Almost Perfect Nonlinear Permutations

Dáša Krasnayová

Spring School, April 2017

Table of contents

Table of Contents

Boolean function

Definition (Boolean function)

A *boolean function* is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ for some non-negative integer n.
A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where $n \geq m \geq 1$, n, m non-negative integers, is called a *vectorial boolean function*.

Boolean function

Definition (Boolean function)

A *boolean function* is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ for some non-negative integer n.
A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where $n \geq m \geq 1$, n, m non-negative integers, is called a *vectorial boolean function*.

Notice that $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ are isomorphic as a vector spaces over $\mathbb{F}_2$.

Almost Perfect Nonlinear function I

Definition (Almost Perfect Nonlinear function)

A function F is called *Almost Perfect Nonlinear (APN)* if

$$F(x) + F(x + a) = b$$

has two or zero solutions $x \in \mathbb{F}$ for every $a, b \in \mathbb{F}$, $a \neq 0$.

Almost Prefect Nonlinear function II

Definition (Derivatives)

Derivatives of a function F are functions $D_aF(x) : \mathbb{F} \to \mathbb{F}$, $a \in \mathbb{F}^*$,

$$D_aF(x) = F(x) + F(x+a) + F(a) + F(0).$$

Almost Prefect Nonlinear function II

Definition (Derivatives)

Derivatives of a function F are functions $D_aF(x) : \mathbb{F} \to \mathbb{F}$, $a \in \mathbb{F}^*$,

$$D_aF(x) = F(x) + F(x+a) + F(a) + F(0).$$

Definition (Equivalent definition of an APN function)

F is called an *APN function* if and only if
$|D_aF| = |\{D_aF(x) : x \in \mathbb{F}\}| = \frac{|\mathbb{F}|}{2}$ for every $a \in \mathbb{F}^*$.

Almost Prefect Nonlinear function - examples

- Gold functions: x^{2k+1}, where $\gcd(n, k) = 1$,

Almost Prefect Nonlinear function - examples

- Gold functions: x^{2k+1}, where $\gcd(n, k) = 1$,
- Kasami functions: $x^{2i} + x^i + 1$, where $\gcd(n, k) = 1$,

Almost Prefect Nonlinear function - examples

- Gold functions: x^{2k+1}, where $\gcd(n, k) = 1$,
- Kasami functions: $x^{2i} + x^i + 1$, where $\gcd(n, k) = 1$,
- Inverse function: $x^{2k} + 1$, where $n = 2k + 1$,

Almost Prefect Nonlinear function - examples

- Gold functions: x^{2k+1}, where $\gcd(n, k) = 1$,
- Kasami functions: $x^{2i} + x^i + 1$, where $\gcd(n, k) = 1$,
- Inverse function: $x^{2k} + 1$, where $n = 2k + 1$,
- ...

Almost Prefect Nonlinear function - examples

- Gold functions: x^{2k+1}, where $\gcd(n, k) = 1$,
- Kasami functions: $x^{2i} + x^i + 1$, where $\gcd(n, k) = 1$,
- Inverse function: $x^{2k} + 1$, where $n = 2k + 1$,
- ...

Almost Prefect Nonlinear function - examples

- Gold functions: x^{2k+1}, where $\gcd(n, k) = 1$,
- Kasami functions: $x^{2i} + x^i + 1$, where $\gcd(n, k) = 1$,
- Inverse function: $x^{2k} + 1$, where $n = 2k + 1$,
- ...

Unfortunately, none of these functions is a permutation in fields with n even.

APN permutations

Big APN problem

Does there exist an APN permutation on $\mathbb{F}_2^n$ if n is even?

APN permutations

Big APN problem

Does there exist an APN permutation on $\mathbb{F}_2^n$ if n is even?

The first and the only example of an APN permutation in even dimension so far was presented by Dillon et al. in 2009.

APN permutations

Big APN problem

Does there exist an APN permutation on $\mathbb{F}_2^n$ if n is even?

The first and the only example of an APN permutation in even dimension so far was presented by Dillon et al. in 2009.

Kim function

The function is known as the *Kim function* or κ *function* and is defined as

$$\kappa(x) = x^3 + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}$ whose minimal polynomial over $\mathbb{F}_2$ is $x^6 + x^4 + x^3 + x + 1$.

Equivalence of functions

Definition (Extended Affine Equivalence)

Vectorial boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *Extended Affine equivalent*, i.e. $f \approx_{EA} g$, if there exist linear functions L_1, L_2 and L_3 such that $L_1 \circ f \circ L_2(x) + L_3(x) = g(x)$, for every $x \in \mathbb{F}_{2^n}$ and L_1 and L_2 are permutations.

Equivalence of functions

Definition (Extended Affine Equivalence)

Vectorial boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *Extended Affine equivalent*, i.e. $f \approx_{EA} g$, if there exist linear functions L_1, L_2 and L_3 such that $L_1 \circ f \circ L_2(x) + L_3(x) = g(x)$, for every $x \in \mathbb{F}_{2^n}$ and L_1 and L_2 are permutations.

EA equivalence preserves a lot of features, for example algebraic degree, being a permutation and being an APN function.

Equivalence of functions

Definition (Extended Affine Equivalence)

Vectorial boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *Extended Affine equivalent*, i.e. $f \approx_{EA} g$, if there exist linear functions L_1, L_2 and L_3 such that $L_1 \circ f \circ L_2(x) + L_3(x) = g(x)$, for every $x \in \mathbb{F}_{2^n}$ and L_1 and L_2 are permutations.

EA equivalence preserves a lot of features, for example algebraic degree, being a permutation and being an APN function.

Definition (CCZ equivalence)

Boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *CCZ-equivalent* if their graphs G_f, G_g are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $y = f(x)$ if and only if $L_2(x, y) = g(L_2(x, y))$ (or $L(G_f) = G_g$).

Equivalence of functions

Definition (Extended Affine Equivalence)

Vectorial boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *Extended Affine equivalent*, i.e. $f \approx_{EA} g$, if there exist linear functions L_1, L_2 and L_3 such that $L_1 \circ f \circ L_2(x) + L_3(x) = g(x)$, for every $x \in \mathbb{F}_{2^n}$ and L_1 and L_2 are permutations.

EA equivalence preserves a lot of features, for example algebraic degree, being a permutation and being an APN function.

Definition (CCZ equivalence)

Boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called *CCZ-equivalent* if their graphs G_f, G_g are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $y = f(x)$ if and only if $L_2(x, y) = g(L_2(x, y))$ (or $L(G_f) = G_g$).

CCZ equivalence does not preserve many features of a function but it preserves the APN property.

Table of Contents

Trace-0/Trace-1 decomposition I

- We define

$$\mathcal{T}_1 = \left\{ g \in \mathbb{F}_{q^2} : \mathrm{Tr}_m^n(g) = g^q + g = 1 \right\} \cup \{1\}$$

  a set of all Trace-1 elements and 1.

Trace-0/Trace-1 decomposition I

- We define

$$\mathcal{T}_1 = \left\{ g \in \mathbb{F}_{q^2} : \mathrm{Tr}_m^n(g) = g^q + g = 1 \right\} \cup \{1\}$$

  a set of all Trace-1 elements and 1.
- Moreover, we can notice that elements of the sub-field $\mathbb{F}_q$ are exactly all Trace-0 elements of $\mathbb{F}_{q^2}$, i.e. $\mathbb{F}_q = \{X \in \mathbb{F}_{q^2} : \mathrm{Tr}_m^n(X) = 0\}$.

Trace-0/Trace-1 decomposition I

- We define

$$\mathcal{T}_1 = \left\{ g \in \mathbb{F}_{q^2} : \mathrm{Tr}_m^n(g) = g^q + g = 1 \right\} \cup \{1\}$$

  a set of all Trace-1 elements and 1.
- Moreover, we can notice that elements of the sub-field $\mathbb{F}_q$ are exactly all Trace-0 elements of $\mathbb{F}_{q^2}$, i.e. $\mathbb{F}_q = \{X \in \mathbb{F}_{q^2} : \mathrm{Tr}_m^n(X) = 0\}$.
- Every element of $\mathbb{F}_{q^2}$ can then be written using elements of $\mathcal{T}_1$ and $\mathbb{F}_q$ in two ways presented in following propositions.

Trace-0/Trace-1 decomposition II

First decomposition

Every $X \in \mathbb{F}_{q^2}^*$ can be uniquely written as $X = xg$, where $x \in \mathbb{F}_q^*$ and $g \in \mathcal{T}_1$.

Trace-0/Trace-1 decomposition II

First decomposition

Every $X \in \mathbb{F}_{q^2}^*$ can be uniquely written as $X = xg$, where $x \in \mathbb{F}_q^*$ and $g \in \mathcal{T}_1$.

Second decomposition

For every $g \in \mathcal{T}_1 \setminus \{1\}$, any $X \in \mathbb{F}_{q^2}$ can be uniquely written as $X = xg + y$, where $x, y \in \mathbb{F}_q$.

Trace-0/Trace-1 decomposition II

First decomposition

Every $X \in \mathbb{F}_{q^2}^*$ can be uniquely written as $X = xg$, where $x \in \mathbb{F}_q^*$ and $g \in \mathcal{T}_1$.

Second decomposition

For every $g \in \mathcal{T}_1 \setminus \{1\}$, any $X \in \mathbb{F}_{q^2}$ can be uniquely written as $X = xg + y$, where $x, y \in \mathbb{F}_q$.

Both have been proven in *APN trinomials and hexanomials* by Faruk Göloğlu in 2015.

Table of Contents

Chosen family of functions

- We studied a family of the functions which can be written in a form

$$F(x) = x^3 + bx^{3q} + cx^{2q+1} + dx^{q+2},$$

where $q = 2^m$ and $b, c, d \in \mathbb{F}_q$.

Chosen family of functions

- We studied a family of the functions which can be written in a form

$$F(x) = x^3 + bx^{3q} + cx^{2q+1} + dx^{q+2},$$

where $q = 2^m$ and $b, c, d \in \mathbb{F}_q$.

- Both Kim function and our family of functions satisfy so-called *subspace property* for $k = 1$. We say that a function $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ satisfies the subspace property, if there is an integer k such that

$$f(\lambda X) = \lambda^{2^k+1} f(X)$$

for every $\lambda \in \mathbb{F}_q$ and $X \in \mathbb{F}_{q^2}$.

Chosen family of functions

- We studied a family of the functions which can be written in a form

$$F(x) = x^3 + bx^{3q} + cx^{2q+1} + dx^{q+2},$$

where $q = 2^m$ and $b, c, d \in \mathbb{F}_q$.

- Both Kim function and our family of functions satisfy so-called *subspace property* for $k = 1$. We say that a function $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ satisfies the subspace property, if there is an integer k such that

$$f(\lambda X) = \lambda^{2^k+1} f(X)$$

for every $\lambda \in \mathbb{F}_q$ and $X \in \mathbb{F}_{q^2}$.

- Kim function is CCZ-equivalent to a member of this family.

Technique I

- According to the second definition of an APN function, F is APN if and only if $|D_A F| = \frac{|\mathbb{F}|}{2}$ for every $A \in \mathbb{F}^*$.

Technique I

- According to the second definition of an APN function, F is APN if and only if $|D_A F| = \frac{|\mathbb{F}|}{2}$ for every $A \in \mathbb{F}^*$.
- Since F is a quadratic function, $D_A F$ is a linear function and previous point is equivalent to $D_A F = 0$ has exactly 2 solutions in F for every $A \in \mathbb{F}^*$.

Technique I

- According to the second definition of an APN function, F is APN if and only if $|D_A F| = \frac{|\mathbb{F}|}{2}$ for every $A \in \mathbb{F}^*$.
- Since F is a quadratic function, $D_A F$ is a linear function and previous point is equivalent to $D_A F = 0$ has exactly 2 solutions in F for every $A \in \mathbb{F}^*$.
- We are trying to find conditions for b, c, d under which $D_A F = 0$ has exactly two solutions.

Technique I

- According to the second definition of an APN function, F is APN if and only if $|D_A F| = \frac{|\mathbb{F}|}{2}$ for every $A \in \mathbb{F}^*$.
- Since F is a quadratic function, $D_A F$ is a linear function and previous point is equivalent to $D_A F = 0$ has exactly 2 solutions in F for every $A \in \mathbb{F}^*$.
- We are trying to find conditions for b, c, d under which $D_A F = 0$ has exactly two solutions.
- Since $D_A F(0) = F(0) + F(0 + A) + F(0) + F(A) = 0$, 0 is always a solution and we are looking for b, c, d such that $D_A F$ has exactly one solution in $\mathbb{F}^*$.

Technique II

- According to the first decomposition, A can be uniquely written as $A = ah$, where $a \in \mathbb{F}_q^*$ and $h \in TI$

Technique II

- According to the first decomposition, A can be uniquely written as $A = ah$, where $a \in \mathbb{F}_q^*$ and $h \in TI$
- Notice that

$$\begin{aligned} D_A F(aX) &= F(aX) + F(aX + ah) + F(ah) \\ &= a^3 \left[F(X) + F(X + h) + F(h)\right] \\ &= a^3 D_h F(X). \end{aligned}$$

Therefore number of solutions of $D_A F = 0$ only depends on h.

Technique II

- According to the first decomposition, A can be uniquely written as $A = ah$, where $a \in \mathbb{F}_q^*$ and $h \in TI$
- Notice that

$$\begin{aligned} D_A F(aX) &= F(aX) + F(aX + ah) + F(ah) \\ &= a^3 \left[F(X) + F(X + h) + F(h)\right] \\ &= a^3 D_h F(X). \end{aligned}$$

  Therefore number of solutions of $D_A F = 0$ only depends on h.
- We will consider two cases – $h = 1$ and $h \in \mathcal{T}_1 \setminus \{1\}$.

Case $h = 1$

- For $h = 1$ we have

$$\begin{aligned} D_1F(X) &= F(X) + F(X+1) + F(0) + F(1) \\ &= X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2} \\ &+ (X+1)^3 + b(X+1)^{3q} + c(X+1)^{2q+1} + dX^{q+2} + F(1) \\ &= X(1+c) + X^2(1+d) + X^q(b+d) + X^{2q}(b+c) = 0. \end{aligned}$$

Case $h = 1$

- For $h = 1$ we have

$$\begin{aligned} D_1F(X) &= F(X) + F(X+1) + F(0) + F(1) \\ &= X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2} \\ &+ (X+1)^3 + b(X+1)^{3q} + c(X+1)^{2q+1} + dX^{q+2} + F(1) \\ &= X(1+c) + X^2(1+d) + X^q(b+d) + X^{2q}(b+c) = 0. \end{aligned}$$

- We can write $X \in \mathbb{F}_{q^2}^*$ as xg such that $x \in \mathbb{F}_q^*$ and $g \in \mathcal{T}_1$.

Case $h = 1$

- For $h = 1$ we have

$$\begin{aligned} D_1F(X) &= F(X) + F(X+1) + F(0) + F(1) \\ &= X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2} \\ &+ (X+1)^3 + b(X+1)^{3q} + c(X+1)^{2q+1} + dX^{q+2} + F(1) \\ &= X(1+c) + X^2(1+d) + X^q(b+d) + X^{2q}(b+c) = 0. \end{aligned}$$

- We can write $X \in \mathbb{F}_{q^2}^*$ as xg such that $x \in \mathbb{F}_q^*$ and $g \in \mathcal{T}_1$.
- We get two equations

$$x^2g^2(1+b+c+d) + xg(1+b+c+d) + x^2(b+c) + x(b+d) = 0 \tag{1}$$

for $g \in \mathcal{T}_1 \setminus \{1\}$ and

$$(x^2+x)(1+b+c+d) = 0 \tag{2}$$

for $g = 1$.

Case $h = 1$

- From the equation (2) we get a condition $\Delta = 1 + b + c + d \neq 0$.

Case $h = 1$

- From the equation (2) we get a condition $\Delta = 1 + b + c + d \neq 0$.
- Equation (1),

$$x^2 g^2 \Delta + xg\Delta + x^2(b + c) + x(b + d) = 0,$$

should not have any solution.

Case $h = 1$

- From the equation (2) we get a condition $\Delta = 1 + b + c + d \neq 0$.
- Equation (1),

$$x^2 g^2 \Delta + xg\Delta + x^2(b + c) + x(b + d) = 0,$$

  should not have any solution.
- We will write $g^2 = g + \mathrm{Tr}_m^n(g^3) + 1$ and denote $S_g = \mathrm{Tr}_m^n(g^3) = g^2 + g + 1$.

Case $h = 1$

- From the equation (2) we get a condition $\Delta = 1 + b + c + d \neq 0$.
- Equation (1),

$$x^2 g^2 \Delta + x g \Delta + x^2(b + c) + x(b + d) = 0,$$

  should not have any solution.
- We will write $g^2 = g + \mathrm{Tr}_m^n(g^3) + 1$ and denote $S_g = \mathrm{Tr}_m^n(g^3) = g^2 + g + 1$.
- Equation (1) is now

$$g(x^2 + x)\Delta + x^2(1 + d) + x(b + d) + x^2 S_g \Delta = 0.$$

Case $h = 1$

- From the equation (2) we get a condition $\Delta = 1 + b + c + d \neq 0$.
- Equation (1),

$$x^2 g^2 \Delta + x g \Delta + x^2(b + c) + x(b + d) = 0,$$

  should not have any solution.
- We will write $g^2 = g + \mathrm{Tr}_m^n(g^3) + 1$ and denote $S_g = \mathrm{Tr}_m^n(g^3) = g^2 + g + 1$.
- Equation (1) is now

$$g(x^2 + x)\Delta + x^2(1 + d) + x(b + d) + x^2 S_g \Delta = 0.$$

- According to the first decomposition, this is true if and only if $(x^2 + x)\Delta = 0$ and $x^2(1 + d) + x(b + d) + x^2 S_g \Delta = 0$.

Case $h = 1$

- First part, $(x^2 + x)\Delta$, is 0 if $x = 1$. For $x = 1$ the second part looks like this:

$$(1 + d) + (1 + b) + S_g\Delta = 0$$

Case $h = 1$

- First part, $(x^2 + x)\Delta$, is 0 if $x = 1$. For $x = 1$ the second part looks like this:
$$(1 + d) + (1 + b) + S_g\Delta = 0$$
- This means that if for some g
$$S_g = \frac{b + d}{\Delta},$$
then $A = g$ is a solution which should not exist.

Case $h = 1$

- First part, $(x^2 + x)\Delta$, is 0 if $x = 1$. For $x = 1$ the second part looks like this:
$$(1 + d) + (1 + b) + S_g\Delta = 0$$
- This means that if for some g
$$S_g = \frac{b + d}{\Delta},$$
then $A = g$ is a solution which should not exist.
- We know that
$$\mathrm{Tr}_1^m(S_g) \begin{cases} 1, & \text{if } m \text{ is even,} \\ 0, & \text{if } m \text{ is odd.} \end{cases}$$

Case $h = 1$

- First part, $(x^2 + x)\Delta$, is 0 if $x = 1$. For $x = 1$ the second part looks like this:
$$(1 + d) + (1 + b) + S_g\Delta = 0$$
- This means that if for some g
$$S_g = \frac{b + d}{\Delta},$$
then $A = g$ is a solution which should not exist.
- We know that
$$\mathrm{Tr}_1^m(S_g) \begin{cases} 1, & \text{if } m \text{ is even,} \\ 0, & \text{if } m \text{ is odd.} \end{cases}$$
- This means that $S_g = (b + d)/\Delta$ happens if and only if their traces are equal.

Conditions from the case $h = 1$

m odd	m even
$1 + b + c + d \neq 0$	
$\mathrm{tr}_1^m\left(\frac{1+b}{1+b+c+d}\right) = 1$	$\mathrm{tr}_1^m\left(\frac{1+b}{1+b+c+d}\right) = 0$

Case $h \neq 1$

- Equations are more complicated.

Case $h \neq 1$

- Equations are more complicated.
- Conditions found by using Trace-0/Trace-1 decomposition repeatedly.

Case $h \neq 1$

- Equations are more complicated.
- Conditions found by using Trace-0/Trace-1 decomposition repeatedly.

Case $h \neq 1$

- Equations are more complicated.
- Conditions found by using Trace-0/Trace-1 decomposition repeatedly.

m odd	m even
$\Delta = 1 + b + c + d \neq 0$	
$\mathrm{Tr}_1^m(\frac{1+b}{1+b+c+d}) = 1$	$\mathrm{Tr}_1^m(\frac{1+b}{1+b+c+d}) = 0$
$1 + c + b^2 + bd \neq 0$	–
$\mathrm{Tr}_1^m(\frac{\Delta^2}{1+b^2+c+bd}) = 1$	–
if $\mathrm{Tr}_1^m(\frac{bd+c}{\Delta^2}) = 1$, then $b^2c^2 + d^2 \neq \Delta^2(bd + c)$	
$\mathrm{Tr}_1^m\left(\frac{\Delta(T\Delta+c+d)(T^2\Delta^2+bd+c)}{(T\Delta^2+bc+d)^2}\right) = 1,$ for every T such that $\mathrm{Tr}_1^m(T) = 1$, $\Delta T + 1 + b \neq 0$, $T\Delta^2 + bc + d \neq 0$ and $\Delta^2 T^2 + bd + c \neq 0$	

Table of Contents

Petr's simplification

- The most complicated condition is the last one:

$$\mathrm{Tr}_1^m\left(\frac{\Delta(T\Delta+c+d)(T^2\Delta^2+bd+c)}{(T\Delta^2+bc+d)^2}\right)=1,$$

for every T such that $\mathrm{Tr}_1^m(T)=1$, $\Delta T+1+b\neq 0$, $T\Delta^2+bc+d\neq 0$ and $\Delta^2T^2+bd+c\neq 0$.

Petr's simplification

- The most complicated condition is the last one:

$$\mathrm{Tr}_1^m\left(\frac{\Delta(T\Delta+c+d)(T^2\Delta^2+bd+c)}{(T\Delta^2+bc+d)^2}\right)=1,$$

for every T such that $\mathrm{Tr}_1^m(T)=1$, $\Delta T+1+b\neq 0$, $T\Delta^2+bc+d\neq 0$ and $\Delta^2T^2+bd+c\neq 0$.

- Petr Lisoněk was able to find an equivalent condition, which is easier to work with:

$$\mathrm{Tr}_1^m\left(\frac{(T\Delta+c+d)(bd+c+c^2+d^2)(bd+c+b^2+1)}{\Delta(T\Delta^2+bc+d)}\right)=0$$

for every T such that $\mathrm{Tr}_1^m(T)=1$, $\Delta T+1+b\neq 0$, $T\Delta^2+bc+d\neq 0$ and $\Delta^2T^2+bd+c\neq 0$.

Petr's simplification

- If $(bd + c + c^2 + d^2) = 0$ or $(bd + c + b^2 + 1) = 0$, then function F is APN but it is affinely equivalent to a Gold function (x^3 or $x^{2^{m-1}} + 1$).

Petr's simplification

- If $(bd + c + c^2 + d^2) = 0$ or $(bd + c + b^2 + 1) = 0$, then function F is APN but it is affinely equivalent to a Gold function (x^3 or $x^{2^{m-1}} + 1$).
- It is known that Gold functions are not CCZ-equivalent to a permutation for n even.

Faruk's contribution

- If $(bd + c + c^2 + d^2) \neq 0$, $(bd + c + b^2 + 1) \neq 0$ and $n > 6$, then

$$\mathrm{Tr}_1^m \left(\frac{(T\Delta + c + d)(bd + c + c^2 + d^2)(bd + c + b^2 + 1)}{\Delta(T\Delta^2 + bc + d)} \right) = 0$$

  cannot hold for so many Ts.

Faruk's contribution

- If $(bd + c + c^2 + d^2) \neq 0$, $(bd + c + b^2 + 1) \neq 0$ and $n > 6$, then

$$\mathrm{Tr}_1^m \left(\frac{(T\Delta + c + d)(bd + c + c^2 + d^2)(bd + c + b^2 + 1)}{\Delta(T\Delta^2 + bc + d)} \right) = 0$$

  cannot hold for so many Ts.
- Every element of $\mathbb{F}_q$ with trace 0 can be written as $x^2 + x$ for some $x \in \mathbb{F}_q$.

Faruk's contribution

- If $(bd + c + c^2 + d^2) \neq 0$, $(bd + c + b^2 + 1) \neq 0$ and $n > 6$, then

$$\mathrm{Tr}_1^m \left(\frac{(T\Delta + c + d)(bd + c + c^2 + d^2)(bd + c + b^2 + 1)}{\Delta(T\Delta^2 + bc + d)} \right) = 0$$

  cannot hold for so many Ts.
- Every element of $\mathbb{F}_q$ with trace 0 can be written as $x^2 + x$ for some $x \in \mathbb{F}_q$.
- Every T can be written as $y^2 + y + k$ for some $y \in \mathbb{F}_q$ and some fixed $k \in \mathbb{F}_q$ such that $\mathrm{Tr}_1^m(k) = 1$.

Faruk's contribution

- If $(bd + c + c^2 + d^2) \neq 0$, $(bd + c + b^2 + 1) \neq 0$ and $n > 6$, then

$$\mathrm{Tr}_1^m \left(\frac{(T\Delta + c + d)(bd + c + c^2 + d^2)(bd + c + b^2 + 1)}{\Delta(T\Delta^2 + bc + d)} \right) = 0$$

  cannot hold for so many Ts.
- Every element of $\mathbb{F}_q$ with trace 0 can be written as $x^2 + x$ for some $x \in \mathbb{F}_q$.
- Every T can be written as $y^2 + y + k$ for some $y \in \mathbb{F}_q$ and some fixed $k \in \mathbb{F}_q$ such that $\mathrm{Tr}_1^m(k) = 1$.
- Our condition can be rewritten as an equation in x and y.

Faruk's contribution

- If $(bd + c + c^2 + d^2) \neq 0$, $(bd + c + b^2 + 1) \neq 0$ and $n > 6$, then

$$\mathrm{Tr}_1^m \left(\frac{(T\Delta + c + d)(bd + c + c^2 + d^2)(bd + c + b^2 + 1)}{\Delta(T\Delta^2 + bc + d)} \right) = 0$$

  cannot hold for so many Ts.
- Every element of $\mathbb{F}_q$ with trace 0 can be written as $x^2 + x$ for some $x \in \mathbb{F}_q$.
- Every T can be written as $y^2 + y + k$ for some $y \in \mathbb{F}_q$ and some fixed $k \in \mathbb{F}_q$ such that $\mathrm{Tr}_1^m(k) = 1$.
- Our condition can be rewritten as an equation in x and y.
- Every T satisfying the condition corresponds to exactly two solutions of the equation.

Faruk's contribution

- Our equation corresponds to an absolutely irreducible algebraic curve, solutions correspond to its points.

Faruk's contribution

- Our equation corresponds to an absolutely irreducible algebraic curve, solutions correspond to its points.

Hasse-Weil Bound

If we denote the number of points on the curve C of genus g over the finite field $\mathbb{F}_q$ as $\#C(\mathbb{F}_q)$, then

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

Faruk's contribution

- Our equation corresponds to an absolutely irreducible algebraic curve, solutions correspond to its points.

Hasse-Weil Bound

If we denote the number of points on the curve C of genus g over the finite field $\mathbb{F}_q$ as $\#C(\mathbb{F}_q)$, then

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

- This bound says that our condition does not hold for bigger fields.

Conslusion

There are no new APN permutations in the chosen family.

Thank you for your attention.