More Constructions of Differentially 4-Uniform Permutations on $\mathbb{F}_{2^{2k}}$

Yin Tan

Department of Electrical and Computer Engineering
University of Waterloo, ON, Canada

yin.tan@uwaterloo.ca

(Joint work with L. Qu, C. Li and G. Gong)

September 3, 2014
Motivation and Definitions

1. Motivations
2. Definitions

Construction of differentially 4-uniform permutations

2. Power functions
3. Construction from the switching method

Number of CCZ-inequivalent PPs via the switching method

Non-decomposable preferred Boolean functions
Requirements for a substitution box

Assuming $F$ is the Substitution box chosen by a block cipher with SPN structure. To avoid various attacks, $F$ should satisfy the following conditions:

- Low differential uniformity (to avoid differential attack);
- High nonlinearity (to avoid linear attack);
- High algebraic degree (to avoid higher order differential attack);
- Defined on $\mathbb{F}_{2^k}$ (for software implementation);
- Others.
Differential uniformity

Let $F$ be a function over $\mathbb{F}_{2^n}$. We have the following two different common methods to characterize its nonlinearity.

For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, define

$$\delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\}|,$$

and

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta_F(a, b).$$

To prevent the differential attack, we want the value $\Delta_F$ to be as small as possible.

---

1PN functions do not exist in the field with even characteristic.
Differential uniformity

Let $F$ be a function over $\mathbb{F}_{2^n}$. We have the following two different common methods to characterize its nonlinearity. For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, define

$$\delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\}|,$$
and

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta_F(a, b).$$

To prevent the differential attack, we want the value $\Delta_F$ to be as small as possible.

- If $\Delta_F = 1$, $F$ is called perfect nonlinear function (PN); \(^1\)

---

\(^1\)PN functions do not exist in the field with even characteristic.
Differential uniformity

Let $F$ be a function over $\mathbb{F}_{2^n}$. We have the following two different common methods to characterize its nonlinearity.

For any $a \in \mathbb{F}^{*}_{2^n}$ and $b \in \mathbb{F}_{2^n}$, define

$$
\delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\}|, \text{ and } \\
\Delta_F = \max_{a \in \mathbb{F}^{*}_{2^n}, b \in \mathbb{F}_{2^n}} \delta_F(a, b).
$$

To prevent the differential attack, we want the value $\Delta_F$ to be as small as possible.

- If $\Delta_F = 1$, $F$ is called perfect nonlinear function (PN); \(^1\)
- If $\Delta_F = 2$, $F$ is called almost perfect nonlinear function (APN);

\(^1\)PN functions do not exist in the field with even characteristic.
Differential uniformity

Let $F$ be a function over $\mathbb{F}_{2^n}$. We have the following two different common methods to characterize its nonlinearity.

For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, define

$$
\delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\}|, \quad \text{and}
$$

$$
\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta_F(a, b).
$$

To prevent the differential attack, we want the value $\Delta_F$ to be as small as possible.

- If $\Delta_F = 1$, $F$ is called \textit{perfect nonlinear function} (PN);\(^1\)
- If $\Delta_F = 2$, $F$ is called \textit{almost perfect nonlinear function} (APN);
- If $\Delta_F = 4$, $F$ is called \textit{differentially 4-uniform function}.

\(^1\)PN functions do not exist in the field with even characteristic.
Motivation and Definitions

Construction of differentially 4-uniform permutations
Number of CCZ-inequivalent PPs via the switching method
Non-decomposable preferred Boolean functions

Nonlinearity

(2) For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, define

$$
\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(aF(x) + bx)},
$$

$$
\mathcal{W}_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} |\mathcal{W}_F(a, b)|,
$$

$$
\text{NL}_F = 2^{n-1} - \frac{1}{2} \mathcal{W}_F.
$$

To be resistant to the linear attack, we want the value $\text{NL}_F$ to be as large as possible.
(2) For any \( a \in \mathbb{F}_{2^n}^* \) and \( b \in \mathbb{F}_{2^n} \), define

\[
\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(aF(x)+bx)},
\]

\[
\mathcal{W}_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} |\mathcal{W}_F(a, b)|,
\]

\[
\text{NL}_F = 2^{n-1} - \frac{1}{2} \mathcal{W}_F.
\]

To be resistant to the linear attack, we want the value \( \text{NL}_F \) to be as large as possible.

- When \( n \) is even, \( \mathcal{W}_F \leq 2^{n/2+1} \);
(2) For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, define

$$
\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(aF(x) + bx)},
$$

$$
\mathcal{W}_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} |\mathcal{W}_F(a, b)|,
$$

$$
\text{NL}_F = 2^{n-1} - \frac{1}{2} \mathcal{W}_F.
$$

To be resistant to the linear attack, we want the value $\text{NL}_F$ to be as large as possible.

- When $n$ is even, $\mathcal{W}_F \leq 2^{n/2+1}$;
- When $n$ is odd, it is conjectured that $\mathcal{W}_F \leq 2^{(n+1)/2}$;
- The function $F$ is called \textit{maximal nonlinear} if $\mathcal{W}_F = 2^{n/2+1}$ when $n$ is even, or $\mathcal{W}_F = 2^{(n+1)/2}$ when $n$ is odd.
(1) The differential uniformity and nonlinearity of a function $F$ is preserved by EA-equivalence and CCZ-equivalence;
(2) CCZ-equivalence implies EA-equivalence, but not vice versa;
(3) Therefore, obtaining an ideal Sbox can lead to a large class of ideal Sboxes.
(4) However, given two functions $F$ and $G$, it is difficult to tell whether they are CCZ-equivalent (if differential and linear spectrum are the same).
EA-equivalence and CCZ-equivalence

**Definition 1**

Two functions $F, G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ are called *extended affine equivalent* (EA) if there exist two affine permutations $A_1, A_2$ of $\mathbb{F}_2^n$ and an affine function $A : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ such that

$$G = A_1 \circ F \circ A_2 + A,$$

where $\circ$ denotes the composition of two functions.

For a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, we denote by $\mathcal{G}_F$ the graph of the function of $F$

$$\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\} \subset \mathbb{F}_2^{2n}.$$

We say two functions $F, G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ *CCZ-equivalence* if there exists an affine permutation $A : \mathbb{F}_2^{2n} \rightarrow \mathbb{F}_2^{2n}$ such that $A(\mathcal{G}_F) = \mathcal{G}_G$. 
It is natural to search for ideal Sboxes from power functions.

**Table** : Known differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ with **maximal nonlinearity**

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

It is conjectured the above table is complete, i.e. all power permutations with maximal nonlinearity are one of the four families.
Binomial function

**Theorem 2 (Bracken, T. and Tan, 2012)**

Let $n = 3k$ and $k$ is an even integer with $3 
\not| \ k$, $k/2$ is odd. Let $s$ be an integer with $\gcd(3k, s) = 2$ and $3 \mid k + s$. Define the function

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

$$F(x) = \alpha x^{2^s+1} + \alpha^{2^k} x^{2^{k-s}+2^{k+s}},$$

where $\alpha$ is a primitive element of $\mathbb{F}_{2^n}$. Then $F$ is a differentially 4-uniform permutation with maximal nonlinearity.

Note that when $\gcd(3k, s) = 1$, the function $F$ is APN which is discovered by Budaghyan, Carlet and Leander.
Switching method

If we do not require maximal nonlinearity but "good" nonlinearity, much more infinite classes of differentially 4-uniform permutations can be obtained. A powerful tool is the so-called switching method, i.e. adding a Boolean function to $F$.

Switching method has been previously applied on:

1. APN functions: a well-known example $x^3 + \text{Tr}(x^9)$ (B-C-L); Many new APN examples from switching method in E-P’s paper;

2. planar function: certain CCZ-inequivalent PN functions are switching neighbors, in P-Z’s paper.

3. permutation polynomial: many PPs with the form $F(x) + \gamma \text{Tr}(H(x))$ are obtained in C-K’s papers.
Switching method

If we do not require maximal nonlinearity but "good" nonlinearity, much more infinite classes of differentially 4-uniform permutations can be obtained. A powerful tool is the so-called *switching method*, i.e. adding a Boolean function to $F$.

Switching method has been previously applied on:

(1). APN functions: a well-known example $x^3 + \text{Tr}(x^9)$ (B-C-L); Many new APN examples from switching method in E-P’s paper;

(2). planar function: certain CCZ-inequivalent PN functions are switching neighbors, in P-Z’s paper.

(3). permutation polynomial: many PPs with the form $F(x) + \gamma \text{Tr}(H(x))$ are obtained in C-K’s papers.

In the following we apply the switching method on constructing differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$. 
Preferred functions

Let \( n = 2k \) be an even integer and \( R \) be an \((n, n)\)-function. Define the Boolean function \( D_R \) by \( D_R(x) = \text{Tr}(R(x + 1) + R(x)) \), and the functions \( Q_R, P_R \) as

\[
Q_R(x, y) = D_R\left(\frac{1}{x}\right) + D_R\left(\frac{1}{x} + y\right), \quad P_R(y) = Q_R(0, y) = D_R(0) + D_R(y).
\]

Let \( U \) be the subset of \( \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \) defined by

\[
U = \{(x, y)|x^2 + \frac{1}{y}x + \frac{1}{y(y+1)} = 0, \; y \not\in \mathbb{F}_2\}.
\]

If

\[
Q_R(x, y) + P_R(y) = 0
\]

satisfies for any elements in \((x, y) \in U\), then we call \( R \) a preferred function (PF), or said to be preferred.
Properties of PFs

Proposition 1

Let $S$ be a set of PFs defined on $\mathbb{F}_{2^n}$. Then the set $S$ defined by

$$S = \left\{ \sum_{f \in S} a_f f : a_f \in \mathbb{F}_2 \right\}$$

is a subspace of $(\mathcal{V}F^n, +)$. 
Proposition 1

Let $S$ be a set of PFs defined on $\mathbb{F}_{2^n}$. Then the set $S$ defined by

$$S = \left\{ \sum_{f \in S} a_f f : a_f \in \mathbb{F}_2 \right\}$$

is a subspace of $(\mathbb{V}\mathbb{F}^n, +)$.

If we can find $t$ PFs, we then obtain $2^t$ PFs.
Why we consider preferred functions?

**Theorem 3**

Let $n = 2k$ be an even integer, $l(x) = x^{-1}$ be the inverse function and $R$ be an $(n, n)$-function. Define

$$H(x) = x + \text{Tr}(R(x) + R(x + 1)),$$
$$G(x) = H(l(x)).$$

Then if $R(x)$ is a preferred function,

1. $G(x)$ is a differentially 4-uniform permutation polynomial;
2. The algebraic degree of $G$ is $n - 1$;
3. The nonlinearity of $F$

$$NL_F \geq 2^{n-2} - \frac{1}{4} \lfloor 2^{\frac{n}{2} + 1} \rfloor - 1.$$
### Examples of preferred functions

**Example 4**

Let \( R(x) = x^d : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k} \) and \( F(x) = x + \text{Tr}(R(x + 1) + R(x)) \), where

1. \( n = 2k = 4m, \ d = 2^{2m} + 2^m + 1 \),
2. \( d = 2^t + 1 \), where \( 1 \leq t \leq k - 1 \),
3. \( d = 3(2^t + 1) \), where \( 2 \leq t \leq k - 1 \).
Examples of preferred functions

**Example 4**

Let \( R(x) = x^d : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k} \) and \( F(x) = x + \text{Tr}(R(x + 1) + R(x)) \), where

\begin{align*}
(1) \quad & n = 2k = 4m, \quad d = 2^{2m} + 2^m + 1, \\
(2) \quad & d = 2^t + 1, \quad \text{where } 1 \leq t \leq k - 1, \\
(3) \quad & d = 3(2^t + 1), \quad \text{where } 2 \leq t \leq k - 1.
\end{align*}

Therefore, the function \( F(x^{-1}) \) is differentially 4-uniform permutations. Many PFs can be found in [Qu, T., Tan, Li, IEEE IT (2013)].
Since we obtain a lot of new differentially 4-uniform permutations, it is interesting to consider

**Problem 5**

Let $n = 2k$ and $\mathcal{PF}$ be the set of all PFs on $\mathbb{F}_{2^n}$. Define

$$S_n = \{ H(x^{-1}) \mid H(x) = x + \text{Tr}(R(x + 1) + R(x)), \ R \in \mathcal{PF} \}.$$

How many CCZ-inequivalent classes of differentially 4-uniform permutations among $S_n$?
Preferred Boolean functions

Definition 6

Let $n = 2k$ be an even integer and $f$ be an $n$-variable Boolean function. We call $f$ a preferred Boolean function (PBF for short) if it satisfies the following two conditions:

(i) $f(x + 1) = f(x)$ for any $x \in \mathbb{F}_{2^n}$;

(ii) $f\left(\frac{1}{x}\right) + f\left(\frac{1}{x} + y\right) + f(0) + f(y) = 0$ for any pair $(x, y) \in U$, where $U$ is the same set when define PFs.
Properties of preferred Boolean functions

Proposition 2

$R : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is a PF if and only if $D_R(x) = \text{Tr}(R(x) + R(x + 1))$ is a PBF. Furthermore, for any PBF $f$ with $n$ variables, there are $2^n \cdot 2^n - 2^n - 1$ preferred functions $R$ such that $D_R(x) = f(x)$. 

Properties of preferred Boolean functions

**Proposition 2**

\[ R : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} \text{ is a PF if and only if } D_R(x) = \text{Tr}(R(x) + R(x + 1)) \text{ is a PBF. Furthermore, for any PBF } f \text{ with } n \text{ variables, there are } 2^n \cdot 2^n - 2^n - 1 \text{ preferred functions } R \text{ such that } D_R(x) = f(x). \]

**Proposition 3**

Let \( \omega \) be an element of \( \mathbb{F}_{2^n} \) with order 3. Then \( f \) is a PBF if and only if it satisfies the following two conditions:

(i) \( f(x + 1) = f(x) \) for any \( x \in \mathbb{F}_{2^n} \);

(ii) \( f(\alpha + \frac{1}{\alpha}) + f(\omega \alpha + \frac{1}{\omega \alpha}) + f(\omega^2 \alpha + \frac{1}{\omega^2 \alpha}) = 0 \) for any \( \alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4 \).
Determine all preferred Boolean functions

Define the following two sets:

\[ L_1 = \left\{ \{x, x + 1\} : x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \right\}, \]

\[ L_2 = \left\{ \left\{ \alpha + \frac{1}{\alpha}, \omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha} \right\} : \alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4 \right\}. \]

Let \( v_x \) and \( v_\alpha \) be the characteristic function in \( \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \) of each \( \{x, x + 1\} \in L_1 \) and \( \left\{ \alpha + \frac{1}{\alpha}, \omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha} \right\} \in L_2 \), respectively.

Define the \((|L_1| + |L_2|) \times (2^n - 2)\) matrix \( M \) by

\[
M = \begin{bmatrix}
v_x \\
v_\alpha
\end{bmatrix}, \tag{1}
\]

where the columns and rows of \( M \) are indexed by the elements in \( \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \) and \( L_1 \cup L_2 \) respectively. Then the dimension of \( \mathcal{PBF} \) is \( 2^n - 1 - \text{rank}(M) \), and the dimension of \( \mathcal{PF} \) is \( n \cdot 2^n + 2^{n-1} - 1 - \text{rank}(M) \).
Determine all preferred Boolean functions

Problem 7

Is the rank of the matrix $M$ above $\frac{2^{n+1} - 5}{3}$? We have verified this true for $n = 6, 8, 10, 12, 14$. 
Determine all preferred Boolean functions

Problem 7

Is the rank of the matrix $M$ above $\frac{2^{n+1} - 5}{3}$? We have verified this true for $n = 6, 8, 10, 12, 14$.

Lemma 8

We have

1. \( \text{rank}(M) \leq \min\{|L_1| + |L_2|, 2^n - 2\} = \min\{\frac{2^{n+1} - 5}{3}, 2^n - 2\} = \frac{2^{n+1} - 5}{3}. \)

2. For each \((n,n)\)-function $F$, there are at most \((2^n)^{4n+2} = 2^{4n^2 + 2n}\) functions which are CCZ-equivalent to it.
Lower bound on the CCZ-inequivalent number of PPs

**Theorem 9**

There are at least \(2^{\frac{2^n+2}{3}-4n^2-2n}\) CCZ-inequivalent differentially 4-uniform permutations over \(\mathbb{F}_{2^n}\) among all the functions constructed by Theorem 3.
Motivation and Definitions
Construction of differentially 4-uniform permutations
Number of CCZ-inequivalent PPs via the switching method
Non-decomposable preferred Boolean functions

Lower bound on the CCZ-inequivalent number of PPs

Theorem 9

There are at least $2^{2^n+2/3} - 4n^2 - 2^n$ CCZ-inequivalent differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ among all the functions constructed by Theorem 3.

Remarks:

(1.) The number of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ with highest algebraic degree and nonlinearity greater than the one in Theorem 3 grows exponentially when $n$ increase;

(2.) A similar question is raised by Edel and Pott on the number of CCZ-inequivalent APN functions, which is still open now.
### Some statistics

**Table**: Nonlinearity of the differentially 4-uniform permutations constructed by Theorem 3 on $\mathbb{F}_{2^n}$ when $6 \leq n \leq 10$ ($n$ even)

| $n$ | Sample size | Ave(NL) | Var(NL) | Dist(NL) | Bound in Theorem 3 | KMNL |
|-----|--------------|---------|---------|----------|---------------------|------|
| 6   | 10,000       | 18.4022 | 1.2034  | 14, 16, 18, 20 | 14                 | 24   |
| 8   | 10,000       | 94.2740 | 2.2576  | 82, 84, 86, 88, 90, 92, 94, 96 | 55    | 112  |
| 10  | 5,000        | 434.2524| 3.7225  | 418, 420, 422, 424, 426, 428, 432, 434, 436, 438 | 239   | 480  |
Motivation and Definitions

Construction of differentially 4-uniform permutations
Number of CCZ-inequivalent PPs via the switching method
Non-decomposable preferred Boolean functions

What about the case $n$ odd?

Does the number of differentially 4-uniform permutations grows exponentially when $n$ increases?

Yes. Consider $G(x) = x - 1 + f(x)$, where $f$ is Boolean. It is shown in \cite{T, Qu, Tan, Li, SETA12} that there are $2^{2n-1}f$ such that $G$ is PP. So there are at least $2^{2n-1} - 4n^2 - 2n$ CCZ-inequivalent permutations over $\mathbb{F}_{2^n}$ ($n$ odd) with differential uniformity at most 4.
Does the number of differentially 4-uniform permutations grows exponentially when \( n \) increases?

Yes. Consider \( G(x) = x^{-1} + f(x) \), where \( f \) is Boolean. It is shown in [T, Qu, Tan, Li, SETA12] that there are \( 2^{2n-1} \) \( f \) such that \( G \) is PP. So there are at least

\[
\frac{2^{2n-1}}{2^{4n^2+2n}} = 2^{2n-1-4n^2-2n}
\]

CCZ-inequivalent permutations over \( \mathbb{F}_{2^n} \) (\( n \) odd) with differential uniformity at most 4.
Motivation and Definitions

Construction of differentially 4-uniform permutations

Number of CCZ-inequivalent PPs via the switching method

Non-decomposable preferred Boolean functions

**Triple set**

- For any $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$, we call the set
  \[ A_\alpha = \{ \alpha + \frac{1}{\alpha}, \omega \alpha + \frac{1}{\omega \alpha}, \omega^2 \alpha + \frac{1}{\omega^2 \alpha} \} \]
  a *triple set* with respect to $\alpha$ (or TS for short).

- Let $A_1$ and $A_2$ be two triple sets. They are called *adjacent* if there exist $a \in A_1$ and $b \in A_2$ such that $a + b = 1$. To be more clear, we call $A_2$ is adjacent to $A_1$ at $a$, and call $A_1$ is adjacent to $A_2$ at $b$.

- For any triple set $A_\alpha$, it has either three or exactly one neighbors. If it has one neighbor, we call it *slim*, otherwise call it *fat*. 
Non-decomposable PBFs

**Definition 10**
Let $f$ be a nonzero PBF. If there exist two PBFs $f_1$ and $f_2$ such that $f = f_1 + f_2$ and $\text{supp}(f_i) \subset \text{supp}(f)$, $1 \leq i \leq 2$, then $f$ is called **decomposable**. Otherwise it is called **non-decomposable**.

**Definition 11**
We define the following sets for later usage:

\[
T_1 = \{ x \in \mathbb{F}_{2^n} | \text{Tr} \left( \frac{1}{x} \right) = \text{Tr} \left( \frac{1}{x + 1} \right) = 1 \},
\]
\[
T_2 = \{ x \in \mathbb{F}_{2^n} | \text{Tr} \left( \frac{1}{x} \right) + \text{Tr} \left( \frac{1}{x + 1} \right) = 1 \},
\]
\[
T_3 = \{ x \in \mathbb{F}_{2^n} | \text{Tr} \left( \frac{1}{x} \right) = \text{Tr} \left( \frac{1}{x + 1} \right) = 0 \}.
\]
Theorem 12

Let $f$ be a Boolean function with $n$ variables. Assume that $|\text{supp}(f)| = 2t$ and there are $r$ ($0 \leq r \leq t$) TSs $A_i = \{a_i, b_i, a_i + b_i\}$ such that $\text{supp}(f) \cap A_i = \{a_i, b_i\}$. Then the following results hold:

(i) If $t = 1$, then $f$ is a non-decomposable PBF if and only if $r = 0$ and there exists $\beta \in T_1$ such that $\text{supp}(f) = \{\beta, 1 + \beta\}$;

(ii) If $t = 2$, then $f$ is a non-decomposable PBF if and only if $r = 1$ and there exists a slim TS $A = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$ such that $\text{supp}(f) = \{\beta_1, \beta_2, 1 + \beta_1, 1 + \beta_2\}$, where $\beta_1, \beta_2 \in T_2$;
Characterization of non-decomposable PBFs

(cont.)

(iii) If $t \geq 3$, then either $r = t$ or $r = t - 1$. Furthermore,

(a) If $r = t$, then $f$ is a non-decomposable PBF if and only if there exist fat TSs $A_1 = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$,

$A_i = \{1 + \beta_{i-1}, \beta_{i+1}, 1 + \beta_{i-1} + \beta_{i+1}\}$, $2 \leq i \leq t - 1$, and

$A_t = \{1 + \beta_{t-1}, 1 + \beta_t, \beta_{t-1} + \beta_t\}$ such that $A_1, \cdots, A_{t-1}$ and $A_t$ form a circle of TSs, and $\text{supp}(f) = \{\beta_i, 1 + \beta_i | 1 \leq i \leq t\}$.

(b) If $r = t - 1$, then $f$ is a non-decomposable PBF if and only if there exist TSs $A_1 = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$, $A_2 = \{1 + \beta_1, \beta_3, 1 + \beta_1 + \beta_3\}$, and $A_i = \{1 + \beta_i, \beta_{i+1}, 1 + \beta_i + \beta_{i+1}\}$, $3 \leq i \leq r$ such that $A_1, A_r$ are slim TSs and $A_2, \cdots, A_{r-1}$ are fat TSs, and $\text{supp}(f) = \{\beta_i, 1 + \beta_i | 1 \leq i \leq t\}$. 
Thanks for the Attention!

Question?