(x,y,z)(x+y)(z+y)(x+z) = 0$$

The component of X_∞ which contains the line $x + y = 0$ in the plane at infinity is defined over $\mathbb{F}_2$.
It corresponds to a component of X defined over $\mathbb{F}_q$.

The conjecture on APN functions

Polynomials of degree $d = 4e$

Theorem (FR)

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.

This case is far more intricate than the previous cases, because there are some polynomials which are CCZ equivalent to monomials for $e = 3$.

The conjecture on APN functions

Polynomials of degree $d = 4e$

Sketch of proof. We have in this case:

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

Let X_0 a reduced absolutely irreducible component of X which contains the line $x + y = 0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,
- and the action of the Galois group of the field of definition of X_0 over $\mathbb{F}_q$

one is reduced to the case where

- there are three components X_0, X_1 and X_2 which contain each of the 3 lines, they are defined over the field $\mathbb{F}_{q^3}$,
- X_0, X_1 and X_2 are of the form $(x + y)(x + z)(y + z) + P$ where P is a polynomial of the form

$$P(x, y, z) = c_1(x^2 + y^2 + z^2) + c_2(xy + xz + zy) + b(x + y + z) + d$$

Investigating these polynomials, one proves that it is impossible that they divide ϕ for $e \neq 3$.

The conjecture on APN functions

Polynomials of degree $d = 4 \times 3$

Theorem (FR)

If the degree of the polynomial f is 12, then

- *either f is not APN over $\mathbb{F}_{q^n}$ for n 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.

The conjecture on APN functions

Polynôme de degré d = degré de Gold

Theorem (Aubry, McGuire, Rodier)

Suppose $f(x) = x^d + g(x)$ *where*
the degree of f *is* $d = 2^k + 1$ *and* $\deg(g) \leq 2^{k-1} + 1$.
Suppose moreover that there exists a nonzero coefficient of x^r *in* g *such that*

$$\frac{x^r + y^r + z^r + (x+y+z)^r}{(x+y)(z+y)(x+z)}$$

is irreducible.
Then X *is absolutely irreducible.*

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

Computation of some examples

As we get explicit bounds, we could make some computations.

Theorem

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

Suppose that the surface X is absolutely irreducible.

Then if

$$9 \leq d < 0.45q^{1/4} + 0.5$$

f is not APN.

A second bound

We can improve the bound for some cases.

Theorem (FR)

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

$$\frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(z+y)(x+z)}=0$$

has only a finite number of singular points.
Then if

$$10 \leq d < q^{1/4}+4,$$

f is not APN.

- Improvement of Lang et Weil's bound by Deligne and by Ghorpade-Lachaud
- Sufficient conditions so that there is only a finite number of singular points has been given by Janwa et Wilson

Proposition

The surface X has only a finite number of singular points for the values of $d = 2l + 1$ where

- *l is an odd integer such as there exists an integer r with $2^r \equiv -1 \pmod{l}$.*
- *l is a prime number larger than 17 such as the order of 2 modulo l is $(l-1)/2$.*

In particular the first condition is satisfied if l is a prime number congruent to ± 3 modulo 8.

Numerical examples

When the surface X is irreducible, the function f can be APN only if $m \leq m_{max}$ where m_{max} is given by the following table.

$d \leq$	7	9	10	12	15	17	21	23	29	36	41	49
m_{max}	15	16	17	18	19	20	21	22	23	24	25	26

When moreover the surface X has only a finite number of singularities, the function f can be APN only if $m \leq m_{max}$ where m_{max} is given by the following table.

$d \leq$	7	9	10	12	13	15	17	20	23	26	30	36
m_{max}	6	9	10	11	12	13	14	15	16	17	18	19

Polynomials of small degrees

- For polynomials of small degrees (up to 9) we deduced with Leander that there was no other APN functions than the ones which are already known.

Mappings $x^{-1} + g(x)$

Theorem (Leander, Rodier)

Let g be a polynomial mapping from $\mathbb{F}_q$ in itself, d its degree. Then, if $5 \leq d < 0.45q^{1/4} - 4.5$, $f = x^{q-2} + g$ is not APN.

Proof

The surface X is of degree $q - 5$.
We study instead the surface X'

$$\frac{g(x) + g(y) + g(z) + g(x + y + z)}{(x + y)(z + y)(x + z)} xyz(x + y + z) = 1$$

The surface X' is irreducible.
If f is APN then $X'(\mathbb{F}_q) \leq 8dq + 4$.

Example

The functions $x^{q-2} + ax^d$ for $a \neq 0$, exponents d up to 29 and not a power of 2 are not APN.

Differentially 4-uniform functions

Definition

The function f is said to be differentially 4-uniform if for every $a \neq 0$ in $\mathbb{F}_2^m$ and $b \in \mathbb{F}_2^m$, there exists at most 4 elements x of $\mathbb{F}_2^m$ such that

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

Characterization of differentially 4-uniform functions

Let f be a polynomial mapping of $\mathbb{F}_q$ in itself. We have the following result:

Theorem (Aubry, Rodier)

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?

Differentially 4-uniform function

One can get a conclusion for some functions.

Theorem (Aubry, Rodier)

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, of degree $d = 2^r - 1$.

Then, if $31 \leq d < q^{1/8} + 2$, f has differential uniformity greater than 6.

Conclusion

Criteria for Boolean functions

We have shown that many polynomials cannot be APN or differentially 4-uniform

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.

Conclusion

The conjecture on APN functions

To prove the conjecture on APN functions we have

- to prove the bound for several classes of degrees not Gold or Kasami;
  I mean $d = 2^i(2^i\ell + 1)$ with $\ell \neq 1$ and $\ell \neq 2^i - 1$ and $i \geq 2$.
- to study polynomials of Gold or Kasami degree.

Conclusion

Some perspectives

- To get more numerical values
- To study other Boolean functions with differential uniformity 4
- To study polynomial functions of degree 10, ...
- To study polynomial functions of low degrees plus a quadratic function.
- Can one get better bounds on m and d by studying the special form of the surface X (for instance the symmetry of the equation in x, y, z)?

Merci