On quadratic APN functions $F(x) + \mathrm{Tr}(x)L(x)$

– BFA2023 –

Hiroaki Taniguchi

Yamato University

2023 September 3–8

A motivation

A switching

Let $b:\mathbb{F}_2^n \to \mathbb{F}_2$. Let $\mathbb{F}_2^n \ni x \mapsto (F(x), b(x)) \in \mathbb{F}_2^n \oplus \mathbb{F}_2 = \mathbb{F}_2^{n+1}$ be an APN $(n, n+1)$ function. Then $F + ub : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN (n, n)-function for some $u \in (\mathbb{F}_2^n)^\times$ if and only if

- if $F(x+a) + F(x) + F(t+a) + F(t) = u$, then $b(x+a) + b(x) + b(t+a) + b(t) = 0$.

A motivation

A switching

Let $b : \mathbb{F}_2^n \to \mathbb{F}_2$. Let $\mathbb{F}_2^n \ni x \mapsto (F(x), b(x)) \in \mathbb{F}_2^n \oplus \mathbb{F}_2 = \mathbb{F}_2^{n+1}$ be an APN $(n, n+1)$ function. Then $F + ub : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN (n, n)-function for some $u \in (\mathbb{F}_2^n)^\times$ if and only if

- if $F(x+a) + F(x) + F(t+a) + F(t) = u$, then $b(x+a) + b(x) + b(t+a) + b(t) = 0$.

The Inverse function $F(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$ for n even

There are many $b : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that $\mathbb{F}_{2^n} \ni x \mapsto (F(x), b(x)) \in \mathbb{F}_{2^n} \oplus \mathbb{F}_2 = \mathbb{F}_2^{n+1}$ are APN $(n, n+1)$ functions. Howevere it seems no $u \in (\mathbb{F}_{2^n})^\times$ satisfying the above condition for $F(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$, n even.

A motivation

A switching

Let $b : \mathbb{F}_2^n \to \mathbb{F}_2$. Let $\mathbb{F}_2^n \ni x \mapsto (F(x), b(x)) \in \mathbb{F}_2^n \oplus \mathbb{F}_2 = \mathbb{F}_2^{n+1}$ be an APN $(n, n+1)$ function. Then $F + ub : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN (n, n)-function for some $u \in (\mathbb{F}_2^n)^\times$ if and only if

- if $F(x+a) + F(x) + F(t+a) + F(t) = u$, then $b(x+a) + b(x) + b(t+a) + b(t) = 0$.

The Inverse function $F(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$ for n even

There are many $b : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that $\mathbb{F}_{2^n} \ni x \mapsto (F(x), b(x)) \in \mathbb{F}_{2^n} \oplus \mathbb{F}_2 = \mathbb{F}_2^{n+1}$ are APN $(n, n+1)$ functions. Howevere it seems no $u \in (\mathbb{F}_{2^n})^\times$ satisfying the above condition for $F(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$, n even.

We consider how to use these APN $(n, n+1)$ functions.

APN function, Quadratic function, CCZ equivalence

Let $\mathbb{F}_2$ be a binary field.

APN function

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an APN function if $|\{x \mid F(x+a) + F(x) = b\}| \leq 2$ for any $a \in (\mathbb{F}_2^n)^\times$ and for any $b \in \mathbb{F}_2^m$.

Quadratic function

We call a function F *quadratic* if $B_F(x, y) := F(x+y) + F(x) + F(y) + F(0)$ is $\mathbb{F}_2$-bilinear.

CCZ equivalence

Two functions F_1 and F_2 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called *CCZ-equivalent* if the graphs $G_{F_1} := \{(x, F_1(x)) \mid x \in \mathbb{F}_2^n\}$ and $G_{F_2} := \{(x, F_2(x)) \mid x \in \mathbb{F}_2^n\}$ in $\mathbb{F}_2^n \oplus \mathbb{F}_2^m$ are affine equivalent,

Known APN functions $F:\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Known APN power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	Degree
Gold	2^i+1	$\gcd(i,n)=1$	2
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$
Welch	2^t+3	$n=2t+1$	3
Niho	$2^t+2^{t/2}-1$ (t even)	$n=2t+1$	$t+1/2$
Niho	$2^t+2^{(3t+1)/2}-1$ (t odd)	$n=2t+1$	$t+1$
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$

Known quadratic APN functions on $\mathbb{F}_{2^n}$

There are more than 12 classes of known quadratic APN functions inequivalent to power functions.

There are no known infinite families of non-power, non-quadratic APN functions.

Γ-rank, Walsh transformation, Walsh spectrum

Γ-rank

The Γ*-rank* of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the rank of the incidence matrix over $\mathbb{F}_2$ of the incidence structure $\{\mathcal{P}, \mathcal{B}, I\}$, where $\mathcal{P} = \mathbb{F}_2^n \oplus \mathbb{F}_2^m$, $\mathcal{B} = \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ and $(a,b)I(u,v)$ for $(a,b) \in \mathcal{P}$ and $(u,v) \in \mathcal{B}$ if and only if $F(a+u) = b+v$.
We know that if two functions F_1 and F_2 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are CCZ-equivalent, then they have the same Γ-rank.

Γ-rank, Walsh transformation, Walsh spectrum

Walsh coefficient

For a function F on $\mathbb{F}_{2^n}$, the Walsh coefficient of F at $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^{\times}$ is defined by

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

Γ-rank, Walsh transformation, Walsh spectrum

Walsh coefficient

For a function F on $\mathbb{F}_{2^n}$, the Walsh coefficient of F at $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^{\times}$ is defined by

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

Walsh spectrum

The Walsh spectrum of F is $\mathcal{W}_F = \{W_F(a,b) \mid a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^{\times}\}$.
For a quadratic APN function F on $\mathbb{F}_{2^n}$, if n is odd, it is known that $W_F(a,b) \in \{0, \pm 2^{(n+1)/2}\}$.
If n is even, it is said that a quadratic APN function F has the classical Walsh spectrum if $\mathcal{W}_F = \{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$, and F has the non-classical Walsh spectrum if otherwise.

A condition to have an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ using functions f, g from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$

Let $f, g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^m$. We regard $\mathbb{F}_2^{n-1} \subset \mathbb{F}_2^n$.
Let $e_0 \in \mathbb{F}_2^n$ with $e_0 \notin \mathbb{F}_2^{n-1}$ and $\mathbb{F}_2^{n-1} + e_0 := \{x + e_0 \mid x \in \mathbb{F}_2^{n-1}\}$.
Then $\mathbb{F}_2^n = \mathbb{F}_2^{n-1} \cup (\mathbb{F}_2^{n-1} + e_0)$.

A condition to have an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ using functions f, g from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$

We want to have an APN function $F : \mathbb{F}_2^n = \mathbb{F}_2^{n-1} \cup (\mathbb{F}_2^{n-1} + e_0) \to \mathbb{F}_2^m$ defined by $F(x) = f(x)$ and $F(x + e_0) = g(x)$ for $x \in \mathbb{F}_2^{n-1}$.

A condition to have an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ using functions f, g from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$

We want to have an APN function $F : \mathbb{F}_2^n = \mathbb{F}_2^{n-1} \cup (\mathbb{F}_2^{n-1} + e_0) \to \mathbb{F}_2^m$ defined by $F(x) = f(x)$ and $F(x + e_0) = g(x)$ for $x \in \mathbb{F}_2^{n-1}$.

Proposition 1

F defined above is an APN function if and only if

(1) f and g are APN functions from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$,

(2) $f(x + a) + f(x) \neq g(y + a) + g(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$ and for any non-zero $a \in \mathbb{F}_2^{n-1}$, and

(3) $G_a : \mathbb{F}_2^{n-1} \ni x \mapsto f(x + a) + g(x) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$.

Proof of Proposition 1, $F(x)=f(x)$ and $F(x+e_0)=g(x)$

Proof 1

Firstly assume that F is an APN function. For $A\neq 0$, let $F(X+A)+F(X)=F(Y+A)+F(Y)$, then $X=Y$ or $X=Y+A$.

Let $A=a\in(\mathbb{F}_2^{n-1})^\times$. For any $Y=y\in\mathbb{F}_2^{n-1}$, we must have $X=y\in\mathbb{F}_2^{n-1}$ or $X=y+a\in\mathbb{F}_2^{n-1}$. Since $X\in\mathbb{F}_2^{n-1}$, we have $f(X+a)+f(X)=f(y+a)+f(y)$. Thus f must be an APN function.

Let $A=a\in(\mathbb{F}_2^{n-1})^\times$ and $Y=y+e_0$ with $y\in\mathbb{F}_2^{n-1}$, then we must have $X=y+e_0$ or $X=y+a+e_0$. Since $X\notin\mathbb{F}_2^{n-1}$, if we put $X=x+e_0$. we have $g(x+a)+g(x)=g(y+a)+g(y)$ from $F(X+a)+F(X)=F(y+e_0+a)+F(y+e_0)$. Hence g must be an APN function. Thus the condition (1) must be satisfied.

Proof of Proposition 1, $F(x) = f(x)$ and $F(x + e_0) = g(x)$

Proof 2, $F(X + A) + F(X) = F(Y + A) + F(Y)$, $A \neq 0$.

Let $A = a \in (\mathbb{F}_2^{n-1})^\times$, $Y = y \in \mathbb{F}_2^{n-1}$. Since $X = y$ or $X = y + a$, $F(X + a) + F(X) = F(y + a) + F(y)$ does not have a solution $X = x + e_0$ for $x \in \mathbb{F}_2^{n-1}$. Thus $F(x + e_0 + a) + F(x + e_0) \neq F(y + a) + F(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$, therefore we must have $g(x + a) + g(x) \neq f(y + a) + f(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$. Thus the condition (2) must be satisfied.

Let $A = a + e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y \in \mathbb{F}_2^{n-1}$. We have $X = y \in \mathbb{F}_2^{n-1}$ or $X = y + a + e_0$ with $y + a \in \mathbb{F}_2^{n-1}$ from $F(X + a + e_0) + F(X) = F(y + a + e_0) + F(y)$. For $X \in \mathbb{F}_2^{n-1}$, we have $g(X + a) + f(X) = g(y + a) + f(y)$, hence $g(X + a) + f(X) = g(y + a) + f(y)$ must have only one solution $X = y$ for any $y, a \in \mathbb{F}_2^{n-1}$. Hence $\mathbb{F}_2^{n-1} \ni X \mapsto g(X + a) + f(X)$ are one-to-one mappings. Thus the condition (3) must be satisfied.

Proof of Proposition 1, $F(x) = f(x)$ and $F(x+e_0) = g(x)$

(1) f and g are APN functions from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$,

(2) $f(x+a) + f(x) \neq g(y+a) + g(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$ and for any non-zero $a \in \mathbb{F}_2^{n-1}$, and

(3) $G_a : \mathbb{F}_2^{n-1} \ni x \mapsto f(x+a) + g(x) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$.

Proof 3

Conversely, let us assume the conditions (1), (2) and (3). Assume $F(X+A) + F(X) = F(Y+A) + F(Y)$, $A \neq 0$. We will prove $X = Y$ or $X = Y + A$. We divide the case into four cases

(i) $A = a \in (\mathbb{F}_2^{n-1})^\times$ and $Y = y \in \mathbb{F}_2^{n-1}$,

(ii) $A = a \in (\mathbb{F}_2^{n-1})^\times$ and $Y = y + e_0$ with $y \in \mathbb{F}_2^{n-1}$,

(iii) $A = a + e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y$ with $y \in \mathbb{F}_2^{n-1}$, and

(iv) $A = a + e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y + e_0$ with $y \in \mathbb{F}_2^{n-1}$.

Proof of Proposition 1, $F(x) = f(x)$ and $F(x + e_0) = g(x)$

Proof 4, $F(X + A) + F(X) = F(Y + A) + F(Y)$, $A \neq 0$.

(i) $A = a \in (\mathbb{F}_2^{n-1})^\times$ and $Y = y \in \mathbb{F}_2^{n-1}$. If $X = x \in \mathbb{F}_2^{n-1}$, then we have $f(x + a) + f(x) = f(y + a) + f(y)$ hence $X = x = y$ or $X = x = y + a$ by (1). Let $X = x + e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $g(x + a) + g(x) = f(y + a) + f(y)$ which has no solution by (2). Therefore, $X = Y$ or $X = Y + A$.
(ii) $A = a \in (\mathbb{F}_2^{n-1})^\times$ and $Y = y + e_0$ with $y \in \mathbb{F}_2^{n-1}$. Assume $X = x \in \mathbb{F}_2^{n-1}$, then we have $f(x + a) + f(x) = g(y + a) + g(y)$ which has no solution by (2). If $X = x + e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $g(x + a) + g(x) = g(y + a) + g(y)$ hence $X = x + e_0 = y + e_0$ or $X = x + e_0 = y + e_0 + a$ by (1). Thus we have $X = Y$ or $X = Y + A$.

Proof of Proposition 1, $F(x)=f(x)$ and $F(x+e_0)=g(x)$

Proof 5, $F(X+A)+F(X)=F(Y+A)+F(Y)$, $A\neq 0$.

(iii) $A=a+e_0$ with $a\in\mathbb{F}_2^{n-1}$ and $Y=y$ with $y\in\mathbb{F}_2^{n-1}$.
If $X=x\in\mathbb{F}_2^{n-1}$, then we have $g(x+a)+f(x)=g(y+a)+f(y)$. Since $x\mapsto f(x)+g(x+a)$ are one-to-one mappings by (3), we have $X=x=y$. If $X=x+e_0$ with $x\in\mathbb{F}_2^{n-1}$, then we have $f(x+a)+g(x)=g(y+a)+f(y)$. Since $x\mapsto f(x+a)+g(x)$ are one-to-one mappings, we have $X=x+e_0=y+(a+e_0)$. Thus we have $X=Y$ or $X=Y+A$.
(iv) $A=a+e_0$ with $a\in\mathbb{F}_2^{n-1}$ and $Y=y+e_0$ with $y\in\mathbb{F}_2^{n-1}$.
If $X=x\in\mathbb{F}_2^{n-1}$, then we have $g(x+a)+f(x)=f(y+a)+g(y)$. Since $x\mapsto f(x+a)+g(x)$ are one-to-one mappings by (3), we have $X=x=(y+e_0)+(a+e_0)$. If $X=x+e_0$ with $x\in\mathbb{F}_2^{n-1}$, then we have $f(x+a)+g(x)=f(y+a)+g(y)$. Since $x\mapsto f(x+a)+g(x)$ are one-to-one mappings, we have $X=x+e_0=y+e_0$. Thus we also have $X=Y$ or $X=Y+A$.

The case f is a quadratic APN function and $g(x) = f(x) + L'(x)$ with L' a linear mapping

Let f be a function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$ and $B_f(x,a) := f(x+a) + f(x) + f(a) + f(0)$. We consider the case that f is a quadratic APN function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$, and $g(x) = f(x) + L'(x)$ for $x \in \mathbb{F}_2^{n-1}$ with L' an $\mathbb{F}_2$-linear mapping from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$.

The case f is a quadratic APN function and $g(x) = f(x) + L'(x)$ with L' a linear mapping

Let f be a function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$ and $B_f(x,a) := f(x+a) + f(x) + f(a) + f(0)$. We consider the case that f is a quadratic APN function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$, and $g(x) = f(x) + L'(x)$ for $x \in \mathbb{F}_2^{n-1}$ with L' an $\mathbb{F}_2$-linear mapping from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$.

Proposition 2

Let $F(x) := f(x)$ and $F(x+e_0) := f(x) + L'(x)$ for $x \in \mathbb{F}_2^{n-1}$. Then $F:\mathbb{F}_2^n \to \mathbb{F}_2^m$ is a quadratic APN function if and only if $\mathbb{F}_2^{n-1} \ni x \mapsto L'(x) + B_f(x,a) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$.

Proof of Proposition 2

Proof.

Since f and $g = f + L'$ are quadratic APN functions, the condition (1) is satisfied.
The condition (2) implies
$f(x+a) + f(x) \neq f(y+a) + f(y) + L'(a)$ for any $x, y \in \mathbb{F}_2^{n-1}$ if $a \neq 0$, that is, $L'(a) + (f(x+a) + f(x)) + (f(y+a) + f(y)) \neq 0$ for any $x, y \in \mathbb{F}_2^{n-1}$ if $a \neq 0$, which means
$L'(a) + B_f(a, x+y) \neq 0$ for any $x, y \in \mathbb{F}_2^{n-1}$ if $a \neq 0$, $a \in \mathbb{F}_2^{n-1}$.
The condition (3) implies
$G_a : \mathbb{F}_2^{n-1} \ni x \mapsto f(x+a)+g(x) = L'(x)+(f(x+a)+f(x)) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$, that is,
$\mathbb{F}_2^{n-1} \ni x \mapsto L'(x) + B_f(x, a) + f(a) + f(0) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$.
Thus we see that the conditions (1), (2) and (3) in Proposition 1 are satisfied if and only if $\mathbb{F}_2^{n-1} \ni x \mapsto L'(x) + B_f(x, a) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$. $\square$

The case f is a quadratic APN function and $g(x) = f(x) + L'(x)$ with L' a linear mapping

Proposition 2

Let $F(x) := f(x)$ and $F(x + e_0) := f(x) + L'(x)$ for $x \in \mathbb{F}_2^{n-1}$. Then $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a quadratic APN function if and only if $\mathbb{F}_2^{n-1} \ni x \mapsto L'(x) + B_f(x, a) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$.

Similar conditions as in Proposition 2 are obtained in the case $n = m$ and f has an $(n-1, n-1)$-APN subfunction in the papers (personal communication with Christof on 22 August 2023).

[1] Christof Beierle, Gregor Leander and Léo Perrin, Trim and extensions of quadratic APN functions, 2022.

[2] Christof Beierle and Claude Carlet, Gold functions and switched cube functions are not 0-extendable in dimension $n > 5$, 2022.

$F(x) + \mathrm{Tr}(x)L(x)$ for a quadratic APN function F on $\mathbb{F}_{2^n}$

Let $T_0 := \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(x) = 0\}$ and $e_0 \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(e_0) = 1$. Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ and $B_F(x, a) := F(x + a) + F(x) + F(a) + F(0)$ for $x, a \in \mathbb{F}_{2^n}$. Let L be an $\mathbb{F}_2$-linear mapping on $\mathbb{F}_{2^n}$.

$F(x) + \mathrm{Tr}(x)L(x)$ for a quadratic APN function F on $\mathbb{F}_{2^n}$

Let $T_0 := \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(x) = 0\}$ and $e_0 \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(e_0) = 1$. Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ and $B_F(x, a) := F(x + a) + F(x) + F(a) + F(0)$ for $x, a \in \mathbb{F}_{2^n}$. Let L be an $\mathbb{F}_2$-linear mapping on $\mathbb{F}_{2^n}$.

Theorem

$F(x) + \mathrm{Tr}(x)L(x)$ is a quadratic APN function on $\mathbb{F}_{2^n}$ if and only if $L_a : T_0 \ni x \mapsto L(x) + B_F(x, a + e_0) \in \mathbb{F}_{2^n}$ are one-to-one mappings from T_0 to $\mathbb{F}_{2^n}$ for any $a \in T_0$.

Proof of Theorem

Proof.

Let $f := F|_{T_0}$ be the restriction of F to T_0; f is a quadratic APN function from T_0 to $\mathbb{F}_{2^n}$.
Let G be a function on $\mathbb{F}_{2^n}$ defined by $G(x) := f(x)$ for $x \in T_0$, $G(x + e_0) := f(x) + L(x) + B_F(e_0, x) = f(x) + L'(x)$ for $x \in T_0$.
By Proposition 2, G is a quadratic APN function if and only if $T_0 \ni x \mapsto L(x) + B_F(x, e_0) + B_F(x, a) = L'(x) + B_F(x, a) \in \mathbb{F}_{2^n}$ are one-to-one mappings for any $a \in T_0$.
Let $\tilde{F}(x) := F(x) + \mathrm{Tr}(x)L(x)$.
Since $G(x) = F(x) + \mathrm{Tr}(x)(L(x) + L(e_0) + F(e_0) + F(0))$ for $x \in \mathbb{F}_{2^n}$, $\tilde{F}(x) = G(x) + \mathrm{Tr}(x)(L(e_0) + F(e_0) + F(0))$.
Thus $\tilde{F}(x) = F(x) + \mathrm{Tr}(x)L(x)$ is a quadratic APN function on $\mathbb{F}_{2^n}$ if and only if $L_a : T_0 \ni x \mapsto L(x) + B_F(x, a + e_0) \in \mathbb{F}_{2^n}$ are one-to-one mappings from T_0 to $\mathbb{F}_{2^n}$ for any $a \in T_0$. □

Examples

Example 1

Let e_0 be some fixed element of $\mathbb{F}_{2^n}$ with $\mathrm{Tr}(e_0) = 1$. Let $F(x) = x^3$ on $\mathbb{F}_{2^n}$. Let L be a linear mapping which satisfies the conditions of the Theorem for the quadratic APN function $F(x) = x^3$, and $L(e_0) = 0$. Using a computer, we have 448 L's on $\mathbb{F}_{2^4}$, 4608 L's on $\mathbb{F}_{2^5}$, and many (about $40,000$) L's on $\mathbb{F}_{2^6}$.

Examples

Example 2

Let $F(x) = x^3$ on $\mathbb{F}_{2^6}$. The Γ-rank of F is 1102. Using a computer, we see that there are linear mappings L satisfying the conditions of the Theorem such that the Γ-ranks of $\tilde{F}(x) := F(x) + \mathrm{Tr}(x)L(x)$ are 1144, 1146, 1158, 1166, 1168, 1170, 1172 and 1174.

Examples

Example 3

Let $F(x) = x^3$ on $\mathbb{F}_{2^6}$. Let $L(x) = \alpha^{42}x + \alpha^{19}x^2 + \alpha^{51}x^{2^2} + \alpha^{59}x^{2^3} + \alpha^{26}x^{2^4} + \alpha^{38}x^{2^5}$, where α is a primitive element of $\mathbb{F}_{2^6}$. We see that $\tilde{F}(x) = F(x) + \mathrm{Tr}(x)L(x)$ has non-classical Walsh spectrum $\mathcal{W}_F = \{0, \pm 8, \pm 16, \pm 32\}$ with the Γ-rank 1170.
Since $\tilde{F}(x) = F(x) + \mathrm{Tr}(x)L(x)$ with $L(x) = \alpha^{42}x + \alpha^{47}x^2 + \alpha^{35}x^{2^2} + \alpha^{54}x^{2^3} + \alpha^{23}x^{2^4} + \alpha^{27}x^{2^5}$ has classical Walsh spectrum $\mathcal{W}_F = \{0, \pm 8, \pm 16\}$ with the Γ-rank 1170, we see that there are inequivalent APN functions $\tilde{F}(x) = F(x) + \mathrm{Tr}(x)L(x)$ with the same Γ-rank.

Examples

Example 4

Let $F(x) = x^3$ on $\mathbb{F}_{2^7}$. The Γ-rank of F is 3610. Using a computer, we see that the linear mapping $L(x) := x + x^{2^3} + x^{2^5} + x^{2^6}$ satisfies the conditions of the Theorem and the Γ-rank of $\tilde{F}(x) = F(x) + \mathrm{Tr}(x)L(x)$ is 4048.

Examples

Example 4

Let $F(x) = x^3$ on $\mathbb{F}_{2^7}$. The Γ-rank of F is 3610. Using a computer, we see that the linear mapping $L(x) := x + x^{2^3} + x^{2^5} + x^{2^6}$ satisfies the conditions of the Theorem and the Γ-rank of $\tilde{F}(x) = F(x) + \mathrm{Tr}(x)L(x)$ is 4048.

To find the linear mappings L on $\mathbb{F}_{2^n}$ $(n \geq 8)$ for $F(x) = x^3$, we need much time to check the conditions of the Theorem using a computer. So, at present, we want to have some more theoretical results concerning L.

Examples

Example 4

Let $F(x) = x^3$ on $\mathbb{F}_{2^7}$. The Γ-rank of F is 3610. Using a computer, we see that the linear mapping $L(x) := x + x^{2^3} + x^{2^5} + x^{2^6}$ satisfies the conditions of the Theorem and the Γ-rank of $\tilde{F}(x) = F(x) + \mathrm{Tr}(x)L(x)$ is 4048.

To find the linear mappings L on $\mathbb{F}_{2^n}$ $(n \geq 8)$ for $F(x) = x^3$, we need much time to check the conditions of the Theorem using a computer. So, at present, we want to have some more theoretical results concerning L.

The papers (personal communication with Christof on August '23) will be helpful for more investigations on this subject.

Thank you for your cooperation!