Almost Perfect Nonlinear Functions

Faruk Göloğlu

Claude Shannon Institute, University College Dublin

CSI Workshop on Coding and Cryptography, UCC
May 18, 2010

Block Ciphers

Block Ciphers

- A Block Cipher can be seen as:

$$\mathcal{B} : \{0,1\}^m \rightarrow \{0,1\}^m.$$

Block Ciphers

- A Block Cipher can be seen as:

$$\mathcal{B} : \{0,1\}^m \to \{0,1\}^m.$$

- Claude Shannon introduced the properties *confusion* and *diffusion*.

Block Ciphers

- A Block Cipher can be seen as:

$$\mathcal{B} : \{0,1\}^m \to \{0,1\}^m.$$

- Claude Shannon introduced the properties *confusion* and *diffusion*.
- Confusion introduces complexity or non-linearity to the system

Block Ciphers

- A Block Cipher can be seen as:

$$\mathcal{B} : \{0,1\}^m \to \{0,1\}^m.$$

- Claude Shannon introduced the properties *confusion* and *diffusion*.
- Confusion introduces complexity or non-linearity to the system and achieved generally by the S-Box.

Block Ciphers

- A Block Cipher can be seen as:

$$\mathcal{B} : \{0,1\}^m \to \{0,1\}^m.$$

- Claude Shannon introduced the properties *confusion* and *diffusion*.
- Confusion introduces complexity or non-linearity to the system and achieved generally by the S-Box.

Question

How do we define non-linearity?

Nonlinearity

Definition

Non-linearity of a function is the 'distance' of it to all linear (affine) functions.

Nonlinearity

Definition

Non-linearity of a function is the 'distance' of it to all linear (affine) functions.

We are interested in *Vectorial Boolean Functions*, i.e.,

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

Nonlinearity

Definition

Non-linearity of a function is the 'distance' of it to all linear (affine) functions.

We are interested in *Vectorial Boolean Functions*, i.e.,

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

Let $\mathbb{F} = \mathbb{F}_{2^m}$. For a linear function l:

$$l(x) + l(x + a) = l(a),$$

for any $x \in \mathbb{F}$, i.e.,

Nonlinearity

Definition

Non-linearity of a function is the 'distance' of it to all linear (affine) functions.

We are interested in *Vectorial Boolean Functions*, i.e.,

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

Let $\mathbb{F} = \mathbb{F}_{2^m}$. For a linear function l:

$$l(x) + l(x + a) = l(a),$$

for any $x \in \mathbb{F}$, i.e.,

$$D_l(a) := \{l(x) + l(x + a) : x \in \mathbb{F}\} = \{l(a)\}.$$

Nonlinearity

Definition

Non-linearity of a function is the 'distance' of it to all linear (affine) functions.

We are interested in *Vectorial Boolean Functions*, i.e.,

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

Let $\mathbb{F} = \mathbb{F}_{2^m}$. For a linear function l:

$$l(x) + l(x + a) = l(a),$$

for any $x \in \mathbb{F}$, i.e.,

$$D_l(a) := \{l(x) + l(x + a) : x \in \mathbb{F}\} = \{l(a)\}.$$

By 'non-linear' we mean $\#D_f(a)$ as large as possible.

APN functions

How large can $\#D_f(a)$ be?

APN functions

How large can $\#D_f(a)$ be?
If $\mathbb{F} = \mathbb{F}_{2^m}$ then

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

APN functions

How large can $\#D_f(a)$ be?
If $\mathbb{F} = \mathbb{F}_{2^m}$ then

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

Hence, $\#D_f(a) \leqslant 2^{m-1}$.

APN functions

How large can $\#D_f(a)$ be?
If $\mathbb{F} = \mathbb{F}_{2^m}$ then

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

Hence, $\#D_f(a) \leqslant 2^{m-1}$.

Definition

f is *Almost Perfect Nonlinear (APN)* if for all $a \in \mathbb{F}^*$,

$$\#D_f(a) = 2^{m-1}.$$

APN functions

How large can $\#D_f(a)$ be?
If $\mathbb{F} = \mathbb{F}_{2^m}$ then

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

Hence, $\#D_f(a) \leqslant 2^{m-1}$.

Definition

f is *Almost Perfect Nonlinear (APN)* if for all $a \in \mathbb{F}^*$,

$$\#D_f(a) = 2^{m-1}.$$

If characteristic of $\mathbb{F}$ is odd, Perfect Nonlinear functions exist.

APN example

Let $f = x^3$.

APN example

Let $f = x^3$.

$$\begin{aligned} D_f(a) &= \{x^3 + (x+a)^3\} \\ &= \{x^3 + x^3 + x^2a + a^2x + a^3\} \\ &= \{x^2a + a^2x + a^3\} \\ &= \{a^3\left[\left(\frac{x}{a}\right)^2 + \frac{x}{a} + 1\right]\} \\ &= \{a^3(y^2 + y + 1)\} \end{aligned}$$

with $ay = x$.

APN example

Let $f = x^3$.

$$\begin{aligned} D_f(a) &= \{x^3 + (x+a)^3\} \\ &= \{x^3 + x^3 + x^2a + a^2x + a^3\} \\ &= \{x^2a + a^2x + a^3\} \\ &= \{a^3\left[\left(\frac{x}{a}\right)^2 + \frac{x}{a} + 1\right]\} \\ &= \{a^3(y^2 + y + 1)\} \end{aligned}$$

with $ay = x$.

- $H_\alpha := \{x \in \mathbb{F} \ : \ \mathrm{Tr}\,(\alpha x) = 0\}$, where $\mathrm{Tr}\,(z) = z + z^2 + \cdots + z^{2^{m-1}}$.

APN example

Let $f = x^3$.

$$\begin{aligned} D_f(a) &= \{x^3 + (x+a)^3\} \\ &= \{x^3 + x^3 + x^2 a + a^2 x + a^3\} \\ &= \{x^2 a + a^2 x + a^3\} \\ &= \{a^3 \left[\left(\frac{x}{a}\right)^2 + \frac{x}{a} + 1 \right]\} \\ &= \{a^3 (y^2 + y + 1)\} \end{aligned}$$

with $ay = x$.

- $H_\alpha := \{x \in \mathbb{F} \ : \ \mathrm{Tr}\,(\alpha x) = 0\}$, where $\mathrm{Tr}\,(z) = z + z^2 + \cdots + z^{2^{m-1}}$.
- Image of $y^2 + y$ is H_1.

APN example

Let $f = x^3$.

$$\begin{aligned} D_f(a) &= \{x^3 + (x+a)^3\} \\ &= \{x^3 + x^3 + x^2 a + a^2 x + a^3\} \\ &= \{x^2 a + a^2 x + a^3\} \\ &= \{a^3 \left[\left(\frac{x}{a}\right)^2 + \frac{x}{a} + 1 \right]\} \\ &= \{a^3 (y^2 + y + 1)\} \end{aligned}$$

with $ay = x$.

- $H_\alpha := \{x \in \mathbb{F} \ : \ \mathrm{Tr}\,(\alpha x) = 0\}$, where $\mathrm{Tr}\,(z) = z + z^2 + \cdots + z^{2^{m-1}}$.
- Image of $y^2 + y$ is H_1.
- $H_\alpha = \alpha^{-1} H$.

Crooked functions

This example gives an example of a *crooked function*.

Crooked functions

This example gives an example of a *crooked function*.

Definition

f is *crooked* if for all $a \in \mathbb{F}^*$, $D_f(a)$ is an affine hyperplane.

Crooked functions

This example gives an example of a *crooked function*.

Definition

f is *crooked* if for all $a \in \mathbb{F}^*$, $D_f(a)$ is an affine hyperplane.

- Write f as (with $a_d \in \mathbb{F}^*$).

$$f(x) := \sum_{d \in D} a_d x^d.$$

Crooked functions

This example gives an example of a *crooked function*.

Definition

f is *crooked* if for all $a \in \mathbb{F}^*$, $D_f(a)$ is an affine hyperplane.

- Write f as (with $a_d \in \mathbb{F}^*$).

$$f(x) := \sum_{d \in D} a_d x^d.$$

- Note that one can choose $D := \{0, \ldots, q-1\}$.

Crooked functions

This example gives an example of a *crooked function*.

Definition

f is *crooked* if for all $a \in \mathbb{F}^*$, $D_f(a)$ is an affine hyperplane.

- Write f as (with $a_d \in \mathbb{F}^*$).

$$f(x) := \sum_{d \in D} a_d x^d.$$

- Note that one can choose $D := \{0, \ldots, q-1\}$. And $d = \sum_{i=0}^{m-1} d_i 2^i$.

Crooked functions

This example gives an example of a *crooked function*.

Definition

f is *crooked* if for all $a \in \mathbb{F}^*$, $D_f(a)$ is an affine hyperplane.

- Write f as (with $a_d \in \mathbb{F}^*$).

$$f(x) := \sum_{d \in D} a_d x^d.$$

- Note that one can choose $D := \{0, \ldots, q-1\}$. And $d = \sum_{i=0}^{m-1} d_i 2^i$. Define 2-weight of d as $d = \sum_{i=0}^{m-1} d_i$.

Crooked functions

This example gives an example of a *crooked function*.

Definition

f is *crooked* if for all $a \in \mathbb{F}^*$, $D_f(a)$ is an affine hyperplane.

- Write f as (with $a_d \in \mathbb{F}^*$).

$$f(x) := \sum_{d \in D} a_d x^d.$$

- Note that one can choose $D := \{0, \ldots, q-1\}$. And $d = \sum_{i=0}^{m-1} d_i 2^i$. Define 2-weight of d as $d = \sum_{i=0}^{m-1} d_i$.
- 2-Degree of a function is the maximal 2-weight of $d \in D$.

Some problems

- (Kyureghyan '06) Crooked monomials are quadratic.

Some problems

- (Kyureghyan '06) Crooked monomials are quadratic.
- (Kyureghyan, Bierbrauer '08) Crooked binomials are quadratic.

Some problems

- (Kyureghyan '06) Crooked monomials are quadratic.
- (Kyureghyan, Bierbrauer '08) Crooked binomials are quadratic.
- The crooked problem:

Question

Are all crooked functions quadratic?

Some problems

- (Kyureghyan '06) Crooked monomials are quadratic.
- (Kyureghyan, Bierbrauer '08) Crooked binomials are quadratic.
- The crooked problem:

Question

Are all crooked functions quadratic?

- Try $f \in \mathbb{F}_2[x]$?

Another measure for non-linearity

Let $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$. The *coordinate functions* for a given basis $\{\beta_1, \ldots, \beta_m\}$ are:

$$[\mathrm{Tr}\left(\beta_1 f\right), \ldots, \mathrm{Tr}\left(\beta_m f\right)].$$

Another measure for non-linearity

Let $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$. The *coordinate functions* for a given basis $\{\beta_1, \ldots, \beta_m\}$ are:

$$[\mathrm{Tr}\left(\beta_1 f\right), \ldots, \mathrm{Tr}\left(\beta_m f\right)].$$

The *component functions* are linear combinations of the coordinate functions $\mathrm{Tr}\left(\beta f\right)$ for any $\beta \in \mathbb{F}$.

Another measure for non-linearity

Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$. The *coordinate functions* for a given basis $\{\beta_1, \ldots, \beta_m\}$ are:

$$[\mathrm{Tr}(\beta_1 f), \ldots, \mathrm{Tr}(\beta_m f)].$$

The *component functions* are linear combinations of the coordinate functions $\mathrm{Tr}(\beta f)$ for any $\beta \in \mathbb{F}$.
Another measure on non-linearity could be then the Hamming distance of component functions to affine (Boolean) functions.

Another measure for non-linearity

Let $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$. The *coordinate functions* for a given basis $\{\beta_1, \ldots, \beta_m\}$ are:

$$[\mathrm{Tr}\left(\beta_1 f\right), \ldots, \mathrm{Tr}\left(\beta_m f\right)].$$

The *component functions* are linear combinations of the coordinate functions $\mathrm{Tr}\left(\beta f\right)$ for any $\beta \in \mathbb{F}$.
Another measure on non-linearity could be then the Hamming distance of component functions to affine (Boolean) functions.

Definition

Walsh transform of a function is defined as follows.

$$\mathcal{W}_f(a, b) := \sum_{x \in \mathbb{F}} (-1)^{\mathrm{Tr}(af(x)+bx)}$$

AB functions

Definition

f is Almost Bent (AB) if for all $a \in \mathbb{F}^*, b \in \mathbb{F}$,

$$\mathcal{W}_f(a,b) \in \{0, \pm 2^{\frac{m+1}{2}}\}$$

.

AB functions

Definition

f is Almost Bent (AB) if for all $a \in \mathbb{F}^*, b \in \mathbb{F}$,

$$\mathcal{W}_f(a,b) \in \{0, \pm 2^{\frac{m+1}{2}}\}$$

.

Let m be odd,

AB functions

Definition

f is Almost Bent (AB) if for all $a \in \mathbb{F}^*, b \in \mathbb{F}$,

$$\mathcal{W}_f(a,b) \in \{0, \pm 2^{\frac{m+1}{2}}\}$$

.

Let m be odd,

- crooked $\Rightarrow$ AB $\Rightarrow$ APN.

AB examples

	Exponents d	Conditions	Proven in
Gold	$2^i + 1$	$\gcd(i, m) = 1$	[2]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, m) = 1$	[4]
Welch	$2^t + 3$	$m = 2t + 1$	[3]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$m = 2t + 1$	[3]

Table: Known AB exponents x^d on $\mathbb{F}_{2^m}$

APN monomials

	Exponents d	Conditions	Proven in
Inverse	$2^{2t}-1$	$m=2t+1$	[5]
Dobbertin	$2^{4t}+2^{3t}+2^{2t}+2^{t}-1$	$m=5t$	[1]

Table: Known (non-AB) APN exponents x^d on $\mathbb{F}_{2^m}$

APN permutations

Note that x^3 is a permutation on $\mathbb{F}_{2^m}$ if and only if m is odd.

APN permutations

Note that x^3 is a permutation on $\mathbb{F}_{2^m}$ if and only if m is odd.

Fact

If m is odd, then APN monomials induce permutations on $\mathbb{F}_{2^m}$.

APN permutations

Note that x^3 is a permutation on $\mathbb{F}_{2^m}$ if and only if m is odd.

Fact

If m is odd, then APN monomials induce permutations on $\mathbb{F}_{2^m}$. If m is even, then APN monomials induce $3-1$ maps on $\mathbb{F}_{2^m}^*$.

APN permutations

Note that x^3 is a permutation on $\mathbb{F}_{2^m}$ if and only if m is odd.

Fact

If m is odd, then APN monomials induce permutations on $\mathbb{F}_{2^m}$. If m is even, then APN monomials induce $3-1$ maps on $\mathbb{F}_{2^m}^*$.

Fact

(Dillon et. al.) There are APN permutations on $\mathbb{F}_{2^6}$.

APN permutations

Note that x^3 is a permutation on $\mathbb{F}_{2^m}$ if and only if m is odd.

Fact

If m is odd, then APN monomials induce permutations on $\mathbb{F}_{2^m}$. If m is even, then APN monomials induce $3-1$ maps on $\mathbb{F}_{2^m}^*$.

Fact

(Dillon et. al.) There are APN permutations on $\mathbb{F}_{2^6}$.

Question

(The big APN problem) Are there APN permutations on $\mathbb{F}_{2^{2m}}$, $m > 3$?

APN permutations

Note that x^3 is a permutation on $\mathbb{F}_{2^m}$ if and only if m is odd.

Fact

If m is odd, then APN monomials induce permutations on $\mathbb{F}_{2^m}$. If m is even, then APN monomials induce $3-1$ maps on $\mathbb{F}_{2^m}^*$.

Fact

(Dillon et. al.) There are APN permutations on $\mathbb{F}_{2^6}$.

Question

(The big APN problem) Are there APN permutations on $\mathbb{F}_{2^{2m}}$, $m > 3$?

Cryptographic significance: AES S-Box $f = x^{-1}$ on $\mathbb{F}_{2^8}$ is not APN!

Functions on subfields

Let

- m odd,
- $k|m$,

Functions on subfields

Let

- m odd,
- $k|m$,
- $\mathbb{F} := \mathbb{F}_{2^m}$,
- $\mathbb{K} := \mathbb{F}_{2^k}$,

Functions on subfields

Let

- m odd,
- $k|m$,
- $\mathbb{F} := \mathbb{F}_{2^m}$,
- $\mathbb{K} := \mathbb{F}_{2^k}$,
- $f : \mathbb{F} \to \mathbb{F}, f \in \mathbb{K}[x]$,

Functions on subfields

Let

- m odd,
- $k|m$,
- $\mathbb{F} := \mathbb{F}_{2^m}$,
- $\mathbb{K} := \mathbb{F}_{2^k}$,
- $f : \mathbb{F} \to \mathbb{F}, f \in \mathbb{K}[x]$,
- $f_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}$ is meaningful.

Functions on subfields

Let

- m odd,
- $k|m$,
- $\mathbb{F} := \mathbb{F}_{2^m}$,
- $\mathbb{K} := \mathbb{F}_{2^k}$,
- $f : \mathbb{F} \to \mathbb{F}, f \in \mathbb{K}[x]$,
- $f_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}$ is meaningful.

Question

Are properties of f, i.e. being APN, AB or crooked, inherited downwards?

Functions on subfields

Functions on subfields

Fact

f is APN $\Rightarrow$ $f_{\mathbb{K}}$ is APN.

Functions on subfields

Fact

f is APN $\Rightarrow$ $f_{\mathbb{K}}$ *is APN.*

Theorem

f is crooked $\Rightarrow$ $f_{\mathbb{K}}$ *is crooked.*

Functions on subfields

Fact

f is APN $\Rightarrow$ $f_{\mathbb{K}}$ is APN.

Theorem

f is crooked $\Rightarrow$ $f_{\mathbb{K}}$ is crooked.

Theorem

If $f = x^e$ is AB then $f_{\mathbb{K}}$ is AB.

An Application

Theorem (G., Pott)

If $f = x^d$ is AB on $\mathbb{F}_{2^m} = \mathbb{F}$, then

$$\mathcal{W}_f(1) = \begin{cases} +2^{(m+1)/2} & \text{if } m \equiv \pm 1 \pmod 8, \\ -2^{(m+1)/2} & \text{if } m \equiv \pm 3 \pmod 8. \end{cases}$$

Final problem

Question

(Under which conditions) does
$f = x^d$ *is AB on* $\mathbb{F}_{2^m}$ *imply* $f = x^d$ *is AB on* $\mathbb{F}_{2^k}$*?*

Final problem

Question

(Under which conditions) does
$f = x^d$ *is AB on* $\mathbb{F}_{2^m}$ *imply* $f = x^d$ *is AB on* $\mathbb{F}_{2^k}$*?*

- Quadratic case is simple.

Final problem

Question

(Under which conditions) does
$f = x^d$ *is AB on* $\mathbb{F}_{2^m}$ *imply* $f = x^d$ *is AB on* $\mathbb{F}_{2^k}$*?*

- Quadratic case is simple.
- Exponential case is known.

Final problem

Question

(Under which conditions) does
$f = x^d$ *is AB on* $\mathbb{F}_{2^m}$ *imply* $f = x^d$ *is AB on* $\mathbb{F}_{2^k}$*?*

- Quadratic case is simple.
- Exponential case is known.
- What about $f \in \mathbb{F}_2[x]$?

Final problem

Question

(Under which conditions) does
$f = x^d$ *is AB on* $\mathbb{F}_{2^m}$ *imply* $f = x^d$ *is AB on* $\mathbb{F}_{2^k}$*?*

- Quadratic case is simple.
- Exponential case is known.
- What about $f \in \mathbb{F}_2[x]$? Will imply a generalization of our theorem.

Thanks for your attention.

Dobbertin, H.

Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5.

In *Proceedings of the conference on Finite Fields and Applications, Augsburg, 1999*, D. Jungnickel and H. Niederreiter, Eds., Springer-Verlag, Berlin, 2001, pp. 113–121.

Gold, R.

Maximal recursive sequences with 3-valued recursive cross-correlation functions.

IEEE Trans. Inf. Th. 14 (1968), 377–385.

Hollmann, H., and Xiang, Q.

A proof if the Welsh and Niho conjectures on crosscorrelation of binary sequences.

Finite Fields Appl. 7 (2001), 253–286.

Kasami, T.

The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes.
Information and Control 18 (1971), 369–394.

Nyberg, K.
Differentially uniform mappings for cryptography.
In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, vol. 765 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1994, pp. 55–64.