On the variations of Maiorana-McFarland and (partial) spread class of Boolean functions

Razi Arshad
(joint work with Alexander Pott)

Otto von Guericke University, Magdeburg, Germany

BFA 2018, June 2018

Almost Perfect Nonlinear Function

Example:

$$F(x) = x^3$$

defined on $\mathbb{F}_{2^n}$

$$F(x+a) + F(x) = x^2a + a^2x + a^3$$

is 2 to 1 for all $a \neq 0$.

Almost Perfect Nonlinear Function

Example:

$$F(x) = x^3$$

defined on $\mathbb{F}_{2^n}$

$$F(x+a) + F(x) = x^2a + a^2x + a^3$$

is 2 to 1 for all $a \neq 0$.

Goal:

Find the functions F such that $F(x+a) + F(x)$ are 2 to 1 mapping for all $a \neq 0$.

Almost Perfect Nonlinear Function

A function

$$F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$$

is Almost Perfect Nonlinear (APN) if

$$x \longrightarrow F(x + a) + F(x)$$

is 2 to 1 mapping for all $a \neq 0$.

Almost Perfect Nonlinear Function

A function

$$F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$$

is Almost Perfect Nonlinear (APN) if

$$x \longrightarrow F(x+a) + F(x)$$

is 2 to 1 mapping for all $a \neq 0$.
Equivalently, F is non-affine on all 2-dimensional affine subspaces of $\mathbb{F}_2^n$, that is,

$$F(a) + F(x+a) + F(y+a) + F(x+y+a) \neq 0,$$

$\forall$ distinct a, x, y.

Almost Perfect Nonlinear Function

A function

$$F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$$

is Almost Perfect Nonlinear (APN) if

$$x \longrightarrow F(x + a) + F(x)$$

is 2 to 1 mapping for all $a \neq 0$.
Equivalently, F is non-affine on all 2-dimensional affine subspaces of $\mathbb{F}_2^n$, that is,

$$F(a) + F(x + a) + F(y + a) + F(x + y + a) \neq 0,$$

$\forall$ distinct a, x, y.
In the example x^3, the vectorspace $\mathbb{F}_2^n$ has been realized by using the finite field $\mathbb{F}_{2^n}$.

Almost Perfect Nonlinear Function

A function

$$F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$$

is Almost Perfect Nonlinear (APN) if

$$x \longrightarrow F(x+a) + F(x)$$

is 2 to 1 mapping for all $a \neq 0$.
Equivalently, F is non-affine on all 2-dimensional affine subspaces of $\mathbb{F}_2^n$, that is,

$$F(a) + F(x+a) + F(y+a) + F(x+y+a) \neq 0,$$

$\forall$ distinct a, x, y.
In the example x^3, the vectorspace $\mathbb{F}_2^n$ has been realized by using the finite field $\mathbb{F}_{2^n}$.
Note: We need only additive properties.

A complete list of known infinite families in univariate form (from Budaghyan, Helleseth, Li, Sun)

Table 2. Known classes of quadratic APN polynomials inequivalent to power functions on $\mathbb{F}_{2^n}$.

N°	Functions	Conditions
1-2	$x^{2^s+1} + \alpha^{2^k-1} x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,p) = \gcd(s,pk) = 1$, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p - i$, $n \geq 12$, α primitive in $\mathbb{F}_{2^n}^*$
3	$x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, $\gcd(2^i+1, q+1) \neq 1$, $cb^q + b \neq 0$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $c^{q+1} = 1$
4	$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$q = 2^m, n = 2m, \gcd(i,m) = 1$, $c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ is irreducible over $\mathbb{F}_{2^n}$
5	$x^3 + a^{-1}\mathrm{tr}_1^n(a^3x^9)$	$a \neq 0$
6	$x^3 + a^{-1}\mathrm{tr}_3^n(a^3x^9 + a^6x^{18})$	$3 \mid n$, $a \neq 0$
7	$x^3 + a^{-1}\mathrm{tr}_3^n(a^6x^{18} + a^{12}x^{36})$	$3 \mid n$, $a \neq 0$
8-10	$ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1} x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3) = \gcd(s,3k) = 1$, $v, w \in \mathbb{F}_{2^k}, vw \neq 1$, $3 \mid (k+s)$, u primitive in $\mathbb{F}_{2^n}^*$
11	$\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{k+s}+2^k} +$ $\beta x^{2^k+1} + \sum_{i=1}^{k-1} \gamma_i x^{2^{k+i}+2^i}$	$n = 2k$, $\gcd(s,k) = 1$, s, k odd, $\beta \notin \mathbb{F}_{2^k}, \gamma_i \in \mathbb{F}_{2^k}$, α not a cube

A possible systematic approach

- Most constructions of APN functions use finite field. Is there any possible alternative approach?

A possible systematic approach

- Most constructions of APN functions use finite field. Is there any possible alternative approach?
- We are interested in the construction of APN functions by using coordinate functions:

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}.$$

A possible systematic approach

- Most constructions of APN functions use finite field. Is there any possible alternative approach?
- We are interested in the construction of APN functions by using coordinate functions:

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}.$$

- Find the Boolean functions where the number of affine 2-dimensional subspaces which are non-affine is large. Use these to build APN functions.

A possible systematic approach

Step 1: Find a Boolean function $f_1(x)$ and determine the affine 2-dimensional which are affine on f_1:

$$f_1(a) + f_1(x + a) + f_1(y + a) + f_1(x + y + a) = 0.$$

A possible systematic approach

Step 1: Find a Boolean function $f_1(x)$ and determine the affine 2-dimensional which are affine on f_1:

$$f_1(a) + f_1(x + a) + f_1(y + a) + f_1(x + y + a) = 0.$$

Step 2: Find a Boolean function f_2 which is non-affine on many of the affine 2-dimensional which are survived in Steps 1.

A possible systematic approach

Step 1: Find a Boolean function $f_1(x)$ and determine the affine 2-dimensional which are affine on f_1:

$$f_1(a) + f_1(x + a) + f_1(y + a) + f_1(x + y + a) = 0.$$

Step 2: Find a Boolean function f_2 which is non-affine on many of the affine 2-dimensional which are survived in Steps 1.

$$\vdots$$

Step i+1: Find a Boolean function f_{i+1} which is non-affine on many of the affine 2-dimensional which are survived in Steps $1, \ldots, i$.

Number of affine subspaces

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m,\ m \le n$. *Then* F *is affine on*

$$\frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{\substack{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m,\\ b\neq 0}} W_F^4(a,b) + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right]$$

of 2*-dimensional affine subspaces of* $\mathbb{F}_2^n$, *where* $W_F(a,b) = \sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot F(x)+a\cdot x}$.

Number of affine subspaces

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m,\ m \leq n$. *Then* F *is affine on*

$$\frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{\substack{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m,\\ b\neq 0}} W_F^4(a,b) + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right]$$

of 2*-dimensional affine subspaces of* $\mathbb{F}_2^n$*, where* $W_F(a,b) = \sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot F(x)+a\cdot x}$.

- Which functions can be used?

Number of affine subspaces

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m,\ m \leq n$. Then F is affine on

$$\frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{\substack{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m,\\ b\neq 0}} W_F^4(a,b) + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right]$$

of 2-dimensional affine subspaces of $\mathbb{F}_2^n$, where
$W_F(a,b) = \sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot F(x)+a\cdot x}$.

- Which functions can be used?
- $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is plateaued (t-plateaued) function if

$$W_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x} \in \{0, \pm 2^{\frac{n+t}{2}}\},$$

for some fixed $t, 0 \leq t \leq n,\ n+t$ even, $\forall\ a \in \mathbb{F}_2^n$.

Example

Let $F : \mathbb{F}_{2^8} \longrightarrow \mathbb{F}_{2^8}$
defined as

$$F(x) = x^3$$

Table: Reduction in the number of affine subspaces

Total number of 2-dimensional affine subspaces = 690880	
Component function	Number of affine subspaces
1	342720
2	168640
3	81600
4	39616
5	18624
6	8128
7	2880
8	0

Which functions can be used?

- The best functions that can be used are bent functions: They are non-affine on
$$\frac{2^{3n-4} - 2^{2n-4}}{3}$$
of
$$\frac{2^{3n-3} - 3 \cdot 2^{2n-3} + 2^{n-2}}{3}$$
2-dimensional affine subspaces, i.e., approximately half of them.

Which functions can be used?

- The best functions that can be used are bent functions: They are non-affine on
$$\frac{2^{3n-4} - 2^{2n-4}}{3}$$
of
$$\frac{2^{3n-3} - 3 \cdot 2^{2n-3} + 2^{n-2}}{3}$$
2-dimensional affine subspaces, i.e., approximately half of them.
- Quadratic functions of full rank are bent functions. what about functions of smaller rank, for instance $x_1 x_2$?

Which functions can be used?

- The best functions that can be used are bent functions: They are non-affine on
$$\frac{2^{3n-4}-2^{2n-4}}{3}$$
of
$$\frac{2^{3n-3}-3\cdot 2^{2n-3}+2^{n-2}}{3}$$
2-dimensional affine subspaces, i.e., approximately half of them.
- Quadratic functions of full rank are bent functions. what about functions of smaller rank, for instance x_1x_2?
- Quadratic functions of rank $n-t$ are non-affine on
$$\frac{2^{3n-4}-2^{2n+t-4}}{3}$$
of all 2-dimensional affine subspaces.

k-spread Boolean functions

- There are constructions of bent function of the type partial spread.

k-spread Boolean functions

- There are constructions of bent function of the type partial spread.
- **Starting point:** look for (partial) spread Boolean functions.

k-spread Boolean functions

- There are constructions of bent function of the type partial spread.
- **Starting point:** look for (partial) spread Boolean functions.
- Let $n = 2m$, a spread of order k in $\mathbb{F}_2^n$ is a set of k m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$ such that $H_i \cap H_j = \{0\}$ for all $i \neq j$.

k-spread Boolean functions

- There are constructions of bent function of the type partial spread.
- **Starting point:** look for (partial) spread Boolean functions.
- Let $n = 2m$, a spread of order k in $\mathbb{F}_2^n$ is a set of k m-dimensional subspaces $H_1, \ldots, H_k$ of $\mathbb{F}_2^n$ such that $H_i \cap H_j = \{0\}$ for all $i \neq j$.
- k-spread Boolean function is an indicator function of $H^* = \cup_{i=1}^k H_i \setminus \{0\}$ which is non-affine on $\frac{1}{24}[-\frac{1}{2^{2m+1}}[(2^{2m} - 2^{m+1}k + 2k)^4 + (2k)^4(2^{2m} - 2^m k + k - 1)) + (2k - 2^{m+1})^4(2^m k - k)] + 2^{6m}]$ of all 2-dimensional affine subspaces.

k-spread Boolean functions

- For $k = 2^{m-1}$, we have bent function. For $k = 2^{m-1} - 1$, the k-spread Boolean function is non-affine on

$$\frac{1}{3}\left[2^{6m-4} - 2^{4m-4} - 5 \cdot 2^{2m} + 3 \cdot 2^{m+2} - 7\right]$$

of all 2-dimensional affine subspaces.

k-spread Boolean functions

- For $k = 2^{m-1}$, we have bent function. For $k = 2^{m-1} - 1$, the k-spread Boolean function is non-affine on
$$\frac{1}{3}\left[2^{6m-4} - 2^{4m-4} - 5 \cdot 2^{2m} + 3 \cdot 2^{m+2} - 7\right]$$
of all 2-dimensional affine subspaces.
- For $k = 2^{m-1} + 1$, the k-spread Boolean function is non-affine on
$$\frac{1}{3}\left[2^{6m-4} - 2^{4m-4} - 2^{2m} + 1\right]$$
of all 2-dimensional affine subspaces.

k-spread Boolean functions

- For $k = 2^{m-1}$, we have bent function. For $k = 2^{m-1} - 1$, the k-spread Boolean function is non-affine on

$$\frac{1}{3}\left[2^{6m-4} - 2^{4m-4} - 5 \cdot 2^{2m} + 3 \cdot 2^{m+2} - 7\right]$$

of all 2-dimensional affine subspaces.

- For $k = 2^{m-1} + 1$, the k-spread Boolean function is non-affine on

$$\frac{1}{3}\left[2^{6m-4} - 2^{4m-4} - 2^{2m} + 1\right]$$

of all 2-dimensional affine subspaces.

- The quadratic Boolean function of rank $n - 2$ is non-affine on

$$\frac{1}{3}\left[2^{6m-4} - 2^{4m-2}\right]$$

of all 2-dimensional affine subspaces.

Maiorana-McFarland Boolean functions

- There are constructions of bent function of the type Maiorana-McFarland (MM).

Maiorana-McFarland Boolean functions

- There are constructions of bent function of the type Maiorana-McFarland (MM).
- Let $n = 2m$ and $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ such that
  $f(x, y) = x \cdot \pi(y) + h(y)$
  is bent if π is a permutation and $h : \mathbb{F}_2^m \to \mathbb{F}_2$ arbitrary.

Maiorana-McFarland Boolean functions

- There are constructions of bent function of the type Maiorana-McFarland (MM).
- Let $n = 2m$ and $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ such that
  $f(x, y) = x \cdot \pi(y) + h(y)$
  is bent if π is a permutation and $h : \mathbb{F}_2^m \to \mathbb{F}_2$ arbitrary.
- Assume that image of π has s elements having 2 preimage, r elements having 1 preimage and $\mid \pi(0) \mid = 1$. Assume h is a zero function.

Maiorana-McFarland Boolean functions

- There are constructions of bent function of the type Maiorana-McFarland (MM).
- Let $n = 2m$ and $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ such that
  $f(x, y) = x \cdot \pi(y) + h(y)$
  is bent if π is a permutation and $h : \mathbb{F}_2^m \to \mathbb{F}_2$ arbitrary.
- Assume that image of π has s elements having 2 preimage, r elements having 1 preimage and $\mid \pi(0) \mid = 1$. Assume h is a zero function.
- The Boolean function f belong to MM class is non-affine on $\frac{1}{24}[-\frac{1}{2^{n+1}}(2^{5m}r + 2^{5m+3}s + 2^{8m}) + 2^{6m}]$ of all 2-dimensional affine subspaces.

Maiorana-McFarland Boolean functions

- There are constructions of bent function of the type Maiorana-McFarland (MM).
- Let $n = 2m$ and $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ such that
  $f(x, y) = x \cdot \pi(y) + h(y)$
  is bent if π is a permutation and $h : \mathbb{F}_2^m \to \mathbb{F}_2$ arbitrary.
- Assume that image of π has s elements having 2 preimage, r elements having 1 preimage and $\mid \pi(0) \mid = 1$. Assume h is a zero function.
- The Boolean function f belong to MM class is non-affine on $\frac{1}{24}[-\frac{1}{2^{n+1}}(2^{5m}r + 2^{5m+3}s + 2^{8m}) + 2^{6m}]$ of all 2-dimensional affine subspaces.
- For $s = 0, r = 2^m$, we have bent function. For $s = 1, r = 2^m - 2$, the MM Boolean function is non-affine on

$$\frac{1}{3}\left[2^{6m-4} - 2^{4m-4} - 3 \cdot 2^{3m-3}\right]$$

of all 2-dimensional affine subspaces.

Conclusion

- Bent function are the best candidate for construction of APN functions by using coordinate function approach.

Conclusion

- Bent function are the best candidate for construction of APN functions by using coordinate function approach.
- For some values of k, t, k-spread Boolean functions are better than t-plateaued Boolean functions.

Conclusion

- Bent function are the best candidate for construction of APN functions by using coordinate function approach.
- For some values of k, t, k-spread Boolean functions are better than t-plateaued Boolean functions.
- For some values of s, t, r, MM Boolean functions are better than t-plateaued Boolean functions.

Conclusion

- Bent function are the best candidate for construction of APN functions by using coordinate function approach.
- For some values of k, t, k-spread Boolean functions are better than t-plateaued Boolean functions.
- For some values of s, t, r, MM Boolean functions are better than t-plateaued Boolean functions.
- k-spread and MM Boolean functions may be good candidate for the construction of new APN functions by using coordinate function approach.

Thanks for your attention!