Changing Points in APN Functions

Nikolay S. Kaleyski
(joint work with Lilya Budaghyan, Claude Carlet and Tor Helleseth)

University of Bergen

June 18, 2018

Preliminaries

- consider $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$;

Preliminaries

- consider $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- derivative $D_a F(x) = F(x) + F(a + x)$;

Preliminaries

- consider $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- derivative $D_a F(x) = F(x) + F(a + x)$;
- $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : D_a F(x) = b\}$;

Preliminaries

- consider $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$;
- derivative $D_aF(x) = F(x) + F(a + x)$;
- $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : D_aF(x) = b\}$;
- differential uniformity $\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \Delta_F(a, b)$;

Preliminaries

- consider $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- derivative $D_a F(x) = F(x) + F(a + x)$;
- $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : D_a F(x) = b\}$;
- differential uniformity $\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \Delta_F(a, b)$;
- measures resistance to differential cryptanalysis;

Preliminaries

- consider $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- derivative $D_aF(x) = F(x) + F(a + x)$;
- $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : D_aF(x) = b\}$;
- differential uniformity $\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \Delta_F(a, b)$;
- measures resistance to differential cryptanalysis;
- always even;

Preliminaries

- consider $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- derivative $D_a F(x) = F(x) + F(a + x)$;
- $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : D_a F(x) = b\}$;
- differential uniformity $\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \Delta_F(a, b)$;
- measures resistance to differential cryptanalysis;
- always even;
- F is *Almost Perfect Nonlinear (APN)* if $\Delta_F = 2$.

Preliminaries (2)

- unique univariate representation of any (n, n)-function as

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, c_i \in \mathbb{F}_{2^n}.$$

Preliminaries (2)

- unique univariate representation of any (n, n)-function as

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, c_i \in \mathbb{F}_{2^n}.$$

- algebraic degree of F is

$$\deg(F) = \max_{i:c_i \neq 0} w_2(i)$$

where $w_2(i)$ is the two-weight of i.

Preliminaries (2)

- unique univariate representation of any (n,n)-function as

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, c_i \in \mathbb{F}_{2^n}.$$

- algebraic degree of F is

$$\deg(F) = \max_{i : c_i \neq 0} w_2(i)$$

where $w_2(i)$ is the two-weight of i.

- Walsh Transform of F is the function $W : \mathbb{F}_{2^n}^2 \to \mathbb{Z}$ defined as

$$W(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bF(x)+ax)}$$

where $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function.

Preliminaries (3)

- $F_b : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined as $F_b(x) = \mathrm{Tr}(bF(x))$ for $b \in \mathbb{F}_{2^n}$ are the component functions of F;

Preliminaries (3)

- $F_b : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined as $F_b(x) = \mathrm{Tr}(bF(x))$ for $b \in \mathbb{F}_{2^n}$ are the component functions of F;
- the Hamming distance between two functions F and G is $\mathrm{d}(F, G) = \#\{x : F(x) \neq G(x)\}$;

Preliminaries (3)

- $F_b : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined as $F_b(x) = \mathrm{Tr}(bF(x))$ for $b \in \mathbb{F}_{2^n}$ are the component functions of F;
- the Hamming distance between two functions F and G is $\mathrm{d}(F, G) = \#\{x : F(x) \neq G(x)\}$;
- the nonlinearity of F is

$$\mathcal{NL}(F) = \max_{b \in \mathbb{F}_{2^n}^*} \min_{a \in \mathbb{F}_{2^n}} \mathrm{d}(F_b, a)$$

with the last minimum over all affine $a : \mathbb{F}_{2^n} \to \mathbb{F}_2$;

Preliminaries (3)

- $F_b : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined as $F_b(x) = \mathrm{Tr}(bF(x))$ for $b \in \mathbb{F}_{2^n}$ are the component functions of F;
- the Hamming distance between two functions F and G is $\mathrm{d}(F, G) = \#\{x : F(x) \neq G(x)\}$;
- the nonlinearity of F is

$$\mathcal{NL}(F) = \max_{b \in \mathbb{F}_{2^n}^*} \min_{a \in \mathbb{F}_{2^n}} \mathrm{d}(F_b, a)$$

  with the last minimum over all affine $a : \mathbb{F}_{2^n} \to \mathbb{F}_2$;
- Useful formula:

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{b \in \mathbb{F}_{2^n}^*, a \in \mathbb{F}_{2^n}} |W_F(a, b)|.$$

Changing a Single Point in a Function

- research on constructions of i.a. APN functions is ongoing;

Changing a Single Point in a Function

- research on constructions of i.a. APN functions is ongoing;
- maximum algebraic degree of APN function is an open problem:

Changing a Single Point in a Function

- research on constructions of i.a. APN functions is ongoing;
- maximum algebraic degree of APN function is an open problem:
- is it possible to have $\deg(F) = n$ for F over $\mathbb{F}_{2^n}$ APN?

Changing a Single Point in a Function

- research on constructions of i.a. APN functions is ongoing;
- maximum algebraic degree of APN function is an open problem:
- is it possible to have $\deg(F) = n$ for F over $\mathbb{F}_{2^n}$ APN?
- *"On upper bounds for algebraic degrees of APN functions"* (Budaghyan, Carlet, Helleseth, Li, Sun): changing one point in a given function F by

$$G(x) = F(x) + (1 + (x+u)^{2^n-1})v = \begin{cases} F(x) & x \neq u \\ F(u) + v & x = u. \end{cases}$$

Changing Multiple Points in a Function

- Given natural $K \geq 1$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, construct G by changing K points:

Changing Multiple Points in a Function

- Given natural $K \geq 1$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, construct G by changing K points:
  - select $u_1, u_2, \dots, u_k$ from $\mathbb{F}_{2^n}$ with $\#\{u_1, u_2, \dots, u_K\} = K$;

Changing Multiple Points in a Function

- Given natural $K \geq 1$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, construct G by changing K points:
  - select $u_1, u_2, \dots, u_k$ from $\mathbb{F}_{2^n}$ with $\#\{u_1, u_2, \dots, u_K\} = K$;
  - select $v_1, v_2, \dots, v_k$ from $\mathbb{F}_{2^n}^*$;

Changing Multiple Points in a Function

- Given natural $K \geq 1$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, construct G by changing K points:
  - select $u_1, u_2, \dots, u_k$ from $\mathbb{F}_{2^n}$ with $\#\{u_1, u_2, \dots, u_K\} = K$;
  - select $v_1, v_2, \dots, v_k$ from $\mathbb{F}_{2^n}^*$;
  - define G as

$$G(x) = F(x) + \sum_{i=1}^{K} (1 + (x + u_1)^{2^n - 1}) v_i$$
$$= \begin{cases} F(x) & x \notin U \\ F(u_i) + v_i & x = u_i, i \in \{1, 2, \dots, K\}. \end{cases}$$

Changing Multiple Points in a Function

- Given natural $K \geq 1$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, construct G by changing K points:
  - select $u_1, u_2, \ldots, u_k$ from $\mathbb{F}_{2^n}$ with $\#\{u_1, u_2, \ldots, u_K\} = K$;
  - select $v_1, v_2, \ldots, v_k$ from $\mathbb{F}_{2^n}^*$;
  - define G as

$$G(x) = F(x) + \sum_{i=1}^{K} (1 + (x + u_1)^{2^n - 1}) v_i$$
$$= \begin{cases} F(x) & x \notin U \\ F(u_i) + v_i & x = u_i, i \in \{1, 2, \ldots, K\}. \end{cases}$$

- What can be said about the properties of F and G?

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of $x^{2^n - k}$;

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of $x^{2^n - k}$;
- assume $\sum_{i=1}^{K} v_i = 0$, otherwise reduces to $\deg(G) = n$;

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of x^{2^n-k};
- assume $\sum_{i=1}^{K} v_i = 0$, otherwise reduces to $\deg(G) = n$;
- G has a term cx^{2^n-2} unless F has a term $c'x^{2^n-2}$ with $c' = \sum_{i=0}^{K} v_i u_i$;

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of x^{2^n-k};
- assume $\sum_{i=1}^{K} v_i = 0$, otherwise reduces to $\deg(G) = n$;
- G has a term cx^{2^n-2} unless F has a term $c'x^{2^n-2}$ with $c' = \sum_{i=0}^{K} v_i u_i$;
- hence $\min\{\deg(F), \deg(G)\} \geq n-1$;

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of $x^{2^n - k}$;
- assume $\sum_{i=1}^{K} v_i = 0$, otherwise reduces to $\deg(G) = n$;
- G has a term cx^{2^n-2} unless F has a term $c' x^{2^n-2}$ with $c' = \sum_{i=0}^{K} v_i u_i$;
- hence $\min\{\deg(F), \deg(G)\} \geq n - 1$;
- bounds on algebraic degree now imply non-existence results:

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of x^{2^n-k};
- assume $\sum_{i=1}^{K} v_i = 0$, otherwise reduces to $\deg(G) = n$;
- G has a term cx^{2^n-2} unless F has a term $c'x^{2^n-2}$ with $c' = \sum_{i=0}^{K} v_i u_i$;
- hence $\min\{\deg(F), \deg(G)\} \geq n - 1$;
- bounds on algebraic degree now imply non-existence results:
  - if F is Almost Bent (AB), then G is not AB for $n > 3$;

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of $x^{2^n - k}$;
- assume $\sum_{i=1}^{K} v_i = 0$, otherwise reduces to $\deg(G) = n$;
- G has a term cx^{2^n-2} unless F has a term $c' x^{2^n-2}$ with $c' = \sum_{i=0}^{K} v_i u_i$;
- hence $\min\{\deg(F), \deg(G)\} \geq n - 1$;
- bounds on algebraic degree now imply non-existence results:
  - if F is Almost Bent (AB), then G is not AB for $n > 3$;
  - if F is plateaued, then G is not plateaued for $n > 4$;

General Observations (Algebraic Degree)

- $F(x) + G(x)$ has coefficient $\sum_{i=1}^{K} v_i u_i^{k-1}$ in front of x^{2^n-k};
- assume $\sum_{i=1}^{K} v_i = 0$, otherwise reduces to $\deg(G) = n$;
- G has a term cx^{2^n-2} unless F has a term $c'x^{2^n-2}$ with $c' = \sum_{i=0}^{K} v_i u_i$;
- hence $\min\{\deg(F), \deg(G)\} \geq n - 1$;
- bounds on algebraic degree now imply non-existence results:
    - if F is Almost Bent (AB), then G is not AB for $n > 3$;
    - if F is plateaued, then G is not plateaued for $n > 4$;
    - same if $\deg(F) < n - 1$.

General Observations (Walsh Transform)

- by mechanical computations:

$$W_G(a,b) = W_F(a,b) + \sum_{i=1}^{K} (-1)^{\mathrm{Tr}(bF(u_i)+au_i)} \left((-1)^{\mathrm{Tr}(bv_i)} - 1 \right);$$

General Observations (Walsh Transform)

- by mechanical computations:

$$W_G(a,b) = W_F(a,b) + \sum_{i=1}^{K} (-1)^{\mathrm{Tr}(bF(u_i)+au_i)} \left((-1)^{\mathrm{Tr}(bv_i)} - 1 \right);$$

- hence $-2K \leq W_G(a,b) - W_F(a,b) \leq 2K$;

General Observations (Walsh Transform)

- by mechanical computations:

$$W_G(a,b) = W_F(a,b) + \sum_{i=1}^{K} (-1)^{\mathrm{Tr}(bF(u_i)+au_i)} \left((-1)^{\mathrm{Tr}(bv_i)} - 1 \right);$$

- hence $-2K \leq W_G(a,b) - W_F(a,b) \leq 2K$;
- hence $-K \leq \mathcal{NL}(G) - \mathcal{NL}(F) \leq K$.

Derivative Analysis

- let $1_{a,b}(x) = 1$ if $x \in \{a, b\}$ and $1_{a,b}(x) = 0$ otherwise;

Derivative Analysis

- let $1_{a,b}(x) = 1$ if $x \in \{a, b\}$ and $1_{a,b}(x) = 0$ otherwise;
- $D_a G$ and $D_a F$ differ on the points in $U \cup (a + U)$:

$$D_a G(x) = D_a F(x) + \sum_{i=1}^{K} 1_{u_i, a+u_i}(x) v_i;$$

Derivative Analysis

- let $1_{a,b}(x) = 1$ if $x \in \{a, b\}$ and $1_{a,b}(x) = 0$ otherwise;
- $D_a G$ and $D_a F$ differ on the points in $U \cup (a + U)$:

$$D_a G(x) = D_a F(x) + \sum_{i=1}^{K} 1_{u_i, a+u_i}(x) v_i;$$

- for $a \in \mathbb{F}_{2^n}^*$, let $aU = \{u_i \in U : u_i + a \in U\}$ and denote by $\bar{i}$ the index j for which $u_i + a = u_j$;

Derivative Analysis

- let $1_{a,b}(x) = 1$ if $x \in \{a, b\}$ and $1_{a,b}(x) = 0$ otherwise;
- $D_a G$ and $D_a F$ differ on the points in $U \cup (a + U)$:

$$D_a G(x) = D_a F(x) + \sum_{i=1}^{K} 1_{u_i, a+u_i}(x) v_i;$$

- for $a \in \mathbb{F}_{2^n}^*$, let $aU = \{u_i \in U : u_i + a \in U\}$ and denote by $\bar{i}$ the index j for which $u_i + a = u_j$;
- G is not APN if and only if $D_a F(x) = D_a F(y)$ for some $a, x, y \in \mathbb{F}_{2^n}$ with $a \neq 0$, $x \neq y$, $x \neq a + y$;

Derivative Analysis

- let $1_{a,b}(x) = 1$ if $x \in \{a, b\}$ and $1_{a,b}(x) = 0$ otherwise;
- $D_a G$ and $D_a F$ differ on the points in $U \cup (a + U)$:

$$D_a G(x) = D_a F(x) + \sum_{i=1}^{K} 1_{u_i, a+u_i}(x) v_i;$$

- for $a \in \mathbb{F}_{2^n}^*$, let $aU = \{u_i \in U : u_i + a \in U\}$ and denote by $\bar{i}$ the index j for which $u_i + a = u_j$;
- G is not APN if and only if $D_a F(x) = D_a F(y)$ for some $a, x, y \in \mathbb{F}_{2^n}$ with $a \neq 0$, $x \neq y$, $x \neq a + y$;
- several cases need to be treated depending on whether x and y are in U and aU;

Derivative Analysis

- let $1_{a,b}(x) = 1$ if $x \in \{a, b\}$ and $1_{a,b}(x) = 0$ otherwise;
- D_aG and D_aF differ on the points in $U \cup (a + U)$:

$$D_aG(x) = D_aF(x) + \sum_{i=1}^{K} 1_{u_i,a+u_i}(x)v_i;$$

- for $a \in \mathbb{F}_{2^n}^*$, let $aU = \{u_i \in U : u_i + a \in U\}$ and denote by $\bar{i}$ the index j for which $u_i + a = u_j$;
- G is not APN if and only if $D_aF(x) = D_aF(y)$ for some $a, x, y \in \mathbb{F}_{2^n}$ with $a \neq 0$, $x \neq y$, $x \neq a + y$;
- several cases need to be treated depending on whether x and y are in U and aU;
- finally, we obtain the following characterization:

Derivative Analysis (2)

Theorem

G is APN if and only if every $a \in \mathbb{F}_{2^n}^*$ satisfies:

- D_aF *is 2-to-1 on* $\mathbb{F}_{2^n} \setminus (U \cup a + U)$;
- $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j + v_{\overline{p_a}(i)} + v_{\overline{p_a}(j)}$ *for* $i, j \in All(p_a)$ *unless* $u_i = u_j$ *or* $u_i + u_j = a$;
- $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j + v_{\overline{p_a}(i)}$ *for* $i \in All(p_a), j \notin All(p_a)$;
- $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j$ *for* $i, j \notin All(p_a)$ *unless* $u_i = u_j$;
- $D_aF(u_i) + D_aF(x) \neq v_i + v_{\overline{p_a}(i)}$ *for* $i \in All(p_a), x \notin (U \cup a + U)$;
- $D_aF(u_i) + D_aF(x) \neq v_i$ *for* $i \notin All(p_a), x \notin (U \cup a + U)$.

Applications of the Theorem

- if $u_1, u_2, \ldots, u_K$ are known, the theorem can be used to filter the domains of $v_1, v_2, \ldots, v_K$;

Applications of the Theorem

- if $u_1, u_2, \ldots, u_K$ are known, the theorem can be used to filter the domains of $v_1, v_2, \ldots, v_K$;
- for $F(x) = x^3$ over $\mathbb{F}_{2^5}$ and $U = \{\alpha^i : i \in \{0, 1, \ldots, 5\}\}$, where α is primitive in $\mathbb{F}_{2^5}$, no choice for $v_1, \ldots, v_6$ produces an APN function;

Applications of the Theorem

- if $u_1, u_2, \ldots, u_K$ are known, the theorem can be used to filter the domains of $v_1, v_2, \ldots, v_K$;
- for $F(x) = x^3$ over $\mathbb{F}_{2^5}$ and $U = \{\alpha^i : i \in \{0, 1, \ldots, 5\}\}$, where α is primitive in $\mathbb{F}_{2^5}$, no choice for $v_1, \ldots, v_6$ produces an APN function;
- checking all possibilities by hand requires about 75 hours; filtering according to the theorem requires less than a second;

Applications of the Theorem

- if $u_1, u_2, \ldots, u_K$ are known, the theorem can be used to filter the domains of $v_1, v_2, \ldots, v_K$;
- for $F(x) = x^3$ over $\mathbb{F}_{2^5}$ and $U = \{\alpha^i : i \in \{0, 1, \ldots, 5\}\}$, where α is primitive in $\mathbb{F}_{2^5}$, no choice for $v_1, \ldots, v_6$ produces an APN function;
- checking all possibilities by hand requires about 75 hours; filtering according to the theorem requires less than a second;
- various iterative filtering procedures can be applied if some u_i and v_i are known;

Applications of the Theorem

- if $u_1, u_2, \ldots, u_K$ are known, the theorem can be used to filter the domains of $v_1, v_2, \ldots, v_K$;
- for $F(x) = x^3$ over $\mathbb{F}_{2^5}$ and $U = \{\alpha^i : i \in \{0, 1, \ldots, 5\}\}$, where α is primitive in $\mathbb{F}_{2^5}$, no choice for $v_1, \ldots, v_6$ produces an APN function;
- checking all possibilities by hand requires about 75 hours; filtering according to the theorem requires less than a second;
- various iterative filtering procedures can be applied if some u_i and v_i are known;
- even if nothing is known, a lower bound on the distance to the "closest" APN function can be computed from point (vi) of the theorem.

Lower Bound on Distance to Closest APN Function

- by condition (vi), any derivative D_aF having $D_aF(u_i) + v_i$ in its image must satisfy either $a + u_i \in U$ or $D_aF(u_j) = D_aF(u_i) + v_i$ for $j \neq i$;

Lower Bound on Distance to Closest APN Function

- by condition (vi), any derivative D_aF having $D_aF(u_i) + v_i$ in its image must satisfy either $a + u_i \in U$ or $D_aF(u_j) = D_aF(u_i) + v_i$ for $j \neq i$;
- let $m_F^{\beta}(b) = \#\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_aF(x) = b + F(a + \beta))\}$;

Lower Bound on Distance to Closest APN Function

- by condition (vi), any derivative D_aF having $D_aF(u_i) + v_i$ in its image must satisfy either $a + u_i \in U$ or $D_aF(u_j) = D_aF(u_i) + v_i$ for $j \neq i$;
- let $m_F^{\beta}(b) = \#\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_aF(x) = b + F(a + \beta))\}$;
- to count the number of $a \in \mathbb{F}_{2^n}^*$ for which D_aF maps to $D_aF(u_i) + v_i$ for arbitrary values of u_i and v_i we need to find the maximum value of $m_F^{\beta}(b)$ through all $b, \beta \in \mathbb{F}_{2^n}$;

Lower Bound on Distance to Closest APN Function

- by condition (vi), any derivative D_aF having $D_aF(u_i) + v_i$ in its image must satisfy either $a + u_i \in U$ or $D_aF(u_j) = D_aF(u_i) + v_i$ for $j \neq i$;
- let $m_F^\beta(b) = \#\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_aF(x) = b + F(a + \beta))\}$;
- to count the number of $a \in \mathbb{F}_{2^n}^*$ for which D_aF maps to $D_aF(u_i) + v_i$ for arbitrary values of u_i and v_i we need to find the maximum value of $m_F^\beta(b)$ through all $b, \beta \in \mathbb{F}_{2^n}$;
- as an "intermediate step" we let $m_F^\beta = \max\{m_F^\beta(b) : b \in \mathbb{F}_{2^n}\}$;

Lower Bound on Distance to Closest APN Function

- by condition (vi), any derivative D_aF having $D_aF(u_i) + v_i$ in its image must satisfy either $a + u_i \in U$ or $D_aF(u_j) = D_aF(u_i) + v_i$ for $j \neq i$;
- let $m_F^\beta(b) = \#\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_aF(x) = b + F(a+\beta))\}$;
- to count the number of $a \in \mathbb{F}_{2^n}^*$ for which D_aF maps to $D_aF(u_i) + v_i$ for arbitrary values of u_i and v_i we need to find the maximum value of $m_F^\beta(b)$ through all $b, \beta \in \mathbb{F}_{2^n}$;
- as an "intermediate step" we let $m_F^\beta = \max\{m_F^\beta(b) : b \in \mathbb{F}_{2^n}\}$;
- finally, denote $m_F = \max\{m_F^\beta(b) : b, \beta \in \mathbb{F}_{2^n}\} = \max\{m_F^\beta : \beta \in \mathbb{F}_{2^n}\}$;

Lower Bound on Distance to Closest APN Function

- by condition (vi), any derivative D_aF having $D_aF(u_i) + v_i$ in its image must satisfy either $a + u_i \in U$ or $D_aF(u_j) = D_aF(u_i) + v_i$ for $j \neq i$;
- let $m_F^\beta(b) = \#\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_aF(x) = b + F(a + \beta))\}$;
- to count the number of $a \in \mathbb{F}_{2^n}^*$ for which D_aF maps to $D_aF(u_i) + v_i$ for arbitrary values of u_i and v_i we need to find the maximum value of $m_F^\beta(b)$ through all $b, \beta \in \mathbb{F}_{2^n}$;
- as an "intermediate step" we let $m_F^\beta = \max\{m_F^\beta(b) : b \in \mathbb{F}_{2^n}\}$;
- finally, denote $m_F = \max\{m_F^\beta(b) : b, \beta \in \mathbb{F}_{2^n}\} = \max\{m_F^\beta : \beta \in \mathbb{F}_{2^n}\}$;
- then for any APN function G we have

$$d(F, G) \geq \left\lceil \frac{m_F}{3} \right\rceil + 1.$$

Invariance Properties

Proposition

Let F and F' be CCZ-equivalent functions via $\mathcal{L} = (L_1, L_2)$. Then

$$m_F^{\beta}(b) = m_F^{L_1(\beta,b)}(L_2(\beta, b)).$$

Hence, m_F is invariant under CCZ-equivalence.

Proposition

Let F be a quadratic function over $\mathbb{F}_{2^n}$. Then $m_F^{\beta} = m_F^{\beta'}$ holds for any $\beta, \beta' \in \mathbb{F}_{2^n}$.

Hence only e.g. m_F^0 has to be computed for quadratic functions.

Values of m_F for all Switching Class Representatives

Dimension	F	m_F	Distance
4	x^3	3	2
5	x^3	15	6
5	x^5	15	6
5	x^{15}	9	4
6	1.1	27	10
6	1.2	27	10
6	2.1	15	6
6	2.2	27	10
6	2.3	27	10
6	2.4	15	6
6	2.5	15	6
6	2.6	15	6
6	2.7	15	6
6	2.8	15	6
6	2.9	21	8
6	2.10	21	8
6	2.11	15	6
6	2.12	15	6
7	all	63	22
8	1.1	111	38
8	1.2	111	38

Dimension	F	m_F	Distance
8	1.3	111	38
8	1.4	111	38
8	1.5	111	38
8	1.6	111	38
8	1.7	111	38
8	1.8	111	38
8	1.9	111	38
8	1.10	111	38
8	1.11	111	38
8	1.12	111	38
8	1.13	111	38
8	1.14	99	34
8	1.15	111	38
8	1.16	111	38
8	1.17	111	38
8	2.1	111	38
8	3.1	111	38
8	4.1	99	34
8	5.1	105	36
8	6.1	105	36
8	7.1	111	38

The Case of Constant Shift

- if $v_1 = v_2 = \cdots = v_K = v \neq 0$, the APN-ness of G can be characterized by solving a system of linear equations;

The Case of Constant Shift

- if $v_1 = v_2 = \cdots = v_K = v \neq 0$, the APN-ness of G can be characterized by solving a system of linear equations;
- for $(a, x, y) \in \mathbb{F}_{2^n}^3$, count the number $N_{a,x,y}$ of elements from the set $\{x, y, a + x, a + y\}$ that are in U;

The Case of Constant Shift

- if $v_1 = v_2 = \cdots = v_K = v \neq 0$, the APN-ness of G can be characterized by solving a system of linear equations;
- for $(a, x, y) \in \mathbb{F}_{2^n}^3$, count the number $N_{a,x,y}$ of elements from the set $\{x, y, a + x, a + y\}$ that are in U;
- $D_a G(x) = b$ can have more than two solutions if and only if

$$D_a F(x) + D_a F(y) = v N_{a,x,y}$$

for some $x, y \in \mathbb{F}_{2^n}$ with $x + y \neq a$;

The Case of Constant Shift

- if $v_1 = v_2 = \cdots = v_K = v \neq 0$, the APN-ness of G can be characterized by solving a system of linear equations;
- for $(a, x, y) \in \mathbb{F}_{2^n}^3$, count the number $N_{a,x,y}$ of elements from the set $\{x, y, a + x, a + y\}$ that are in U;
- $D_a G(x) = b$ can have more than two solutions if and only if

$$D_a F(x) + D_a F(y) = vN_{a,x,y}$$

  for some $x, y \in \mathbb{F}_{2^n}$ with $x + y \neq a$;
- a system of linear equations with the unknowns u_a can be constructed that prevents this from happening;

The Case of Constant Shift

- if $v_1 = v_2 = \cdots = v_K = v \neq 0$, the APN-ness of G can be characterized by solving a system of linear equations;
- for $(a, x, y) \in \mathbb{F}_{2^n}^3$, count the number $N_{a,x,y}$ of elements from the set $\{x, y, a + x, a + y\}$ that are in U;
- $D_a G(x) = b$ can have more than two solutions if and only if

$$D_a F(x) + D_a F(y) = v N_{a,x,y}$$

  for some $x, y \in \mathbb{F}_{2^n}$ with $x + y \neq a$;
- a system of linear equations with the unknowns u_a can be constructed that prevents this from happening;
- here any $a \in \mathbb{F}_{2^n}$, let u_a be an indicator variable such that $u_a = 1 \iff a \in U$.

The Case of Constant Shift

- find all (x, y, a) such that $D_aF(x) + D_aF(y) = v$;

The Case of Constant Shift

- find all (x, y, a) such that $D_aF(x) + D_aF(y) = v$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 0$;

The Case of Constant Shift

- find all (x, y, a) such that $D_aF(x) + D_aF(y) = v$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 0$;
- find also all (x, y, a) such that $D_aF(x) + D_aF(y) = 0$;

The Case of Constant Shift

- find all (x, y, a) such that $D_aF(x) + D_aF(y) = v$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 0$;
- find also all (x, y, a) such that $D_aF(x) + D_aF(y) = 0$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 1$;

The Case of Constant Shift

- find all (x, y, a) such that $D_a F(x) + D_a F(y) = v$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 0$;
- find also all (x, y, a) such that $D_a F(x) + D_a F(y) = 0$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 1$;
- solve this system of equations, e.g. by constructing an $e \times (2^n)$ matrix over $\mathbb{F}_2$, where e is the number of tuples that we consider;

The Case of Constant Shift

- find all (x, y, a) such that $D_aF(x) + D_aF(y) = v$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 0$;
- find also all (x, y, a) such that $D_aF(x) + D_aF(y) = 0$;
- consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 1$;
- solve this system of equations, e.g. by constructing an $e \times (2^n)$ matrix over $\mathbb{F}_2$, where e is the number of tuples that we consider;
- the solutions give precisely those sets $U \subseteq \mathbb{F}_{2^n}$ for which G is APN.

Directions of Research

- improve the lower bound on the distance between APN functions or show that it is tight;

Directions of Research

- improve the lower bound on the distance between APN functions or show that it is tight;
- investigate the structure of sets $u_1, u_2, \ldots, u_K$ for which G can be APN;

Directions of Research

- improve the lower bound on the distance between APN functions or show that it is tight;
- investigate the structure of sets $u_1, u_2, \ldots, u_K$ for which G can be APN;
- investigate similar relations between functions other than APN, e.g. AB, plateaued, differentially 4-uniform;

Directions of Research

- improve the lower bound on the distance between APN functions or show that it is tight;
- investigate the structure of sets $u_1, u_2, \ldots, u_K$ for which G can be APN;
- investigate similar relations between functions other than APN, e.g. AB, plateaued, differentially 4-uniform;
- derive efficient search procedures for constructing one APN function from another.