Bounds on the degree of APN polynomials
The Case of $x^{-1} + g(x)$

G. Leander[1] F. Rodier[2]

[1] Department of Mathematics
Technical University of Denmark
Denmark

[2] Institut de Mathématiques de Luminy
Marseille
France

Outline

Outline

APN functions.

- Vectorial Boolean functions are useful in private key cryptography for designing block ciphers.

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.

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 $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$.

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 best 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
  - $d = 2^{(m-1)/2} + 3$ 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).

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.

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

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

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

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

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

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

Towards a full classification of all APN functions

One approach that already proved to be successful:
to show that certain polynomials are not APN for infinitely many extensions of $\mathbb{F}_2$.

Towards a full classification of all APN functions

One approach that already proved to be successful:
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 ask the question:
Can this function be APN on infinitely many extensions of $\mathbb{F}_q$?

Towards a full classification of all APN functions

One approach that already proved to be successful:
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 ask the question:
Can this function 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.

Towards a full classification of all APN functions

One approach that already proved to be successful:
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 ask the question:
Can this function 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.

More precisely, we will give here some bound on the degree of a Boolean polynomial not to be almost perfect nonlinear.

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

Equivalent polynomials

Proposition

The class of APN functions is invariant by addition of a q-affine polynomial (that is a polynomial whose monomials are of degree 0 or a power of 2).

Equivalent polynomials

Proposition

The class of APN functions is invariant by addition of a q-affine polynomial (that is a polynomial whose monomials are of degree 0 or a power of 2).

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.

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

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

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 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.

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.

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 $2^i - 1$;*

Irreducibility of X

Proposition

If f is of degree d then the bound for f to be APN is true for

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

Irreducibility of X

Proposition

If f is of degree d then the bound for f to be APN is true for

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

One can prove also some improvements.

Proposition

The bound for f to be APN is true for

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

A second bound

In most of the cases the surface X can be shown to have a finite number of singular points

A second bound

In most of the cases the surface X can be shown to have a finite number of singular points (that is points where the surface X is not locally isomorphic to a manifold).

A second bound

In most of the cases the surface X can be shown to have a finite number of singular points (that is points where the surface X is not locally isomorphic to a manifold).

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.

A second bound

In most of the cases the surface X can be shown to have a finite number of singular points (that is points where the surface X is not locally isomorphic to a manifold).

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.

This is due to an improvement of a theorem of Deligne on Weil's conjectures by Ghorpade-Lachaud

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

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

We study the function

$$f(x) = \qquad\qquad x^{-1} + g(x)$$

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

We study the function

$$f(x) = x^{q-2} + g(x) = x^{-1} + g(x)$$

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

We study the function

$$f(x) = x^{q-2} + g(x) = x^{-1} + g(x)$$

Proposition

Let g be a polynomial mapping from $\mathbb{F}_q$ in itself, d its degree. Then if

$$5 \leq d < 0.45q^{1/4} - 3.5$$

f is not APN.

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

We study the function

$$f(x) = x^{q-2} + g(x) = x^{-1} + g(x)$$

Proposition

Let g be a polynomial mapping from $\mathbb{F}_q$ in itself, d its degree. Then if

$$5 \leq d < 0.45q^{1/4} - 3.5$$

f is not APN.

Functions of this form are particularly interesting for cryptography as important criteria for functions used in symmetric ciphers are

- high algebraic degree
- balancedness

as is achieved by functions of this form.

$f(x) = x^{q-2} + g(x)$

Proof

- The surface X is of degree $q - 5$.

$f(x) = x^{q-2} + g(x)$ $\qquad xf(x) = 1 + xg(x)$

Proof

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

$$\frac{g(x_0) + g(x_1) + g(x_2) + g(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} x_0 x_1 x_2 (x_0 + x_1 + x_2) = 1$$

$f(x) = x^{q-2} + g(x)$ $\qquad xf(x) = 1 + xg(x)$

Proof

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

$$\frac{g(x_0) + g(x_1) + g(x_2) + g(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} x_0 x_1 x_2 (x_0 + x_1 + x_2) = 1$$

- The surface X' is irreducible.

$f(x) = x^{q-2} + g(x)$ $\qquad xf(x) = 1 + xg(x)$

Proof

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

$$\frac{g(x_0) + g(x_1) + g(x_2) + g(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} x_0 x_1 x_2 (x_0 + x_1 + x_2) = 1$$

- The surface X' is irreducible.
  Hence the number of rational points of X' is bounded
  by Lang-Weil ang Ghorpade-Lachaud bound.

$f(x) = x^{q-2} + g(x)$ $\qquad xf(x) = 1 + xg(x)$

Proof

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

$$\frac{g(x_0) + g(x_1) + g(x_2) + g(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} x_0 x_1 x_2 (x_0 + x_1 + x_2) = 1$$

- The surface X' is irreducible.
  Hence the number of rational points of X' is bounded
  by Lang-Weil ang Ghorpade-Lachaud bound.
- If f is APN
  then $X'(\mathbb{F}_q)$ is contained in the union of 4 planes
  and $\#X'(\mathbb{F}_q) \leq 4dq + 4q + 8$.

Computer experiment

For the functions of the form $x^{-1} + g(x)$ we deduced that there was no other APN function for $m \geq 4$

- for $\deg g \leq 6$
- or for g a monomial, up to degree 25.

Outline

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 have given some results toward this conjecture.

THANK YOU