Almost Perfect Nonlinear Functions

Faruk Göloğlu

Claude Shannon Institute, University College Dublin

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

A Block Cipher can be seen as:

\[ B : \{0, 1\}^m \rightarrow \{0, 1\}^m. \]

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

**Confusion** introduces complexity or non-linearity to the system and is achieved generally by the S-Box.

**Question**

How do we define non-linearity?
A Block Cipher can be seen as:

\[ \mathcal{B} : \{0, 1\}^m \rightarrow \{0, 1\}^m. \]
A Block Cipher can be seen as:

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

Claude Shannon introduced the properties *confusion* and *diffusion*.
A Block Cipher can be seen as:

\[ B : \{0, 1\}^m \rightarrow \{0, 1\}^m. \]

Claude Shannon introduced the properties \textit{confusion} and \textit{diffusion}.

Confusion introduces complexity or non-linearity to the system.
A Block Cipher can be seen as:

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

Claude Shannon introduced the properties \textit{confusion} and \textit{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:

\[ B : \{0, 1\}^m \rightarrow \{0, 1\}^m. \]

- Claude Shannon introduced the properties \textit{confusion} and \textit{diffusion}.

- Confusion introduces complexity or non-linearity to the system and achieved generally by the S-Box.

Question

\textit{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.,

\[ f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m. \]
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.,

\[ f : \mathbb{F}^m_2 \rightarrow \mathbb{F}^m_2. \]

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

\[ l(x) + l(x + a) = l(a), \]

for any \( x \in F \), i.e.,

\[ D_l(a) := \{ l(x) + l(x + a) : x \in F \} = \{ l(a) \}. \]
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?

If \( F = F_2^m \) then
\[
f(x) + f(x + a) = f(x + a) + f((x + a) + a).
\]
Hence, \( \#D_f(a) \leq 2^m - 1 \).

Definition

\( f \) is Almost Perfect Nonlinear (APN) if for all \( a \in F^* \),
\[
\#D_f(a) = 2^m - 1.
\]

If characteristic of \( F \) is odd, Perfect Nonlinear functions exist.

Faruk Göloğlu
APN Functions
APN functions

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

If $\mathbb{F} = \mathbb{F}_{2^m}$ then

$$f(x) + f(x + a) = f(x + a) + f((x + a) + a).$$
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, \( \#D_f(a) \leq 2^{m-1} \).
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, $\#D_f(a) \leq 2^{m-1}$.

**Definition**

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

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

**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 $f = x^3$. 
Let $f = x^3$.

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

with $ay = x$. 
Let $f = x^3$. 

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

with $ay = x$.

- $H_\alpha := \{x \in \mathbb{F} : \text{Tr}(\alpha x) = 0\}$, where 

$\text{Tr}(z) = z + z^2 + \cdots + z^{2^{m-1}}$. 

Faruk Göloğlu  APN Functions
**APN example**

Let \( f = x^3 \).

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

with \( ay = x \).

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

Let \( f = x^3 \).

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

with \( ay = x \).

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

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

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

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

Define the 2-weight of $d$ as

$$ d = \sum_{i=0}^{m-1} d_i 2^i. $$

The 2-degree of a function is the maximal 2-weight of $d \in D$. 
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 $a_d \in \mathbb{F}^*$).

\[
 f(x) := \sum_{d \in D} a_d x^d.
\]
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 
  \[ d = \sum_{i=0}^{m-1} d_i 2^i. \text{ Define 2-weight of } d \text{ as } d = \sum_{i=0}^{m-1} d_i. \]
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.
(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 \( f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \). The \textit{coordinate functions} for a given basis \( \{ \beta_1, \ldots, \beta_m \} \) are:

\[
[\text{Tr} (\beta_1 f), \ldots, \text{Tr} (\beta_m f)].
\]
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:

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

The component functions are linear combinations of the coordinate functions $\text{Tr} (\beta f)$ 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:

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

The component functions are linear combinations of the coordinate functions $\text{Tr} (\beta f)$ 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 $f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$. The coordinate functions for a given basis $\{\beta_1, \ldots, \beta_m\}$ are:

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

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

Another measure on non-linearity could be then the Hamming distance of component functions to affine (Boolean) functions.

**Definition**

*Walsh transform* of a function is defined as follows.

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

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

Let $m$ be odd,
**AB functions**

**Definition**

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

\[ W_f(a, b) \in \{0, \pm 2^{\frac{m+1}{2}}\} \]

\[ \bigwedge \]

Let \( m \) be odd,  

- crooked \( \Rightarrow \) AB \( \Rightarrow \) APN.
### AB examples

<table>
<thead>
<tr>
<th></th>
<th>Exponents $d$</th>
<th>Conditions</th>
<th>Proven in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>$2^i + 1$</td>
<td>$\gcd(i, m) = 1$</td>
<td>[2]</td>
</tr>
<tr>
<td>Kasami</td>
<td>$2^{2i} - 2^i + 1$</td>
<td>$\gcd(i, m) = 1$</td>
<td>[4]</td>
</tr>
<tr>
<td>Welch</td>
<td>$2^t + 3$</td>
<td>$m = 2t + 1$</td>
<td>[3]</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Function</th>
<th>Exponents $d$</th>
<th>Conditions</th>
<th>Proven in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inverse</td>
<td>$2^{2t} - 1$</td>
<td>$m = 2t + 1$</td>
<td>[5]</td>
</tr>
<tr>
<td>Dobbertin</td>
<td>$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$</td>
<td>$m = 5t$</td>
<td>[1]</td>
</tr>
</tbody>
</table>

**Table:** Known (non-AB) APN exponents $x^d$ on $\mathbb{F}_{2^m}$
Note that $x^3$ is a permutation on $\mathbb{F}_{2^m}$ if and only if $m$ is odd.
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 $\mathbb{F}_{2^m}$.***
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 $\mathbb{F}_{2^m}^*$. 
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 $\mathbb{F}_{2^6}$. 

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 $\mathbb{F}_{2^{2m}}$, $m > 3$?***
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!
Let
- $m$ odd,
- $k | m$, 

$F \colon = F_2^m$, 
$K \colon = F_2^k$, 
$f \colon F \rightarrow F$, 
$f \in K[x]$, 
$f_K \colon K \rightarrow K$ is meaningful.

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

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

**Question**

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

- If \( f \) is APN, then \( f^K \) is APN.

- If \( f \) is crooked, then \( f^K \) is crooked.

- If \( f = x^e \) is AB, then \( f^K \) is AB.
Fact

\[ f \text{ is APN} \Rightarrow f_K \text{ is APN.} \]
Fact
\[ f \text{ is APN} \Rightarrow f_K \text{ is APN.} \]

Theorem
\[ f \text{ is crooked} \Rightarrow f_K \text{ is crooked.} \]
Fact
\[ f \text{ is APN} \implies f_K \text{ is APN}. \]

Theorem
\[ f \text{ is crooked} \implies f_K \text{ is crooked}. \]

Theorem
\[ \text{If } f = x^e \text{ is AB then } f_K \text{ is AB}. \]
If $f = x^d$ is AB on $\mathbb{F}_{2^m} = \mathbb{F}$, then

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

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

Gold, R.
Maximal recursive sequences with 3-valued recursive cross-correlation functions.

Hollmann, H., and Xiang, Q.
A proof if the Welsh and Niho conjectures on crosscorrelation of binary sequences.

Kasami, T.
The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes.


**Nyberg, K.**

Differentially uniform mappings for cryptography.