Polynomials on $\mathbb{F}_{2^m}$ with good resistance to cryptanalysis

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

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

Outline

APN functions

A lower bound for the degree of an APN polynomial

- Characterization of APN polynomials
- A lower bound
- Some examples

Some prospect as a conclusion

Outline

APN functions

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

APN functions

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

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 functions

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

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

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

If we use the function f in a S-box of a cryptosystem, they are the functions which resist best to differential cryptanalysis.

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).

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).

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

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

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

F. Hernando and G. McGuire proved recently the following :

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

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

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

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.

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

New Conjecture

G. McGuire proposed the following conjecture about APN functions.

Conjecture

The Gold and Kasami power function (up to equivalence) are the only APN functions which are APN on infinitely many extensions of their field of definition.

New Conjecture

G. McGuire proposed the following conjecture about APN functions.

Conjecture

The Gold and Kasami power function (up to equivalence) 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.

Result on monomials

We will generalize this result on monomials by Anne Canteaut.

Proposition

Suppose that the curve

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

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

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

Outline

Characterisation of APN polynomials

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself.

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

Characterisation of APN polynomials

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself.

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

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 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.

Sketch of proof

- The number of rational points on the surface X is bounded.

  One has bound of Weil type for $\overline{X}(\mathbb{F}_q)$.

Sketch of proof

- The number of rational points on the surface X is bounded.

  One has bound of Weil type for $\overline{X}(\mathbb{F}_q)$.

  Namely from an improvement of Lang-Weil's bound by Ghorpade-Lachaud, we deduce

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

Sketch of proof

- The number of rational points on the surface X is bounded.

  One has bound of Weil type for $\overline{X}(\mathbb{F}_q)$.

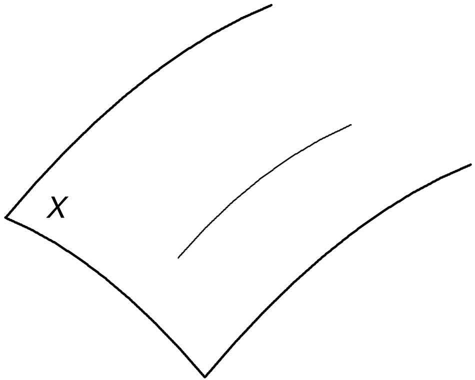
  Namely from an improvement of Lang-Weil's bound by Ghorpade-Lachaud, we deduce

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

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

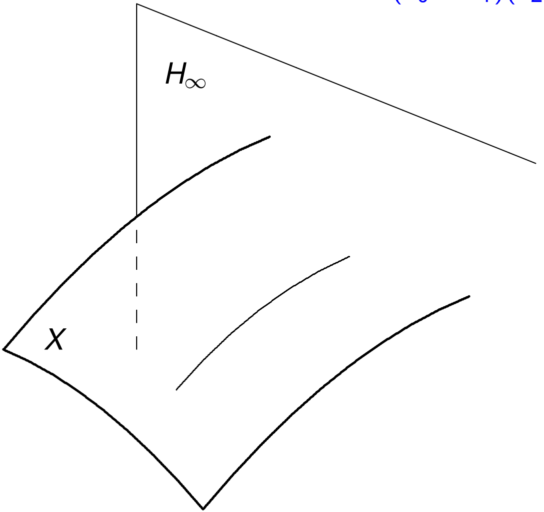
Irreducibility of X

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



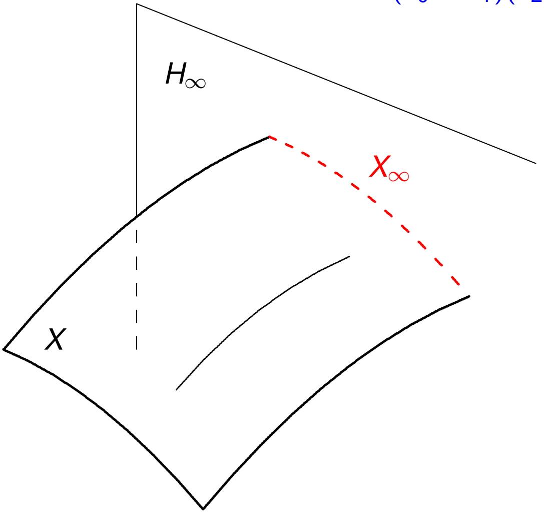
Irreducibility of X

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



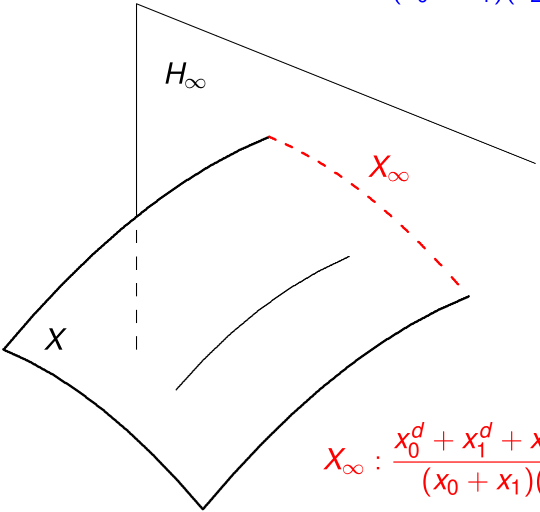
Irreducibility of X

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



Irreducibility of X

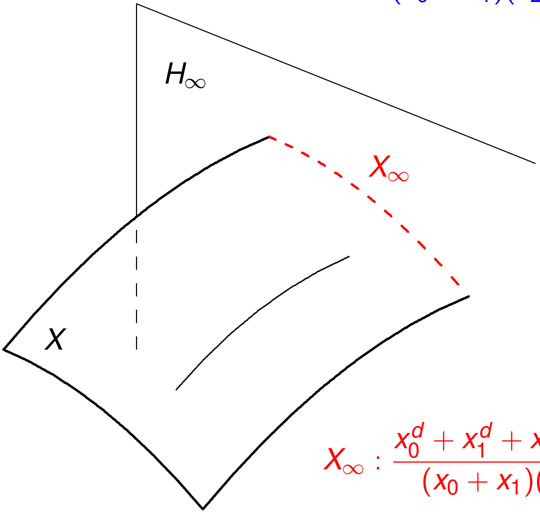
$$X : \frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$



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

Irreducibility of X

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



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

X_∞ absolutely irreducible $\Rightarrow X$ absolutely irreducible

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* $2^i - 1$*;*

Computation of some examples

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

Computation of some examples

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

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

Outline

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 $i \geq 1$.

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 $i \geq 1$.
- to study polynomials of Gold or Kasami degree.

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 $i \geq 1$.
- to study polynomials of Gold or Kasami degree.

Proposition

Suppose $f(x) = x^d + g(x)$ *where*
the degree of f *is* $d = 2^k + 1$ *and* $\deg(g) \leq 2^{k-1} + 1$.
Then X *is absolutely irreducible.*

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

Differentially 4-uniform function

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is 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

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

Differentially 4-uniform function

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is 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

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

The function is differentially 4-uniform if and only if the set of points $(x, y, z, t) \in \mathbb{F}_q^4$ 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
$(x+y)(x+z)(x+t)(y+z)(y+t)(z+t)(x+y+z+t) = 0.$

Differentially 4-uniform function

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

Differentially 4-uniform function

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

The surface S is reducible.

Can one get a nice bound?

Differentially 4-uniform function

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

The surface S is reducible.

Can one get a nice bound?

One can get a conclusion for some functions.

Proposition

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 is not differentially 4-uniform.

THANK YOU