Constructing Infinite Families of Low Differential Uniformity (n, m)-Functions with $m > n/2$

Claude Carlet, Xi Chen* and Longjiang Qu

Abstract

Little theoretical work has been done on (n, m)-functions when $\frac{n}{2} < m < n$, even though these functions can be used in Feistel ciphers, and actually play an important role in several block ciphers. Nyberg has shown that the differential uniformity of such functions is bounded below by $2^{n-m} + 2$ if n is odd or if $m > \frac{n}{2}$. In this paper, we first characterize the differential uniformity of those (n, m)-functions of the form $F(x, z) = \phi(z)I(x)$, where $I(x)$ is the (m, m)-Inverse function and $\phi(z)$ is an $(n - m, m)$-function. Using this characterization, we construct an infinite family of differentially Δ-uniform $(2m-1, m)$-functions with $m \geq 3$ achieving Nyberg's bound with equality, which also have high nonlinearity and not too low algebraic degree. We then discuss an infinite family of differentially 4-uniform $(m+1, m)$-functions in this form, which leads to many differentially 4-uniform permutations. We also present a method to construct infinite families of $(m+k, m)$-functions with low differential uniformity and construct an infinite family of $(2m-2, m)$-functions with $\Delta \leq 2^{m-1} - 2^{m-6} + 2$ for any $m \geq 8$. The constructed functions in this paper may provide more choices for the design of Feistel ciphers.

Keywords APN function, Differential Uniformity, Nyberg's bound, Substitution boxes, Semi-bent function.
Mathematics Subject Classification (2010) 06E30, 11T60, 94A60.

I. Introduction

In the design of many block ciphers, substitution boxes (S-boxes) play an important role because they provide nonlinear relationship between the input bits and the output bits in a controllable fashion. These S-boxes are functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, and are called (n, m)-functions. They are often the only nonlinear parts of block ciphers [14] and used by a variety of modern block ciphers such as AES [12], [20], Serpent [2], [3], PRESENT [5], MISTY [16], its variant KASUMI [13], DES [19], CAST [1], KN [21], and many others. Some of these S-boxes are bijective with $n = m$ and can then be used in the Substitution-Permutation-Network (SPN) structure. However, some of these S-boxes are defined with $m < n$ or even $m > n$ when used in block ciphers of Feistel structure. For example, the DES cipher has 8 S-boxes each mapping 6 bits to 4 bits and the CAST block ciphers have 4 S-boxes each mapping 8 bits to 32 bits. The Feistel model of block cipher gives more flexibility than the SPN model. In particular it does not need the S-boxes to be permutations nor to be balanced, see [23]. One may assume, a priori, that the (n, m)-functions with $m < n$ cannot achieve the same cryptographic properties as (n, n)-functions. But in practice, the S-box of the AES

*Corresponding author: Xi Chen.
Claude Carlet is with LAGA, UMR 7539, CNRS, Department of Mathematics, University of Paris 8 and Paris 13, 93526 Saint-Denis, France. E-mail: claude.carlet@univ-paris8.fr. Xi Chen and Longjiang Qu are with the College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, China. E-mail: 1138470214@qq.com, ljqu_happy@hotmail.com. Part of this work was done when Xi Chen was a joint Ph.D. student in University of Paris 8.

This work is supported by the National Science and Technology Major Project under Grant 2017YFB0802001 and the Nature Science Foundation of China (NSFC) under Grants 61722213, 11531002, 61572026.

is the concatenation of sixteen differentially 4-uniform functions and the differential uniformity of the whole S-box is then 2^{121} (recall that the AES has been obliged to use a non-APN function as substitution box because all known APN functions in even numbers of variables larger than 6 are non-bijective). A comparison with a model involving a Feistel structure is not always at the advantage of the SPN model. Moreover, the Feistel structure has the advantage that encryption and decryption operations are very similar. Thus there is much work nowadays on new models combining the Feistel model and studying (n, m)-functions with $m < n$ is then definitely necessary [24]. Since we mainly focus on the case $m < n$ here, we always let $n = m + k$ with $k \geq 1$ throughout this paper.

When used in Feistel ciphers, the functions do not need mandatorily to be balanced. But using a non-balanced function as S-box obliges to complexity the structure of the cipher (see e.g. [21]). Other criteria also exist, like the transparency order, which are still less mandatory. It has been observed that addressing the transparency order makes the search of functions more difficult and may result in less good functions, while it is possible to add counter-measures after choosing the S-box. To prevent various attacks on the cipher, such functions are required to have low differential uniformity, high nonlinearity and not too low algebraic degree. It is well known that the lowest differential uniformity that an $(m + k, m)$-function can achieve is 2^k; those $(m+k, m)$-functions which achieve such nonlinearity are called perfect nonlinear (PN). According to Nyberg's results [18], PN $(m + k, m)$-functions are also bent, and such bent functions do not exist when $m > k \geq 1$. Then the value of the differential uniformity of $(m+k, m)$-function with $m > k \geq 1$ is bounded below by $2^k + 2$, we call it Nyberg's bound in this paper.

An $(m + k, m + k)$-function is called almost perfect nonlinear (APN) if its differential uniformity equals 2, which is the lowest possible value. Differentially 2^{k+1}-uniform $(m + k, m)$-functions are easily found by composing on the left any APN $(m + k, m + k)$-function by a surjective affine $(m + k, m)$-function. When $k = 1$, these functions achieving Nyberg's bound which is 4. As mentioned in [7], no function achieving Nyberg's bound with $m > k \geq 2$ is known except sporadic examples found by Carlet and AlSalami for $m = 3, k = 2$ [6]. The existence of such functions when $m \geq 4, k \geq 2$ is still an open problem. More generally, the existence of differentially Δ-uniform $(m + k, m)$-functions with $m > k \geq 2, m \neq 3$ and $\Delta < 2^{k+1}$ is an open question. In this paper, we will study this open problem when $k = m - 1$ and $k = m - 2$.

Maiorana-McFarland class, of those functions of the form $F(x, z) = \phi(z)G(x)$ with ϕ linear or affine, seems more or less the first framework to be tried. We have made long mathematical and computer investigation on it, without success except when using the multiplicative inverse function as function G. This function behaves nicely because, after the reduction to a common denominator in the equations, its behavior in the numerators is not so far from that of a linear function, while it avoids the trivial solutions. Contrary to the case of (n, n)-functions where Gold functions are the simplest to be handled, the inverse function behaves function G more nicely than Gold functions (even than x^3).

The rest of this paper is organized as follows. In Section II, we recall some necessary definitions and useful lemmas. We characterize in Section III the differential uniformity of $(m+k, m)$-functions of the form $F(x, z) = \phi(z)I(x)$, where $I(x)$ is the (m, m)-Inverse function and $\phi(z)$ is a (k, m)-function. In Section IV, infinite families of low differential uniformity $(m + k, m)$-functions are investigated with $k = m - 1$, $k = 1$ and $1 \leq k \leq m - 2$ thanks to this characterization. More precisely, an infinite family of differentially Δ-uniform $(2m-1, m)$-functions with $m \geq 3$ achieving Nyberg's bound with equality is constructed in Section IV-A. In Section IV-B, we discuss an infinite family of differentially 4-uniform $(m+1, m)$-functions which leads to many differentially 4-uniform permutations. In Section IV-C, we present a method to construct infinite families of $(m + k, m)$-functions with low differential uniformity by modifying the constructed $(2m-1, m)$-function and we construct an infinite family of $(2m-2, m)$-functions with $\Delta \leq 2^{m-1}-2^{m-6}+2$ for any $m \geq 8$. In Section V, we discuss the possibility of constructing functions achieving Nyberg's bound

from Maiorana-McFarland bent functions or almost bent functions. The constructed functions in this paper may provide more choices for the design of Feistel ciphers.

II. Preliminaries

In this section, we give the definitions and lemmas which will be used in the paper.

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. It is a vector space of dimension n over $\mathbb{F}_2$, and can then be identified with $\mathbb{F}_2^n$. More precisely, assume $\Gamma(x) \in \mathbb{F}_2[x]$ is an irreducible monic polynomial with degree n and α is a root of Γ in its splitting field, then

$$\mathbb{F}_{2^n} = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \big| a_0, a_1, \cdots, a_{n-1} \in \mathbb{F}_2\}.$$

For any $a = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in \mathbb{F}_{2^n}$, the mapping $a \mapsto \vec{a} := (a_0, a_1, \cdots, a_{n-1})^{\mathrm{T}}$ is an isomorphism from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^n$. In the following, we will switch between these two points of view without explanation if the context is clear. Define the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by $\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Denote by $\mathbb{F}_{2^n}^*$ (resp. $\mathbb{F}_2^{n*}$) the set of all nonzero elements of $\mathbb{F}_{2^n}$ (resp. $\mathbb{F}_2^n$). Throughout this paper, for the multiplicative inverse function $I(x) = \frac{1}{x}$, we always define $I(0) = 0$.

Let $\mathbb{M}$ be a vector space over $\mathbb{F}_2$ and let $\mathbb{M}^\perp$ be its dual space, i.e.,

$$\mathbb{M}^\perp = \{\beta \in \mathbb{F}_{2^n} | \mathrm{Tr}_n(\gamma\beta) = 0 \ for\ all\ \gamma \in \mathbb{M}\}.$$

Let S be a subset of $\mathbb{M}$, the span of S is defined as the set of all linear combinations of elements of S, that is,

$$\mathrm{Span}(S) = \{\sum_{i=1}^{k} \lambda_i v_i | k \in \mathbb{N}, v_i \in S, \lambda_i \in \mathbb{F}_2\}.$$

Given two positive integers n and m, a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an (n, m)-*function*. Particularly, when $m = 1$, F is a *Boolean function* over $\mathbb{F}_2^n$ and is called an n-variable Boolean function.

There exist several types of unique representations for (n, m)-functions [9]. One such representation is the *algebraic normal form* (ANF):

$$F(x) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right), \text{ where } a_I \in \mathbb{F}_2^m, \tag{1}$$

The *algebraic degree* of the function is by definition the global degree of its ANF:

$$d^\circ(F) = \max\{\#|I|, \text{ where } a_I \neq 0\}.$$

Let F be a function from $\mathbb{F}_2^{m+k}$ to $\mathbb{F}_2^m$. For any $\bar{a} \in \mathbb{F}_2^{m+k*}, b \in \mathbb{F}_2^m$, let $\bar{a} = (a, d)$, where $a \in \mathbb{F}_2^m, d \in \mathbb{F}_2^k$, we define the *differential value* of F at $(\bar{a}, b)$ as:

$$\begin{aligned} \delta_F(\bar{a}, b) &= \#\{(x, z) \in \mathbb{F}_2^{m+k} | F(x, z) + F(x + a, z + d) = b\} \\ &= \sum_{z \in \mathbb{F}_2^k} \#\{x \in \mathbb{F}_2^m | F(x, z) + F(x + a, z + d) = b\}. \end{aligned}$$

Here we use $\#S$ to denote the number of the elements in a set S.

The multiset $\{* \ \delta_F(\bar{a}, b) | \bar{a} \in \mathbb{F}_2^{m+k*}, b \in \mathbb{F}_2^m \ *\}$ is called the *differential spectrum* of F. The value

$$\Delta_F = \max_{\bar{a} \in \mathbb{F}_2^{m+k*}, b \in \mathbb{F}_2^m} \delta_F(\bar{a}, b)$$

is called the *differential uniformity* of F, and we call F a *differentially Δ_F-uniform* function.

Let F be a function from $\mathbb{F}_2^{m+k}$ to $\mathbb{F}_2^m$. It is clear that for any $\bar{a} = (a, d) \in \mathbb{F}_2^{m+k*}$,

$$\sum_{b \in \mathbb{F}_2^m} \#\{(x, z) \in \mathbb{F}_2^{m+k} | F(x, z) + F(x + a, z + d) = b\} = 2^{m+k}.$$

Then

$$2^m \max_{b \in \mathbb{F}_2^m} \#\{(x, z) \in \mathbb{F}_2^{m+k} | F(x, z) + F(x + a, z + d) = b\} \geq 2^{m+k}.$$

For arbitrary $\bar{a}$ we have that $2^k \leq \Delta_F \leq 2^{m+k}$. We call F *perfect nonlinear* (PN) when Δ_F equals 2^k.

When $k = 0$, we call (m, m)-function F an *almost perfect nonlinear* (APN) function if $\Delta_F = 2$. It is easy to see that APN functions achieve the minimal value of differential uniformity for functions defined on fields with an even characteristic.

Assuming that an inner product in $\mathbb{F}_2^{m+k}$ and an inner product in $\mathbb{F}_2^m$ have been chosen and are written with the same symbol "$\cdot$", the *Walsh transform* $F^{\mathcal{W}} : \mathbb{F}_2^{m+k} \times \mathbb{F}_2^{m*} \to \mathbb{C}$ of F is defined by:

$$F^{\mathcal{W}}(u, v) = \sum_{x \in \mathbb{F}_2^{m+k}} (-1)^{v \cdot F(x) + u \cdot x}.$$

The multiset $\mathcal{W}_F = \{* F^{\mathcal{W}}(u, v) | u \in \mathbb{F}_2^{m+k}, v \in \mathbb{F}_2^{m*} *\}$ is called the *Walsh spectrum* of F. The *nonlinearity* of F is defined as

$$NL(F) = 2^{m-1} - \frac{1}{2} \max_{(u,v) \in \mathbb{F}_2^{m+k} \times \mathbb{F}_2^{m*}} |F^{\mathcal{W}}(u, v)|$$

and corresponds to the minimum Hamming distance between the component functions of F (that is, $v \cdot F$ for any $v \in \mathbb{F}_2^{m*}$) and affine Boolean functions over $\mathbb{F}_2^{m+k}$.

An n-variable Boolean function is called *bent* (resp. *semi-bent*) if the value of its Walsh transform only takes values $\pm 2^{\frac{n}{2}}$, with n even (resp. 0, $\pm 2^{\frac{n}{2}+1}$ when n is even, and 0, $\pm 2^{\frac{n+1}{2}}$ when n is odd).

Bent functions achieve the highest nonlinearity when n is even. When n is odd, the best possible nonlinearity is unknown for $n \geq 9$; semi-bent functions achieve good nonlinearity and can be balanced (what cannot be bent functions). For n even, semi-bent functions also achieve good nonlinearity and can be balanced. An $(m + k, m)$-function F is called a *vectorial bent function* (resp. *vectorial semi-bent function*) if all its component functions are bent functions (resp. semi-bent functions). We call F a *balanced vectorial function* if all its component functions are balanced, that is, if it takes the same number of times any value in the output space.

When $k = 0$, we call (m, m)-function F an *almost bent* (AB) function if $NL(F) = 2^{m-1} - 2^{\frac{m-1}{2}}$, which achieves the minimal value of nonlinearity when m is odd. When m is even, the known the minimal value of nonlinearity is $2^{m-1} - 2^{\frac{m}{2}-1}$.

The classical example for a bent function is the *Maiorana-McFarland bent* function [11] from $\mathbb{F}_2^{2m}$ to $\mathbb{F}_2^m$, which is defined by

$$F(x, z) = \pi(x)L(z) + h(x),$$

where $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a bijection, $L : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a linear bijection and h is any function from $\mathbb{F}_2^m$ to $\mathbb{F}_2^m$.

The following results are useful in our further discussion.

Fact 1: [17] Let n, m be integers. Let $\phi(z) : \mathbb{F}_2^n \to \mathbb{F}_{2^m}$ be an affine function. Assume that there exists $z \in \mathbb{F}_2^n$ such that $\mathrm{Tr}_m(\phi(z)) = 1$. Then

$$\#\{z \in \mathbb{F}_2^n | \mathrm{Tr}_m(\phi(z)) = 1\} = 2^{n-1} \text{ or } 2^n.$$

Lemma 2.1: [15] For any $a, b \in \mathbb{F}_{2^m}$ and $a \neq 0$, the polynomial $F(x) = x^2 + ax + b \in \mathbb{F}_{2^m}[x]$ is irreducible if and only if $\mathrm{Tr}_m(\frac{b}{a^2}) = 1$.

Theorem 2.2: [22] Let t_1, t_2 denote the roots of $t^2 + bt + a^3 = 0$, where $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*$. Then the factorization of $f(x) = x^3 + ax + b$ over $\mathbb{F}_{2^n}$ are characterized as follows:
f has three zeros in F_{2^n} if and only if

$$Tr_1^n(\frac{a^3}{b^2} + 1) = 0$$

and t_1, t_2 are cubes in $\mathbb{F}_{2^n}$ (n even), $\mathbb{F}_{2^{2n}}$ (n odd).
f has exactly one zero in $\mathbb{F}_{2^n}$ if and only if

$$Tr_1^n(\frac{a^3}{b^2} + 1) = 1.$$

f f has no zero in $\mathbb{F}_{2^n}$ if and only if

$$Tr_1^n(\frac{a^3}{b^2} + 1) = 0$$

and t_1, t_2 are not cubes in $\mathbb{F}_{2^n}$ (n even), $\mathbb{F}_{2^{2n}}$ (n odd).

III. A CHARACTERIZATION OF THE DIFFERENTIAL UNIFORMITY OF $F(x, z) = \phi(z)I(x)$

In the following proposition, we characterize the differential uniformity of the functions $F : \mathbb{F}_2^{m+k} \to \mathbb{F}_{2^m}$ in the form $F(x, z) = \phi(z)I(x)$.

Proposition 3.1: Let m and k be integers satisfying $1 \leq k \leq m - 1$. Any function $F : \mathbb{F}_2^{m+k} \to \mathbb{F}_{2^m}$ in the form $F(x, z) = \phi(z)I(x)$, where $\phi(z) : \mathbb{F}_2^k \to \mathbb{F}_{2^m}$ and $I(x)$ is the (m, m)-Inverse function, is a differentially Δ-uniform function with $\Delta < 2^{k+1}$ if and only if all of the conditions below hold.
1. $\phi(z) \neq 0$ for any $z \in \mathbb{F}_2^k$.
2. $\phi(z)$ is an injection.
3. For any $d \in \mathbb{F}_2^k$, $t \in \mathbb{F}_{2^m}^*$,

$$\begin{aligned}\Delta \quad \geq \quad & 2^{k+1} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t + \phi(z) + \phi(z + d))^2}\right) = 1\right\} \\ & -\#\{z \in \mathbb{F}_2^k | t = \phi(z) + \phi(z + d)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z + d)\}.\end{aligned}$$

Proof: Necessity: Assume that the differential uniformity of $F(x, z) = \phi(z)I(x)$ is $\Delta < 2^{k+1}$. Then for any $\bar{a} \in \mathbb{F}_2^{m+k*}, b \in \mathbb{F}_{2^m}$ with $\bar{a} = (a, d)$, where $a \in \mathbb{F}_{2^m}, d \in \mathbb{F}_2^k$, we have

$$\sum_{z \in \mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} | \phi(z)I(x) + \phi(z + d)I(x + a) = b\} \leq \Delta. \tag{2}$$

Let us prove that Conditions $1 - 3$ are satisfied.

Let $d = 0, a \in \mathbb{F}_{2^m}^*, b = 0$. Then Eq.(2) is equivalent to

$$\sum_{z \in \mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} | \phi(z)(I(x) + I(x + a)) = 0\} \leq \Delta.$$

Since $\Delta < 2^m$, we have $\phi(z) \neq 0$ for any $z \in \mathbb{F}_2^k$, which means Condition 1 holds.

Let $d \in \mathbb{F}_2^{k*}, a = b = 0$. If there exists $z \in \mathbb{F}_2^k$ such that $\phi(z) = \phi(z + d)$, then

$$\begin{aligned}& \sum_{z \in \mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} | \phi(z)I(x) + \phi(z + d)I(x + a) = b\} \\ = \quad & \sum_{z \in \mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} | (\phi(z) + \phi(z + d))I(x) = 0\} \geq \ 2^m > \Delta.\end{aligned}$$

A contradiction! Thus $\phi(z)$ is an injection, that is, Condition 2 holds.

Let $d \in \mathbb{F}_2^k$ and a, b be arbitrary elements in $\mathbb{F}_{2^m}^*$. Then we have

$$\begin{aligned}
&\sum_{z\in\mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} | \phi(z)I(x) + \phi(z+d)I(x+a) = b\} \\
= &\sum_{z\in\mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} \setminus \{0,a\} | \phi(z)I(x) + \phi(z+d)I(x+a) = b\} \\
&+ \sum_{z\in\mathbb{F}_2^k} \#\{x \in \{0,a\} | \phi(z)I(x) + \phi(z+d)I(x+a) = b\} \\
= &\sum_{z\in\mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} \setminus \{0,a\} | bx^2 + (ab + \phi(z) + \phi(z+d))x + \phi(z)a = 0\} \\
&+\#\{z \in \mathbb{F}_2^k | ab = \phi(z)\} + \#\{z \in \mathbb{F}_2^k | ab = \phi(z+d)\} \\
= &\sum_{z\in\mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} | bx^2 + (ab + \phi(z) + \phi(z+d))x + \phi(z)a = 0\} \\
&+\#\{z \in \mathbb{F}_2^k | ab = \phi(z)\} + \#\{z \in \mathbb{F}_2^k | ab = \phi(z+d)\}.
\end{aligned}$$

The last step holds since neither $x = 0$ nor a is a solution of $bx^2 + (ab + \phi(z) + \phi(z+d))x + \phi(z)a = 0$. Then we get:

$$\begin{aligned}
&\sum_{z\in\mathbb{F}_2^k} \#\{x \in \mathbb{F}_{2^m} | bx^2 + (ab + \phi(z) + \phi(z+d))x + \phi(z)a = 0\} \\
= &\sum_{z\in\mathbb{F}_2^k, ab+\phi(z)+\phi(z+d)\neq 0} \#\{x \in \mathbb{F}_{2^m} | bx^2 + (ab + \phi(z) + \phi(z+d))x + \phi(z)a = 0\} \\
&+ \sum_{z\in\mathbb{F}_2^k, ab+\phi(z)+\phi(z+d)=0} \#\{x \in \mathbb{F}_{2^m} | bx^2 + (ab + \phi(z) + \phi(z+d))x + \phi(z)a = 0\} \\
= &\ 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{\phi(z)ab}{(ab+\phi(z)+\phi(z+d))^2}\right) = 0\right\} + \#\{z \in \mathbb{F}_2^k | ab = \phi(z) + \phi(z+d)\} \\
= &\ 2^{k+1} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{\phi(z)ab}{(ab+\phi(z)+\phi(z+d))^2}\right) = 1\right\} - \#\{z \in \mathbb{F}_2^k | ab = \phi(z) + \phi(z+d)\}.
\end{aligned}$$

The second step holds according to Lemma 2.1.

Let $t = ab$. Then for any $d \in \mathbb{F}_2^k$, $t \in \mathbb{F}_{2^m}^*$,

$$\begin{aligned}
\Delta \ \geq \ &2^{k+1} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right) = 1\right\} \\
&-\#\{z \in \mathbb{F}_2^k | t = \phi(z) + \phi(z+d)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z+d)\}.
\end{aligned}$$

Thus Condition 3 holds.

Sufficiency: Assume that the function $F(x,z) = \phi(z)I(x)$ satisfies all of the three conditions. Then we need to prove that Eq.(2) holds for any $d \in \mathbb{F}_2^k, a, b \in \mathbb{F}_{2^m}$, where d and a can not be 0 at the same time.

The proof is divided into two cases.

Case 1: $ab = 0$.

If $a=0, b\in\mathbb{F}_{2^m}^*$, then

$$\begin{aligned}&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\phi(z)I(x)+\phi(z+d)I(x+a)=b\}\\ =&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\frac{\phi(z)+\phi(z+d)}{b}=x\}=2^k\le\Delta.\end{aligned}$$

If $b=0, d\in\mathbb{F}_2^{k*}, a\in\mathbb{F}_{2^m}$, then it follows from Condition 2, $\phi(z)$ is an injection, that

$$\begin{aligned}&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\phi(z)I(x)+\phi(z+d)I(x+a)=b\}\\ =&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\frac{a\phi(z)}{\phi(z)+\phi(z+d)}=x\}=2^k\le\Delta.\end{aligned}$$

If $b=d=0$, then $a\in\mathbb{F}_{2^m}^*$, and we have

$$\begin{aligned}&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\phi(z)I(x)+\phi(z+d)I(x+a)=b\}\\ =&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\phi(z)(I(x)+I(x+a))=0\}=0\le\Delta.\end{aligned}$$

The last step holds since $\phi(z)\neq 0$ for any $z\in\mathbb{F}_2^k$ and the Inverse function $I(x)$ is a bijection.

Case 2: a, b are arbitrary elements in $\mathbb{F}_{2^m}^*$.

According to the observations made in the sufficiency part of the proof, for any $d\in\mathbb{F}_2^k, a, b\in\mathbb{F}_{2^m}^*$,

$$\begin{aligned}&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\phi(z)I(x)+\phi(z+d)I(x+a)=b\}\\ =\;&2^{k+1}-2\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{\phi(z)ab}{(ab+\phi(z)+\phi(z+d))^2}\right)=1\right\}-\#\{z\in\mathbb{F}_2^k|ab=\phi(z)+\phi(z+d)\}\\ &+\#\{z\in\mathbb{F}_2^k|ab=\phi(z)\}+\#\{z\in\mathbb{F}_2^k|ab=\phi(z+d)\}.\end{aligned}$$

Let $t=ab$. Then according to Condition 3, for any $d\in\mathbb{F}_2^k$, $t\in\mathbb{F}_{2^m}^*$, we have

$$\begin{aligned}\Delta\;\ge\;&2^{k+1}-2\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}\\ -\;&\#\{z\in\mathbb{F}_2^k|t=\phi(z)+\phi(z+d)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z+d)\}\\ =\;&\sum_{z\in\mathbb{F}_2^k}\#\{x\in\mathbb{F}_{2^m}|\phi(z)I(x)+\phi(z+d)I(x+a)=b\}.\end{aligned}$$

The proof is complete. □

As we know, one sporadic differentially 6-uniform $(5,3)$-function (equivalently) has been found by Carlet and AlSalami [6] very recently. It has the form $F(x,z)=\phi(z)I(x)$, where $I(x)$ is the Inverse function on $\mathbb{F}_{2^3}$ and $\phi((0,0))=1, \phi((0,1))=\alpha^3, \phi((1,0))=\alpha^6, \phi((1,1))=\alpha^5$ (α is a primitive element of $\mathbb{F}_{2^3}$). Then a natural question is whether one can generalize it to construct differentially 6-uniform $(m+2,m)$-function with $m>3$. We get a negative conclusion according to the following corollary.

Corollary 3.2: Let $m>2^k$ be an integer. Consider the function $F:\mathbb{F}_2^{m+k}\to\mathbb{F}_{2^m}$ in the form $F(x,z)=\phi(z)I(x)$, where $\phi(z):\mathbb{F}_2^k\to\mathbb{F}_{2^m}$ and $I(x)$ is the (m,m)-Inverse function. Then the differential uniformity Δ of F satisfies: $\Delta\ge 2^{k+1}$.

Proof: Assume that the differential uniformity of $F(x,z)=\phi(z)I(x)$ is less than 2^{k+1}. Then it follows from Proposition 3.1 that $\phi(z)$ is an injection, $\phi(z)\neq 0$ for any $z\in\mathbb{F}_2^k$ and for any $d\in\mathbb{F}_2^k$, $t\in\mathbb{F}_{2^m}^*$,

$$\begin{aligned}2^{k+1}>\Delta \quad &\geq \quad 2^{k+1}-2\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}\\ &\quad -\#\{z\in\mathbb{F}_2^k|t=\phi(z)+\phi(z+d)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z+d)\}.\end{aligned}$$

Let $d=0$. Then $\#\{z\in\mathbb{F}_2^k|t=\phi(z)+\phi(z+d)\}=0$ since $t\in\mathbb{F}_{2^m}^*$. Thus for any $t\in\mathbb{F}_{2^m}^*$,

$$2^{k+1}-2\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{\phi(z)}{t}\right)=1\right\}+2\#\{z\in\mathbb{F}_2^k|t=\phi(z)\}<2^{k+1}.$$

This means

$$\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{\phi(z)}{t}\right)=1\right\}>\#\{z\in\mathbb{F}_2^k|t=\phi(z)\}\geq 0.$$

Thus for any $t\in\mathbb{F}_{2^m}^*$, there exists $z\in\mathbb{F}_2^k$ such that $\mathrm{Tr}_m(\frac{\phi(z)}{t})=1$. Then for any $t\in\mathbb{F}_{2^m}^*$, there exists $\beta\in\mathrm{Span}\{\phi(z)|z\in\mathbb{F}_2^k\}$ such that $\mathrm{Tr}_m(\frac{\beta}{t})=1$. This means for any $t\in\mathbb{F}_{2^m}^*$, $\frac{1}{t}\notin\mathrm{Span}\{\phi(z)|z\in\mathbb{F}_2^k\}^{\perp}$, that is, $\mathrm{Rank}(\mathrm{Span}\{\phi(z)|z\in\mathbb{F}_2^k\})=m$. Thus $2^k\geq m$, a contradiction! □

Corollary 3.2 shows that no functions $F:\mathbb{F}_2^{m+k}\to\mathbb{F}_{2^m}$ in the form $F(x,z)=\phi(z)I(x)$ can have differential uniformity strictly less than 2^{k+1} when $m>2^k$. Let $k=2$. Then we have $\Delta_F\geq 8$ when $m>2^k=4$. We searched all of the possible $\phi(z)$ when $m=3,4$ and found that the example in [6] is the only differentially 6-uniform $(m+2,m)$-function in this form up to CCZ-equivalence. Then we have the following corollary.

Proposition 3.3: Let m be an integer. The example in [6] is the only differentially 6-uniform $(m+2,m)$-function in the form $F(x,z)=\phi(z)I(x)$ up to CCZ-equivalence, where $\phi(z):\mathbb{F}_2^2\to\mathbb{F}_{2^m}$ and $I(x)$ is the (m,m)-Inverse function.

Remark 3.4: We also searched all possible $(5,3)$-functions in the form $F(x,z)=\phi(z)H(x)$, where $\phi(z)$ is any $(3,2)$-function and $H(x)$ is any $(3,3)$-function. Unfortunately, the example in [6] is the only differentially 6-uniform function up to CCZ-equivalence.

IV. Infinite families of low differential uniformity $(m+k,m)$-functions in the form $F(x,z)=\phi(z)I(x)$

A. An infinite family of $(2m-1,m)$-functions achieving Nyberg's bound

In this subsection, low differential uniformity $(m+k,m)$-functions in the form $F(x,z)=\phi(z)I(x)$ with $k=m-1$ are investigated. We construct an infinite family of differentially Δ-uniform $(2m-1,m)$-functions in the form $F(x,z)=\phi(z)I(x)$ achieving Nyberg's bound and prove it with the help of Proposition 3.1.

Proposition 4.1: Let $m\geq 2$ be an integer. Consider the function $F:\mathbb{F}_2^{2m-1}\to\mathbb{F}_{2^m}$ in the form $F(x,z)=\phi(z)I(x)$. Here $I(x)$ is the (m,m)-Inverse function and $\phi:\mathbb{F}_2^{m-1}\to\mathbb{F}_{2^m}$ is affine with $\mathrm{Rank}\{\phi(z)|z\in\mathbb{F}_2^{m-1}\}=m$. Then F is a differentially Δ-uniform function with $\Delta=2^{m-1}+2$.

Proof: Since $\phi(z)$ is affine, let $\phi(z)=L(z)+c_1$, where $L(z):\mathbb{F}_2^{m-1}\to\mathbb{F}_{2^m}$ is a linear function, $c_1\in\mathbb{F}_{2^m}$ is a constant. Further, with $\mathrm{Rank}\{\phi(z)|z\in\mathbb{F}_2^{m-1}\}=m$, we know that $\{\phi(z)|z\in\mathbb{F}_2^{m-1}\}$ cannot be a vector space and cannot be an affine space of dimension less than $m-1$. This means $\phi(z)$ is an injection and it does not vanish for any $z\in\mathbb{F}_2^{m-1}$. Then we only need to verify the last condition in Proposition 3.1, that is, for any $d\in\mathbb{F}_2^{m-1}$, $t\in\mathbb{F}_{2^m}^*$,

$$\begin{aligned}&2^{m-1}+2\geq 2^m-2\#\left\{z\in\mathbb{F}_2^{m-1}\middle|\mathrm{Tr}_m\left(\tfrac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}\\ &-\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z)+\phi(z+d)\}+\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z)\}+\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z+d)\}.\end{aligned}\tag{3}$$

If $t+L(d)=0$, then $\{z\in\mathbb{F}_2^{m-1}|t=\phi(z)+\phi(z+d)\}=\{z\in\mathbb{F}_2^{m-1}|t=L(d)\}=2^{m-1}$. Hence (3) holds in this case clearly. Thus we only need to consider the case $d\in\mathbb{F}_2^{m-1}$, $t\in\mathbb{F}_{2^m}^*$ satisfying $t+L(d)\neq 0$.

Since $\mathrm{Rank}\{\phi(z)|z\in\mathbb{F}_2^{m-1}\}=m$, $\gamma\notin\mathrm{Span}\{\phi(z)|z\in\mathbb{F}_2^{m-1}\}^{\perp}$ holds for any $\gamma\in\mathbb{F}_{2^m}^*$. This means for any $\gamma\in\mathbb{F}_{2^m}^*$, there exists $\beta\in\mathrm{Span}\{\phi(z)|z\in\mathbb{F}_2^{m-1}\}$ such that $\mathrm{Tr}_m(\gamma\beta)=1$. It is equivalent to say that, for any $\gamma\in\mathbb{F}_{2^m}^*$, there exists $z\in\mathbb{F}_2^{m-1}$ such that $\mathrm{Tr}_m(\phi(z)\gamma)=1$.

For any $d\in\mathbb{F}_2^{m-1}$, $t\in\mathbb{F}_{2^m}^*$ satisfying $t+L(d)\neq 0$, let us apply the observation above with $\gamma=\frac{t}{(t+L(d))^2}$. Then there exists $z\in\mathbb{F}_2^{m-1}$ such that $\mathrm{Tr}_m(\frac{\phi(z)t}{(t+L(d))^2})=1$.

According to Fact 1, we have

$$\begin{aligned}2^{m-2} &\leq \#\left\{z\in\mathbb{F}_2^{m-1}\middle|\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+L(d))^2}\right)=1\right\}\\ &= \#\left\{z\in\mathbb{F}_2^{m-1}\middle|\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}.\end{aligned}$$

It is clear that for any $d\in\mathbb{F}_2^{m-1}$, $t\in\mathbb{F}_{2^m}^*$,

$$\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z)\}+\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z+d)\}\leq 2$$

and

$$\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z)+\phi(z+d)\}\geq 0.$$

Thus for any $d\in\mathbb{F}_2^{m-1}$, $t\in\mathbb{F}_{2^m}^*$ satisfying $t+L(d)\neq 0$,

$$\begin{aligned}&2^m-2\#\left\{z\in\mathbb{F}_2^{m-1}\middle|\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}\\ &-\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z)+\phi(z+d)\}+\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z)\}+\#\{z\in\mathbb{F}_2^{m-1}|t=\phi(z+d)\}\\ \leq\ & 2^m-2*2^{m-2}-0+2=2^{m-1}+2.\end{aligned}$$

All in all, $\Delta\leq 2^{m-1}+2$ according to Proposition 3.1. According to Nyberg's results [18], F can not be PN function, thus $\Delta=2^{m-1}+2$. □

Define the vectorial function $\phi(z)=(z,1)$, where $z\in\mathbb{F}_2^{m-1}$. The image set of $\phi(z)$ is $\mathbb{F}_{2^{m-1}}\times\mathbb{F}_2$, which is isomorphic to $\mathbb{F}_{2^m}$ as an m-dimensional vector space. It is clear that $\phi:\mathbb{F}_2^{m-1}\to\mathbb{F}_{2^m}$ is affine and $\mathrm{Rank}\{\phi(z)|z\in\mathbb{F}_2^{m-1}\}=m$. Then we have the following construction according to Proposition 4.1, which gives the first infinite family of $(m+k,m)$-functions with $m>k\geq 2$ achieve Nyberg's bound.

Construction 1: Let $m\geq 2$ be an integer. Consider the function $F:\mathbb{F}_2^{2m-1}\to\mathbb{F}_{2^m}$ in the form $F(x,z)=\phi(z)I(x)$. Here $I(x)$ is the (m,m)-Inverse function and $\phi(z)=(z,1)$, where the image set of $\phi(z)$ is $\mathbb{F}_{2^{m-1}}\times\mathbb{F}_2$. Then F is a differentially Δ-uniform function with $\Delta=2^{m-1}+2$.

At the end of this subsection, we discuss the other cryptographic and combinatorial properties of Construction 1. We prove that every function from Construction 1, whose differential uniformity achieves Nyberg's bound, also has quite high nonlinearity and not too low algebraic degree. Moreover, we prove that it is a balanced vectorial semi-bent function.

We first consider a more general case. Assume that the Maiorana-McFarland bent function $F'(x,z')=\pi(x)L'(z')+h(x)$, where $L':\mathbb{F}_2^m\to\mathbb{F}_{2^m}$ is a linear bijection, $\pi:\mathbb{F}_2^m\to\mathbb{F}_{2^m}$ is a bijection and h is any function from $\mathbb{F}_2^m$ to $\mathbb{F}_{2^m}$. If we restrict Maiorana-McFarland bent function by taking the last coordinate of the input variables zero and delete this coordinate, then we are in the situation of $F(x,z)=I(x)\phi(z)+h(x)$, where ϕ is a linear $(m-1,m)$-function whose image is a linear hyperplane of $\mathbb{F}_{2^m}$. The following lemma indicates that all these $(2m-1,m)$-functions obtained by deleting one coordinate from the Maiorana-McFarland bent function are vectorial semi-bent function with high nonlinearity.

Lemma 4.2: Let $m \geq 2$ be an integer. We define the function $F : \mathbb{F}_2^{2m-1} \to \mathbb{F}_{2^m}$ in the form

$$F(x,z) = \pi(x)L(z) + h(x),$$

where $\pi : \mathbb{F}_2^m \to \mathbb{F}_{2^m}$ is a bijection, $L : \mathbb{F}_2^{m-1} \to \mathbb{F}_{2^m}$ is a linear injection and h is any function from $\mathbb{F}_2^m$ to $\mathbb{F}_{2^m}$. Then F is a vectorial semi-bent function and $NL(F) = 2^{2m-2} - 2^{m-1}$.

Proof: For any $v \in \mathbb{F}_{2^m}^*, u \in \mathbb{F}_2^{2m-1}$, assume that $u_1 \in \mathbb{F}_2^m, u_2 \in \mathbb{F}_2^{m-1}$ satisfy $(u_1, u_2) = u$, we have

$$\begin{aligned} F^{\mathcal{W}}(u,v) &= \sum_{(x,z)\in\mathbb{F}_2^{2m-1}} (-1)^{\mathrm{Tr}_m(vF(x,z))+u\cdot(x,z)} \\ &= \sum_{x\in\mathbb{F}_2^m, z\in\mathbb{F}_2^{m-1}} (-1)^{\mathrm{Tr}_m(vh(x))+\mathrm{Tr}_m(v\pi(x)L(z))+u_1\cdot x+u_2\cdot z} \\ &= \sum_{x\in\mathbb{F}_2^m, z\in\mathbb{F}_2^{m-1}} (-1)^{\mathrm{Tr}_m(vh(x))+u_1\cdot x+L^*(v\pi(x)+u_2)\cdot z} \\ &= \sum_{x\in\mathbb{F}_2^m} (-1)^{\mathrm{Tr}_m(vh(x))+u_1\cdot x} \left(\sum_{z\in\mathbb{F}_2^{m-1}} (-1)^{L^*(v\pi(x)+u_2)\cdot z} \right). \end{aligned}$$

The third equality holds since for any $L : \mathbb{F}_2^{m-1} \to \mathbb{F}_{2^m}$, there exists $L^* : \mathbb{F}_{2^m} \to \mathbb{F}_2^{m-1}$ such that for any $\alpha \in \mathbb{F}_{2^m}, z \in \mathbb{F}_2^{m-1}$, $\mathrm{Tr}_m(\alpha L(z)) = L^*(\alpha) \cdot z$.

It is clear that $L^*(v\pi(x) + u_2) \cdot z$ is linear since $v\pi(x) + u_2$ can be viewed as a constant up to z. Notice that $L : \mathbb{F}_2^{m-1} \to \mathbb{F}_{2^m}$ is a linear injection, then $\sum_{z\in\mathbb{F}_2^{m-1}} (-1)^{L^*(v\pi(x)+u_2)\cdot z}$ is 2^{m-1} if $v\pi(x)+u_2 \in \{L(z)|z \in \mathbb{F}_2^{m-1}\}^\perp$ and it is 0 otherwise. Hence for any $v \in \mathbb{F}_{2^m}^*, u \in \mathbb{F}_2^{2m-1}$,

$$F^{\mathcal{W}}(u,v) = 2^{m-1} \sum_{v\pi(x)+u_2\in\{L(z)|z\in\mathbb{F}_2^{m-1}\}^\perp} (-1)^{\mathrm{Tr}_m(vh(x)+u_1x)} \in \{0, \pm 2^m\}.$$

The last step holds since $\pi(x)$ is a bijection and $\dim(\{L(z)|z \in \mathbb{F}_2^{m-1}\}^\perp) = 1$.

Thus F is a vectorial semi-bent function and

$$NL(F) = 2^{2m-2} - \frac{1}{2} \max_{v\in\mathbb{F}_{2^m}^*, u\in\mathbb{F}_2^{2m-1}} \left| \sum_{(x,z)\in\mathbb{F}_2^{2m-1}} (-1)^{\mathrm{Tr}_m(vF(x,z))+u\cdot(x,z)} \right| = 2^{2m-2} - 2^{m-1}.$$

The proof is complete. □

The differential uniformity of functions in Lemma 4.2 are at most 2^m in general but not $2^{m-1}+2$, except in some very delicately chosen I. We will discuss it in the last section. It is clear that those functions from Construction 1 are the particular cases of Lemma 4.2 with $\pi(x) = I(x), h(x) = (0,1)I(x)$ and $L(z) = (z,0)$, where $(0,1)$ and $(z,0)$ are elements in $\mathbb{F}_{2^{m-1}} \times \mathbb{F}_2$, which is isomorphic to $\mathbb{F}_{2^m}$. Then we have the following proposition.

Proposition 4.3: Let $m \geq 2$ be an integer and $F : \mathbb{F}_2^{2m-1} \to \mathbb{F}_{2^m}$ in the form $F(x,z) = \phi(z)I(x)$, where $I(x)$ is the (m,m)-Inverse function and $\phi(z) = (z,1)$. Then F is an infinite family of $(2m-1,m)$-functions with differential uniformity $2^{m-1}+2$, nonlinearity $2^{2m-2} - 2^{m-1}$ and algebraic degree m. Moreover, these functions are balanced vectorial semi-bent functions.

Proof: Since the algebraic degree of the Inverse function $I(x)$ is $m-1$ and the affine function $\phi(z)$ is 1, the algebraic degree of $(2m-1,m)$-function $F(x,z) = \phi(z)I(x)$ is m according to the definition.

Notice that for any $v \in \mathbb{F}_{2^m}^*$,

$$\begin{aligned} F^{\mathcal{W}}(0,v) &= \sum_{(x,z)\in\mathbb{F}_2^{2m-1}} (-1)^{\mathrm{Tr}_m(vF(x,z))} \\ &= \sum_{z\in\mathbb{F}_2^{m-1}} \left(\sum_{x\in\mathbb{F}_2^m} (-1)^{\mathrm{Tr}_m(v\phi(z)I(x))} \right) \\ &= \sum_{z\in\mathbb{F}_2^{m-1}} 0 = 0. \end{aligned}$$

The last step holds since $I(x)$ is a bijection and $v\phi(z)$ does not vanish, then all component functions of F are balanced.

According to Proposition 4.1 and Lemma 4.2, Construction 1 builds an infinite family of $(2m-1,m)$-functions with the lowest differential uniformity $2^{m-1}+2$, high nonlinearity $2^{2m-2}-2^{m-1}$ and not too low algebraic degree m. Moreover, these constructions are balanced vectorial semi-bent functions.

B. Differentially 4-uniform $(m+1,m)$-functions lead to differentially 4-uniform permutations

In this section, we investigate low differential uniformity $(m+k,m)$-functions in the form $F(x,z)=\phi(z)I(x)$ with $k=1$. We discuss an infinite family of differentially 4-uniform $(m+1,m)$-functions with the help of Proposition 3.1, which leads to many differentially 4-uniform permutations.

Proposition 4.4: Let $m \geq 2$ be an integer. For any element $c \in \mathbb{F}_{2^m} \setminus \{0,1\}$ such that $\mathrm{Tr}_m(c) = \mathrm{Tr}_m(\frac{1}{c}) = 1$, we define the function $F : \mathbb{F}_2^{m+1} \to \mathbb{F}_{2^m}$ in the form $F(x,z)=\phi(z)I(x)$, where $I(x)$ is the (m,m)-Inverse function and $\phi(z)=(c-1)z+1$ is from $\mathbb{F}_2$ to $\mathbb{F}_{2^m}$. Then F is a differentially 4-uniform function.

Proof: It follows from $c \in \mathbb{F}_{2^m} \setminus \{0,1\}$ that Conditions 1 and 2 in Proposition 3.1 are satisfied. We only need to verify Condition 3, which is equivalent to

$$\begin{aligned} 0 \leq\ & 2\#\left\{ z\in\mathbb{F}_2 \middle| \mathrm{Tr}_m\left(\tfrac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1 \right\} + \#\{z\in\mathbb{F}_2 | t=\phi(z)+\phi(z+d)\} \\ & -\#\{z\in\mathbb{F}_2|t=\phi(z)\} - \#\{z\in\mathbb{F}_2|t=\phi(z+d)\} \end{aligned} \tag{4}$$

for any $d \in \mathbb{F}_2$, $t \in \mathbb{F}_{2^m}^*$. The proof is divided into two cases.

Case 1: $d=1$. Notice that $\phi(z)=(c-1)z+1$, then (4) reduce to

$$\begin{aligned} & 2\#\left\{ z\in\mathbb{F}_2 \middle| \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1 \right\} + \#\{z\in\mathbb{F}_2|t=\phi(z)+\phi(z+d)\} \\ & -\#\{z\in\mathbb{F}_2|t=\phi(z)\} - \#\{z\in\mathbb{F}_2|t=\phi(z+d)\} \\ = \ & 2\#\left\{ z\in\mathbb{F}_2 \middle| \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+c-1)^2}\right)=1 \right\} + \#\{z\in\mathbb{F}_2|t=c-1\} \\ & -\#\{z\in\mathbb{F}_2|t=\phi(z)\} - \#\{z\in\mathbb{F}_2|t=\phi(z+1)\} \\ = \ & 2\#\left\{ \mathrm{Tr}_m\left(\frac{t}{(t+c-1)^2}\right)=1 \right\} + 2\#\left\{ \mathrm{Tr}_m\left(\frac{ct}{(t+c-1)^2}\right)=1 \right\} \\ & +2\#\{t=c-1\} - 2\#\{t=1\} - 2\#\{t=c\} \\ \geq \ & 0. \end{aligned}$$

Since $\mathrm{Tr}_m(c)=\mathrm{Tr}_m(\frac{1}{c})=1$, the last step holds when $t=1$ or c, (it clearly holds when $t \neq 1,c$.)

Case 2: $d = 0$. Similarly, we have

$$\begin{aligned}
& 2\#\left\{z \in \mathbb{F}_2 \middle| \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right) = 1\right\} + \#\{z \in \mathbb{F}_2 | t = \phi(z) + \phi(z+d)\} \\
& -\#\{z \in \mathbb{F}_2 | t = \phi(z)\} - \#\{z \in \mathbb{F}_2 | t = \phi(z+d)\} \\
= \; & 2\#\left\{z \in \mathbb{F}_2 \middle| \mathrm{Tr}_m\left(\frac{\phi(z)}{t}\right) = 1\right\} + \#\{z \in \mathbb{F}_2 | t = 0\} - 2\#\{z \in \mathbb{F}_2 | t = \phi(z)\} \\
= \; & 2\#\left\{\mathrm{Tr}_m\left(\frac{1}{t}\right) = 1\right\} + 2\#\left\{\mathrm{Tr}_m\left(\frac{c}{t}\right) = 1\right\} + 2\#\{t = 0\} - 2\#\{t = 1\} - 2\#\{t = c\} \\
\geq \; & 0,
\end{aligned}$$

where the last step holds since $\mathrm{Tr}_m(c) = \mathrm{Tr}_m(\frac{1}{c}) = 1$. □

By using the proposition above, one can construct many differentially 4-uniform permutations.

Construction 2: Let $m \geq 2$ be an integer. For any element $c \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ such that $\mathrm{Tr}_m(c) = \mathrm{Tr}_m(\frac{1}{c}) = 1$, we define the function $F : \mathbb{F}_2^{m+1} \to \mathbb{F}_{2^m}$ in the form $F(x, z) = \phi(z)I(x)$, where $I(x)$ is the (m, m)-Inverse function and $\phi(z) = (c-1)z + 1$ is from $\mathbb{F}_2$ to $\mathbb{F}_{2^m}$. Then

$$F_P(x) = (\phi(z)I(x), f(\frac{x}{\phi(z)}) + z)$$

is a differentially 4-uniform $(m+1, m+1)$-permutation, where f is an arbitrary Boolean function defined on $\mathbb{F}_{2^m}$.

Proof: For any two elements $(x_1, z_1), (x_2, z_2) \in \mathbb{F}_2^{m+1}$, if $z_1 = z_2$ and $x_1 \neq x_2$, then $F_P(x_1, z_1) \neq F_P(x_2, z_2)$ since $\phi(z)I(x)$ is bijective on $\mathbb{F}_{2^m}$ no matter $z = 0$ or 1. If $z_1 \neq z_2$, then without loss of generality, we assume that $z_1 = 0$ and $z_2 = 1$. We can see that $F_P(x_1, z_1) = F_P(x_2, z_2)$ leads to $I(x_1) = cI(x_2)$, which is equivalent to $x_2 = cx_1$. Note that the last coordinate function of $F_P(x_1, z_1)$ is $f(x_1)$ and the last coordinate function of $F_P(x_2, z_2)$ equals $f(\frac{x_2}{c}) + 1 = f(\frac{cx_1}{c}) + 1 = f(x_1) + 1$, which does not equal $f(x_1)$. So F_P is an injection. Therefore, F_P is a permutation.

Notice that the differential uniformity of the function F_P is clearly no more than 4 according to Proposition 4.4. Thus F_P is a differentially 4-uniform $(m+1, m+1)$-permutation. □

When m is odd, the functions in Construction 2 become the differentially 4-uniform permutations presented by C.Carlet, D.Tang, X.Tang and Q.Y.Liao. [10, Construction 1], which is proved by the APN property of the Inverse function on odd dimension. However, Construction 2 shows that F_P is also a differentially 4-uniform $(m+1, m+1)$-permutation when m is even, although the Inverse function with even dimension is not an APN function.

C. More infinite families of $(m+k, m)$-functions with low differential uniformity

In this section, low differential uniformity $(m+k, m)$-functions in the form $F(x, z) = \phi(z)I(x)$ with $1 \leq k \leq m-2$ are investigated. We present a method to construct more infinite families of $(m+k, m)$-functions with low differential uniformity by modifying Construction 1. As an application, we construct an infinite family of differentially Δ-uniform $(2m-2, m)$-functions in the form $F(x, z) = \phi(z)I(x)$ with $\Delta \leq 2^{m-1} - 2^{m-6} + 2$.

The following proposition introduce a method to construct more infinite families of $(m+k, m)$-functions with low differential uniformity by modifying Construction 1. We place the completed proof in Appendix A for interested readers.

Proposition 4.5: Let m, l be positive integers and $1 \leq k \leq m-2$. Let U_i $(1 \leq i \leq m-k-1)$ be disjoint sets in $\mathbb{F}_2^k$ satisfying $\sum_{i=1}^{m-k-1} \#U_i \leq 2^{k-2} - l$ and such that, for any U_i, any element in $\mathbb{F}_2^k$ appears at least $2l$ times in the multiset $\{* \ z_1 + z_2 | (z_1, z_2) \in U_i \times U_i \ *\}$.
Consider the function $F : \mathbb{F}_2^{m+k} \to \mathbb{F}_{2^m}$ in the form $F(x, z) = \phi(z)I(x)$, where $I(x)$ is the (m, m)-Inverse function and $\phi : \mathbb{F}_2^k \to \mathbb{F}_{2^m}$ is defined as

$$\phi(z) = \begin{cases} L(z) + c_i, & \text{when} \quad z \in U_i, \\ L(z) + c_0, & \text{when} \quad z \in \mathbb{F}_2^k \setminus \bigcup_{i=1}^{m-k-1} U_i, \end{cases} \tag{5}$$

and satisfies $Rank\{\phi(z) | z \in \mathbb{F}_2^k\} = m$, $L : \mathbb{F}_2^k \to \mathbb{F}_{2^m}$ is linear and c_i $(0 \leq i \leq m-k-1)$ are constants in $\mathbb{F}_{2^m}$. Then F is a differentially Δ-uniform function with $\Delta \leq 2^{k+1} - 4l + 2$.

In the following construction, we obtain an infinite family of functions satisfying the hypothesis of Proposition 4.5 with $k = m-2$ and $l = 2^{m-8}$.

Construction 3: Let $m \geq 8$ be an integer. Assume that

$$f(z) = ((z_1 + 1)(z_2 + 1)(z_3 + 1) + 1)((z_4 + 1)(z_5 + 1)(z_6 + 1) + 1) + 1,$$

where $z_i, 1 \leq i \leq 6$ are the first 6 bits of $z \in \mathbb{F}_2^{m-2}$. Consider the function $F : \mathbb{F}_2^{2m-2} \to \mathbb{F}_{2^m}$ in the form $F(x, z) = \phi(z)I(x)$. Here $I(x)$ is the (m, m)-Inverse function and $\phi(z) = (z, f(z), f(z) + 1)$. Then F is a differentially Δ-uniform function with $\Delta \leq 2^{m-1} - 2^{m-6} + 2$ and the algebraic degree of F is $m + 5$.
Proof: Since the algebraic degree of the Inverse function $I(x)$ is $m - 1$ and the function $\phi(z)$ is 6, the algebraic degree of $(2m - 2, m)$-function $F(x, z) = \phi(z)I(x)$ is $m + 5$ according to the definition.

Let

$$U_1 = \{(h_1, 0, h_3) | h_1 \in \mathbb{F}_2^3, h_3 \in \mathbb{F}_2^{m-8}\} \bigcup \{(0, h_2, h_3) | h_2 \in \mathbb{F}_2^3, h_3 \in \mathbb{F}_2^{m-8}\}$$

be a set with elements in $\mathbb{F}_2^{m-2}$. Then $\phi(z)$ can be expressed by

$$\phi(z) = \begin{cases} (z, 1, 0), & \text{when} \quad z \in U_1; \\ (z, 0, 1), & \text{when} \quad z \in \mathbb{F}_2^{m-2} \setminus U_1. \end{cases} \tag{6}$$

Further, let $k = m-2$ and $l = 2^{m-8}$, and let us take in Proposition 4.5 for linear function $L : \mathbb{F}_2^{m-2} \to \mathbb{F}_{2^m}$ the function $L(z) = (z, 0, 0)$ and for constants: $c_0 = (0, 0, 1), c_1 = (0, 1, 0) \in \mathbb{F}_{2^m}$. Then we obtain the function $F(x, z)$ as defined in the present proposition. Then we need to prove the following conditions.
1. $\#U_1 \leq 2^{m-4} - 2^{m-8}$.
2. Any element in $\mathbb{F}_2^{m-2}$ appears at least 2^{m-7} times in the multiset

$$\{* \ z_1 + z_2 | (z_1, z_2) \in U_1 \times U_1 \ *\}.$$

3. $\mathrm{Rank}\{\phi(z) | z \in \mathbb{F}_2^{m-2}\} = m$.

Since $\{(h_1, 0, h_3) | h_1 \in \mathbb{F}_2^3, h_3 \in \mathbb{F}_2^{m-8}\} \bigcap \{(0, h_2, h_3) | h_2 \in \mathbb{F}_2^3, h_3 \in \mathbb{F}_2^{m-8}\} = \{(0, 0, h_3) | h_3 \in \mathbb{F}_2^{m-8}\}$, we have

$$\#U_1 = |\mathbb{F}_2^{m-8}|(|\mathbb{F}_2^3| + |\mathbb{F}_2^3| - 1) = 15 \times 2^{m-8} = 2^{m-4} - 2^{m-8},$$

which means Condition 1 holds.

For any $h \in \mathbb{F}_2^{m-2}$, let $h = (h_1', h_2', h_3')$ with $h_1', h_2' \in \mathbb{F}_2^3$ and $h_3' \in \mathbb{F}_2^{m-8}$. If $(h_1', h_2') \neq (0,0)$, then

$$\begin{aligned} h = (h_1', h_2', h_3') &= (h_1', 0, h_3) + (0, h_2', h_3 + h_3') \\ &= (0, h_2', h_3) + (h_1', 0, h_3 + h_3'), \end{aligned}$$

where h_3 is any element in $\mathbb{F}_2^{m-8}$. Notice that $(h_1', 0) \neq (0, h_2')$, then any element in this case appears at least 2^{m-7} times in the multiset $\{* \ z_1 + z_2 | (z_1, z_2) \in U_1 \times U_1 \ *\}$.

If $h_1' = h_2' = 0$, let $\tilde{h}$ be a non-zero element in $\mathbb{F}_2^{m-8}$, then

$$\begin{aligned} h = (0, 0, h_3') &= (0, 0, h_3) + (0, 0, h_3 + h_3') \\ &= (0, \tilde{h}, h_3) + (0, \tilde{h}, h_3 + h_3'), \end{aligned}$$

where h_3 is any element in $\mathbb{F}_2^{m-8}$. Then any element with $h_1' = h_2' = 0$ appears at least 2^{m-7} times in the multiset above. Thus Condition 2 holds.

Then we focus on Condition 3. According to Condition 2, for any $h \in \mathbb{F}_2^{m-2}$, there exists $z_1, z_2 \in U_1$ such that $h = z_1 + z_2$. Since $0 \in U_1$, we know that $(z_1, 1, 0), (z_2, 1, 0)$ and $(0, 1, 0) \in \{(z, 1, 0) | z \in U_1\}$. Because of

$$(h, 1, 0) = (z_1, 1, 0) + (z_2, 1, 0) + (0, 1, 0),$$

we have $(h, 1, 0) \in \mathrm{Span}\{(z, 1, 0) | z \in U_1\}$ for any $h \in \mathbb{F}_2^{m-2}$, that is, $\{(z, 1, 0) | z \in \mathbb{F}_2^{m-2}\} \subseteq \mathrm{Span}\{(z, 1, 0) | z \in U_1\}$. Then

$$\mathrm{Span}\{(z, 1, 0) | z \in \mathbb{F}_2^{m-2}\} \subseteq \mathrm{Span}\{(z, 1, 0) | z \in U_1\}.$$

It is clear that $\mathrm{Span}\{(z, 1, 0) | z \in U_1\} \subseteq \mathrm{Span}\{(z, 1, 0) | z \in \mathbb{F}_2^{m-2}\}$. Then we have

$$\mathrm{Span}\{(z, 1, 0) | z \in U_1\} = \mathrm{Span}\{(z, 1, 0) | z \in \mathbb{F}_2^{m-2}\}. \tag{7}$$

Moreover, let $g = (0, 0, 1, 0, 0, 1, 0), g' = (0, 1, 0, 0, 1, 0, g_3), g'' = (0, 1, 1, 0, 1, 1, g_3)$, where g_3 is an arbitrary element in $\mathbb{F}_2^{m-8}$. Then $g, g', g'' \in \mathbb{F}_2^{m-2} \setminus U_1$ and $(0, 0, 1) = (g, 0, 1) + (g', 0, 1) + (g'', 0, 1)$. This means

$$(0, 0, 1) \in \mathrm{Span}\{(z, 0, 1) | z \in \mathbb{F}_2^{m-2} \setminus U_1\}. \tag{8}$$

Then we have

$$\begin{aligned} & \mathrm{Rank}\{\phi(z) | z \in \mathbb{F}_2^{m-2}\} \\ = \ & \mathrm{Rank}(\{(z, 0, 1) | z \in \mathbb{F}_2^{m-2} \setminus U_1\} \cup \{(z, 1, 0) | z \in U_1\}) \\ = \ & \mathrm{Rank}(\mathrm{Span}\{(z, 0, 1) | z \in \mathbb{F}_2^{m-2} \setminus U_1\} \cup \mathrm{Span}\{(z, 1, 0) | z \in U_1\}) \\ \geq \ & \mathrm{Rank}(\{(0, 0, 1)\} \cup \mathrm{Span}\{(z, 1, 0) | z \in U_1\}) \\ = \ & \mathrm{Rank}(\{(0, 0, 1)\} \cup \mathrm{Span}\{(z, 1, 0) | z \in \mathbb{F}_2^{m-2}\}) \\ = \ & m, \end{aligned}$$

according to (7) and (8). Thus $\mathrm{Rank}\{\phi(z) | z \in \mathbb{F}_2^{m-2}\} = m$ according to $\phi(z) : \mathbb{F}_2^{m-2} \to \mathbb{F}_{2^m}$, which means Condition 3 holds.

Then F is a differentially Δ-uniform function with $\Delta \leq 2^{m-1} - 2^{m-6} + 2$ according to Proposition 4.5 and the algebraic degree of F is $m + 5$. □

Remark 4.6: We calculated by Magma [4] that when $m = 8$, Construction 3 builds a $(14, 8)$-function with differential uniformity 114 (which is much less than 126, the upper bound calculated by Construction 3 when $m = 8$), nonlinearity 7954 and algebraic degree 13 (which achieves the upper bound).

Remark 4.7: We also found some $(2m - 2, m)$-functions with low differential uniformity in the form $F(x, z) = \phi(z)I(x)$ when $m = 5, 6, 7$ by Magma. We list their specific forms in Appendix B and leave it open to generalize them.

V. More Discussions

In this section, we discuss the possibility of constructing functions achieving Nyberg's bound by Maiorana-McFarland bent functions or almost bent functions. The results show the difficulty of constructing functions achieving Nyberg's bound.

All of the functions in Lemma 4.2, which are obtained by deleting one coordinate from the Maiorana-McFarland bent function, are vectorial semi-bent function with high nonlinearity. Then a natural question is how are the differential uniformity of these functions. Let us begin with a more general case. Assume that the Maiorana-McFarland bent function $F'(x,z') = \pi(x)L'(z') + h(x)$, where $L' : \mathbb{F}_2^m \to \mathbb{F}_{2^m}$ is a linear bijection, $\pi : \mathbb{F}_2^m \to \mathbb{F}_{2^m}$ is a bijection and h is any function from $\mathbb{F}_2^m$ to $\mathbb{F}_{2^m}$. Let z_0 be the last $m-k$ coordinates of input variables $z' = (z, z_0)$, where $1 \le k \le m-1$. If we restrict the function by taking all the last $m-k$ coordinates of input variables of z' zero, and delete these coordinates, then we are in the situation of $F(x,z) = I(x)\phi(z) + h(x)$, where ϕ is a linear (k,m)-function.

Remark 5.1: Let $m \ge 2$ and $m-1 \ge k \ge 1$ be integers. We define the function $F : \mathbb{F}_2^{m+k} \to \mathbb{F}_{2^m}$ in the form

$$F(x,z) = \pi(x)L(z) + h(x),$$

where $\pi : \mathbb{F}_2^m \to \mathbb{F}_{2^m}$ is a bijection, $L : \mathbb{F}_2^k \to \mathbb{F}_{2^m}$ is a linear injection and h is any function from $\mathbb{F}_2^m$ to $\mathbb{F}_{2^m}$. Assume that the differential uniformity of $F(x,z)$ is Δ. Then for any $\bar{a} \in \mathbb{F}_2^{m+k*}, b \in \mathbb{F}_{2^m}$ with $\bar{a} = (a,d)$, where $a \in \mathbb{F}_{2^m}, d \in \mathbb{F}_2^k$, the following equation needs to have at most Δ solutions.

$$(\pi(x) + \pi(x+a))L(z) + \pi(x+a)L(d) + h(x) + h(x+a) = b. \tag{9}$$

In the case $a = 0$, we have $\pi(x)L(d) = b$, then (9) have at most 2^k solutions since $\pi(x)$ is a bijection. In the case $a \neq 0$, then we have

$$L(z) = \frac{\pi(x+a)L(d) + h(x) + h(x+a) + b}{\pi(x) + \pi(x+a)}.$$

Notice that $L(z)$ is a linear injection, then the number of the solutions is no more than 2^m. All in all, the differential uniformity of $F(x,z) = \pi(x)L(z) + h(x)$ is no more than 2^m in general.

Remark 5.1 shows an upper bound of the differential uniformity of those functions obtained by deleting coordinates from the Maiorana-McFarland bent function. However, the case $a \neq 0$ is not easy to handle. Even the case $d = 0$ makes already problem. Having π APN or differentially 4-uniform may help, but does not suffice since the choice of linear function L is also sensitive. The following remark indicates that this general upper bound can not be improved.

Remark 5.2: Let $m \ge 2$ and $1 \le k \le m-1$ be integers. For $F(x) = x\phi(z)$, where $x \in \mathbb{F}_{2^m}$ and $z \in \mathbb{F}_2^k$ and where $\phi(z)$ can be any function from $\mathbb{F}_2^k$ to $\mathbb{F}_{2^m}$, we have

$$D_{a,d}F(x,z) = x\phi(z) + (x+a)\phi(z+d) = x(\phi(z) + \phi(z+d)) + a\phi(z+d).$$

Hence, for $d = 0$ and $a \neq 0$, the equation $D_{a,b}F(x,z) = b$ has 2^m solutions for each choice of z such that $\phi(z) = \frac{b}{a}$ and the differential uniformity of F cannot be better than 2^m.

For the case $k = m-1$, these functions will have differential uniformity at most 2^m but not $2^{m-1}+2$ in general, except in some very delicately chosen I. For the case $1 \le k \le m-2$, the upper bound of the differential uniformity of these functions is worse then the known upper bound 2^{k+1} and these functions are also no longer semi-bent functions in general. Further more, the example in [6] is the only differentially 6-uniform $(5,3)$-function up to CCZ-equivalence according to Remark 3.4. All in all, we see that the Maiorana-McFarland construction does not allow to build easily functions achieving Nyberg's bound.

Another interesting question here is whether replacing $I(x)$ by other permutations with good cryptographic properties may also achieve Nyberg's bound, especially by an almost bent function, for odd m. Here we consider the simplest case of quadratic AB functions, e.g. x^3.

Remark 5.3: Assume that the differential uniformity of $F(x,z) = x^3\phi(z)$ is 2^k+2. Then for any $\bar{a} \in \mathbb{F}_2^{m+k*}, b \in \mathbb{F}_{2^m}$ with $\bar{a} = (a,d)$, where $a \in \mathbb{F}_{2^m}, d \in \mathbb{F}_2^k$, the following equation needs to have at most 2^k+2 solutions

$$(\phi(z)+\phi(z+d))x^3 + \phi(z+d)(ax^2+a^2x+a^3) = b. \tag{10}$$

Considering the special case $b=0, a=0, d\neq 0$ and $b=0, a\neq 0, d=0$, we have that $\phi(z)$ is an injection and $\phi(z)\neq 0$ for any $z \in \mathbb{F}_2^k$.
In the case $d=0$, (10) becomes $x^2+ax+a^2+\frac{b}{a\phi(z)}=0$, then we have

$$\sum_{z\in\mathbb{F}_2^k} \#\{x\in\mathbb{F}_{2^m} | Tr_1^n(1+\tfrac{b}{a^3\phi(z)})=0\} \leq 2^k+2. \tag{11}$$

In the case $d\neq 0$, then $\phi(z)+\phi(z+d)\neq 0$ since $\phi(z)$ is an injection. Let us denote $\xi = \frac{\phi(z+d)}{\phi(z)+\phi(z+d)}$ and replace x by $a(y+\xi)$. Then (10) becomes

$$y^3+(\xi^2+\xi)y+\xi^2+\xi+\tfrac{u}{a^3(\phi(z)+\phi(z+d))}=0. \tag{12}$$

Considering (12) as a cubic equation in y, according to Theorem 2.2, it has a unique solution in $\mathbb{F}_{2^n}$ if and only if

$$Tr_1^n\left(\frac{(\frac{\phi(z+d)}{\phi(z)+\phi(z+d)}+1)^3(\frac{\phi(z+d)}{\phi(z)+\phi(z+d)})^3}{(\frac{\phi(z+d)}{\phi(z)+\phi(z+d)})^4+(\frac{\phi(z+d)}{\phi(z)+\phi(z+d)})^2+\frac{b^2}{a^6(\phi(z)+\phi(z+d))^2}}+1\right)=1.$$

It seems quite difficult to go further; in particular, the case when (12) has three solutions seems more complex. Even if it can be simplified in some special case such as when taking $\phi(z)$ affine, it is still very difficult. Assume that $\phi(z)$ is affine, then (12) has one solution if and only if

$$Tr_1^n\left(\frac{(\frac{\phi(z+d)}{\phi(d)}+1)^3(\frac{\phi(z+d)}{\phi(d)})^3}{(\frac{\phi(z+d)}{\phi(d)})^4+(\frac{\phi(z+d)}{\phi(d)})^2+\frac{b^2}{a^6(\phi(d))^2}}+1\right)=1.$$

We see that handling the inverse function is much simpler.

We also made computer experiment for the case that $I(x)$ is replaced by an almost bent function, for odd m. We searched all possible $(9,5)$-functions in the form $F(x,z)=x^3\phi(z)$, where $(5,4)$-function $\phi(z)$ is affine. None of them achieves the Nyberg's bound. We leave it open to construct low differential uniformity functions with AB functions.

VI. Concluding Remarks

Little theoretical work has been done on (n,m)-functions when $\frac{n}{2}<m<n$. In this paper, a characterization of the differential uniformity of those (n,m)-functions of the form $F(x,z)=\phi(z)I(x)$ is presented, where $I(x)$ is the (m,m)-Inverse function and $\phi(z)$ is an $(n-m,m)$-function. Using this characterization, we construct an infinite family of differentially Δ-uniform $(2m-1,m)$-functions with $m\geq 3$ achieving Nyberg's bound with equality. Then we present a method to construct infinite families of $(m+k,m)$-functions with low differential uniformity and construct an infinite family of $(2m-2,m)$-functions with $\Delta \leq 2^{m-1}-2^{m-6}+2$ for any $m\geq 8$. We also study an infinite family of differentially 4-uniform

$(m+1,m)$-functions in this form, which leads to many differentially 4-uniform permutations. The newly obtained functions may provide more choices in Feistel ciphers. For further research, it is interesting to find other constructions of differentially Δ-uniform $(m+k,m)$-functions with $m > k \geq 2, m \neq 3$ and $\Delta < 2^{k+1}$. A more important challenge is whether a differentially 6-uniform $(m+2,m)$-function exists or not.

VII. Acknowledgement

We would like to thank Wolfgang Schmid and Tailin Niu for useful discussions for Construction 3.

References

[1] C.M. Adams, Constructing symmetric ciphers using the CAST design procedure. Designs, Codes, and Cryptography, Vol. 12, pp. 283-316, 1997.
[2] R. Anderson, E. Biham and L. Knudsen, Serpent: A proposal for the advanced encryption standard. NIST AES Proposal, Vol. 174, pp. 1-23, 1998.
[3] E. Biham, R. Anderson and L. Knudsen, Serpent: A new block cipher proposal. International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, Vol. 1372, pp. 222-238, 1998.
[4] W. Bosma, J. Cannon and C. Playoust, The magma algebra system I: The user language. J.Symbolic Comput, Vol. 24, pp. 235-265, 1997.
[5] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y.Seurin and C.Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007, Lecture Notes in Computer Science, Vol. 4727, pp. 450-466, 2007.
[6] C. Carlet and Y. AlSalami, A new construction of differentially 4-uniform $(n,n-1)$-functions. Advances in Mathematics of Communications, Vol. 9(4), pp. 541-565, 2015.
[7] C. Carlet, Open questions on nonlinearity and on APN functions, Arithmetic of Finite Fields, pp. 83-107, 2015.
[8] C. Carlet, Boolean and vectorial plateaued functions and APN functions. Information Theory, IEEE Transactions on, Vol. 61(11), pp. 6272-6289, 2015.
[9] C. Carlet, Vectorial boolean functions for cryptography. Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 398-470, 2010.
[10] C. Carlet, D. Tang, X.H. Tang and Q.Y. Liao, New Construction of Differentially 4-Uniform Bijections. Information Security and Cryptology, Vol. 8567, pp. 22-38, 2014.
[11] J.F. Dillon. Elementary Hadamard difference sets. University of Maryland, 1974.
[12] J. Daemen and V. Rijmen, The Design of Rijndael: AES: The Advanced Encryption Standard, Springer, 2002.
[13] European Telecommunications Standards Institute, Technical Specification 135 202 V9.0.0: Universal mobile telecommunications system (UMTS); LTE; specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification (3GPP TS 35.202 V9.0.0 Release 9).
[14] L.R. Knudsen and M. Robshaw, The Block Cipher Companion, Springer, 2011.
[15] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications 20, (1997).
[16] M. Matsui, New block encryption algorithm MISTY. International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, Vol. 1267, pp. 54-68, 1997.
[17] F.J. Macwilliams, N.J. Sloane. The theory of error-correcting codes. Amsterdam: North Holland, 1977.
[18] K. Nyberg. Perfect non-linear S-boxes. Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science, Vol. 547, pp. 378-386, 1992.
[19] National Institute of Standards and Technology, Data encryption standard (DES), Federal Information Processing Standards Publication 49-3. United States National Institute of Standards and Technology (NIST). Reaffirmed on October 25, 1999.
[20] National Institute of Standards and Technology, Advanced encryption standard (AES), Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST), 2001.
[21] K. Nyberg and L.R. Knudsen, Provable security against a differential attack. Journal of Cryptology, Vol. 8, pp. 27-37, 1995.
[22] K. Williams, Note on cubics over $GF(2^n)$ and $GF(3^n)$. Journal of Number Theory, Vol. 7, pp. 361-365, 1975.
[23] G. Piret, T. Roche, C. Carlet. PICARO - A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. International Conference on Applied Cryptography and Network Security, pp. 311-328, 2012.
[24] W.G. Zhang, C.L. Xie, E. Pasalic. Large Sets of Orthogonal Sequences Suitable for Applications in CDMA Systems. IEEE Transactions on Information Theory, Vol. 62(6), pp. 3757-3767, 2016.

VIII. APPENDIX

A. Completed proof of Proposition 5.1

Proposition 5.1: Let m, l be positive integers and $1 \leq k \leq m-2$. Let U_i $(1 \leq i \leq m-k-1)$ be disjoint sets in $\mathbb{F}_2^k$ satisfying $\sum_{i=1}^{m-k-1} \#U_i \leq 2^{k-2} - l$ and such that, for any U_i, any element in $\mathbb{F}_2^k$ appears at least $2l$ times in the multiset $\{* \ z_1 + z_2 | (z_1, z_2) \in U_i \times U_i \ *\}$.
Consider the function $F : \mathbb{F}_2^{m+k} \to \mathbb{F}_{2^m}$ in the form $F(x, z) = \phi(z)I(x)$, where $I(x)$ is the (m, m)-Inverse function and $\phi : \mathbb{F}_2^k \to \mathbb{F}_{2^m}$ is defined as

$$\phi(z) = \begin{cases} L(z) + c_i, & \text{when} \quad z \in U_i, \\ L(z) + c_0, & \text{when} \quad z \in \mathbb{F}_2^k \setminus \bigcup_{i=1}^{m-k-1} U_i, \end{cases} \tag{13}$$

and satisfies $Rank\{\phi(z) | z \in \mathbb{F}_2^k\} = m$, $L : \mathbb{F}_2^k \to \mathbb{F}_{2^m}$ is linear and c_i $(0 \leq i \leq m-k-1)$ are constants in $\mathbb{F}_{2^m}$. Then F is a differentially Δ-uniform function with $\Delta \leq 2^{k+1} - 4l + 2$.

Proof: Let $U_0 = \mathbb{F}_2^k \setminus \bigcup_{i=1}^{m-k-1} U_i$. According to the conditions on $\phi(z)$ and the fact that $\{L(z) | z \in \mathbb{F}_2^k\}$ is a vector space, we have

$$\begin{aligned} m &= \mathrm{Rank}\{\phi(z) | z \in \mathbb{F}_2^k\} \\ &= \mathrm{Rank}\left(\bigcup_{i=0}^{m-k-1} \{L(z) + c_i | z \in U_i\}\right) \\ &\leq \mathrm{Rank}\left(\bigcup_{i=0}^{m-k-1} \{L(z) + c_i | z \in \mathbb{F}_2^k\}\right) \\ &\leq \mathrm{Rank}(\mathrm{Span}(\{L(z) | z \in \mathbb{F}_2^k\} \cup \{c_i | 0 \leq i \leq m-k-1\})). \end{aligned}$$

The last step holds since for any i, $\{L(z) + c_i | z \in \mathbb{F}_2^k\} \subseteq \mathrm{Span}(\{L(z) | z \in \mathbb{F}_2^k\} \cup c_i)$. It is clear that the span of a set does not change its rank, then

$$\begin{aligned} m &\leq \mathrm{Rank}(\mathrm{Span}(\{L(z) | z \in \mathbb{F}_2^k\} \cup \{c_i | 0 \leq i \leq m-k-1\})) \\ &= \mathrm{Rank}(\{L(z) | z \in \mathbb{F}_2^k\} \cup \{c_i | 0 \leq i \leq m-k-1\}) \\ &= \mathrm{Rank}(\{L(z) | z \in \mathbb{F}_2^k\} \cup \mathrm{Span}\{c_i | 0 \leq i \leq m-k-1\}) \\ &= \mathrm{Rank}\{L(z) | z \in \mathbb{F}_2^k\} + \mathrm{Rank}(\mathrm{Span}\{c_i | 0 \leq i \leq m-k-1\}) \\ &\quad -\mathrm{Rank}(\{L(z) | z \in \mathbb{F}_2^k\} \cap \mathrm{Span}\{c_i | 0 \leq i \leq m-k-1\}) \\ &\leq k + (m-k) - 0 = m. \end{aligned}$$

Thus the last inequality is an equality, we have

$$\mathrm{Rank}\{L(z) | z \in \mathbb{F}_2^k\} = k, \tag{14}$$

$$\mathrm{Rank}(\mathrm{Span}\{c_i | 0 \leq i \leq m-k-1\}) = m-k, \tag{15}$$

and

$$\mathrm{Rank}(\{L(z) | z \in \mathbb{F}_2^k\} \cap \mathrm{Span}\{c_i | 0 \leq i \leq m-k-1\}) = 0. \tag{16}$$

For one thing, $c_i \neq 0$ because of (15) for any $0 \leq i \leq m-k-1$. Moreover, according to (16), we have $c_i \notin \{L(z) | z \in \mathbb{F}_2^k\}$ for any $0 \leq i \leq m-k-1$, which means $\phi(z)$ does not vanish for any $z \in \mathbb{F}_2^k$. For

another, assume that there exists $z_{i_1} \neq z_{i_2} \in \mathbb{F}_2^k$ such that $\phi(z_{i_1}) = \phi(z_{i_2})$, then $L(z_{i_1}) + c_{i_1} = L(z_{i_2}) + c_{i_2}$. If $c_{i_1} = c_{i_2}$, notice that $L(z)$ is a linear injection according to (14), then $z_{i_1} = z_{i_2}$, a contradiction. If $c_{i_1} \neq c_{i_2}$, then $0 \neq c_{i_1} + c_{i_2} \in \{L(z)|z \in \mathbb{F}_2^k\}$. According to (16), then $c_{i_1} + c_{i_2} \notin \mathrm{Span}\{c_i|0 \leq i \leq m-k-1\}$, a contradiction. Thus $\phi(z)$ is an injection. Then we only need to verify the last condition in Proposition 3.1, that is, for any $d \in \mathbb{F}_2^k$, $t \in \mathbb{F}_{2^m}^*$,

$$\begin{aligned} &2^{k+1} - 4l + 2 \geq 2^{k+1} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\tfrac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right) = 1\right\} \\ &-\#\{z \in \mathbb{F}_2^k | t = \phi(z) + \phi(z+d)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z+d)\}. \end{aligned} \tag{17}$$

Notice that U_i $(1 \leq i \leq m-k-1)$ are disjoint sets satisfying $\sum_{i=1}^{m-k-1} \#U_i \leq 2^{k-2} - l$, then $\#U_0 \geq 2^k - (2^{k-2} - l) = 3 * 2^{k-2} + l$, we have for any $d \in \mathbb{F}_2^k$,

$$\#\{z|z, z+d \in U_0\} \geq 2^{k-1} + 2l. \tag{18}$$

The reason of (18) is

$$\begin{aligned} & \#\{z|z, z+d \in U_0\} \\ = \ & \#(\{z|z \in U_0\} \bigcap \{z|z+d \in U_0\}) \\ = \ & \#\{z|z \in U_0\} + \#\{z|z+d \in U_0\} - \#(\{z|z \in U_0\} \bigcup \{z|z+d \in U_0\}) \\ \geq \ & \#\{z|z \in U_0\} + \#\{z|z+d \in U_0\} - \#\{z|z \in \mathbb{F}_2^k\} \\ = \ & 2\#U_0 - 2^k \\ \geq \ & 2^{k-1} + 2l. \end{aligned}$$

For any $d \in \mathbb{F}_2^k$ and $t \in \mathbb{F}_{2^m}^*$, if $t + L(d) = 0$, notice that $\phi(z) = L(z) + c_0$ for any $z \in U_0$, then we have

$$\begin{aligned} & \#\{z \in \mathbb{F}_2^k | t = \phi(z) + \phi(z+d)\} \\ \geq \ & \#\{z|z, z+d \in U_0, t = \phi(z) + \phi(z+d)\} \\ = \ & \#\{z|z, z+d \in U_0\} \\ \geq \ & 2^{k-1} + 2l. \end{aligned}$$

Then (17) holds in this case since

$$\begin{aligned} & 2^{k+1} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right) = 1\right\} \\ - \ & \#\{z \in \mathbb{F}_2^k | t = \phi(z) + \phi(z+d)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z+d)\} \\ \leq \ & 2^{k+1} - 2 \times 0 - \#\{z \in \mathbb{F}_2^k | t = \phi(z) + \phi(z+d)\} + 1 + 1 \\ \leq \ & 2^{k+1} - (2^{k-1} + 2l) + 2 \\ \leq \ & 2^{k+1} - 4l + 2, \end{aligned}$$

the last step follows from $0 \leq \#U \leq 2^{k-2} - l$. Thus we only need to consider the case $d \in \mathbb{F}_2^k$, $t \in \mathbb{F}_{2^m}^*$ satisfying $t + L(d) \neq 0$.

Since $\mathrm{Rank}\{\phi(z)|z \in \mathbb{F}_2^k\} = m$ leads to $\mathrm{Span}\{\phi(z)|z \in \mathbb{F}_2^k\}^\perp = \{0\}$, we have $\gamma \notin \mathrm{Span}\{\phi(z)|z \in \mathbb{F}_2^k\}^\perp$ for any $\gamma \in \mathbb{F}_{2^m}^*$. Hence, for any $\gamma \in \mathbb{F}_{2^m}^*$, there exists $\beta \in \mathrm{Span}\{\phi(z)|z \in \mathbb{F}_2^k\}$ such that $\mathrm{Tr}_m(\gamma\beta) = 1$. That is, for any $\gamma \in \mathbb{F}_{2^m}^*$, there exists $z \in \mathbb{F}_2^k$ such that $\mathrm{Tr}_m(\phi(z)\gamma) = 1$.

For any $d \in \mathbb{F}_2^k$ and $t \in \mathbb{F}_{2^m}^*$ satisfying $t + L(d) \neq 0$, $\frac{t}{(t+L(d))^2}$ does not vanish and the mappings $z \to \frac{(L(z)+c_i)t}{(t+L(d))^2}$ are affine functions since $L(z)$ is linear, where $0 \leq i \leq m-k-1$. Let us apply the observation above with $\gamma = \frac{t}{(t+L(d))^2}$. Then there exists $z_0 \in \mathbb{F}_2^k$ such that $\mathrm{Tr}_m\left(\frac{\phi(z_0)t}{(t+L(d))^2}\right) = 1$. The rest of the proof is divided into two cases $z_0 \in U_0$ and $z_0 \notin U_0$.

Case 1: $z_0 \in U_0$.

Then $\phi(z_0) = L(z_0) + c_0$. Since there exists $z \in \mathbb{F}_2^k$ such that $\mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right) = 1$ and $z \to \frac{(L(z)+c_0)t}{(t+L(d))^2}$ is an affine function, we can apply Fact 1 and we deduce:

$$\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right) = 1\right\} \geq 2^{k-1}. \tag{19}$$

In this case, we will only consider those z satisfying $z, z+d \in U_0$. Then

$$\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right) = \mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right)$$

for these z.

Further, for any $d \in \mathbb{F}_2^k$ and $t \in \mathbb{F}_{2^m}^*$ satisfying $t + L(d) \neq 0$, we have

$$\begin{aligned}
& 2^{k+1} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right) = 1\right\} \\
& -\#\{z \in \mathbb{F}_2^k | t = \phi(z) + \phi(z+d)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z)\} + \#\{z \in \mathbb{F}_2^k | t = \phi(z+d)\} \\
\leq\ & 2^{k+1} - 2\#\left\{z \middle| z, z+d \in U_0, \mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right) = 1\right\} - 0 + 1 + 1 \\
=\ & 2^{k+1} - 2\#\left\{z \middle| z, z+d \in U_0, \mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right) = 1\right\} + 2 \\
=\ & 2^{k+1} - 2\#\left(\{z|z, z+d \in U_0\} \bigcap \left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right) = 1\right\}\right) + 2 \\
=\ & 2^{k+1} - 2\#\{z|z, z+d \in U_0\} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right) = 1\right\} \\
+\ & 2\#\left(\{z|z, z+d \in U_0\} \bigcup \left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right) = 1\right\}\right) + 2 \\
\leq\ & 2^{k+1} - 2\#\{z|z, z+d \in U_0\} - 2\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right) = 1\right\} + 2\#\{z \in \mathbb{F}_2^k\} + 2 \\
\leq\ & 2^{k+1} - 2(2^{k-1} + 2l) - 2^k + 2^{k+1} + 2 \\
=\ & 2^{k+1} - 4l + 2.
\end{aligned}$$

The last inequality follows from (18) and (19).

Case 2: $z_0 \notin U_0$.

Then there exists $1 \leq i \leq m-k-1$ such that $z_0 \in U_i$. Thus $\phi(z_0) = L(z_0) + c_i$, which means there exists $z \in \mathbb{F}_2^k$ such that $\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right) = 1$. Since $z \to \frac{(L(z)+c_i)t}{(t+L(d))^2}$ is an affine function, we have

$$\#\left\{z \in \mathbb{F}_2^k \middle| \mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right) = 1\right\} = 2^{k-1} \ or \ 2^k,$$

according to Fact 1. The rest of the proof is divided into two subcases.

Subcase 2.1: $\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right)=1\right\}=2^{k-1}$.

Then

$$\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right)=0\right\}=2^{k-1}.$$

This means

$$\begin{aligned}\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right)=1\right\} &= \#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right)=\mathrm{Tr}_m\left(\frac{(c_0+c_i)t}{(t+L(d))^2}\right)+1\right\}\\ &= 2^{k-1}\end{aligned}$$

no matter constant $\mathrm{Tr}_m\left(\frac{(c_0+c_i)t}{(t+L(d))^2}\right)+1$ equals 0 or 1.

Notice that both (18) and (19) also hold in this subcase; similar to Case 1, we only consider those z satisfying $z, z+d\in U_0$. Then

$$\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=\mathrm{Tr}_m\left(\frac{(L(z)+c_0)t}{(t+L(d))^2}\right)$$

for these z.

Thus for any $d\in\mathbb{F}_2^k$ and $t\in\mathbb{F}_{2^m}^*$ satisfying $t+L(d)\neq 0$,

$$\begin{aligned}&2^{k+1}-2\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}\\ &-\#\{z\in\mathbb{F}_2^k|t=\phi(z)+\phi(z+d)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z+d)\}\\ \leq\ & 2^{k+1}-4l+2.\end{aligned}$$

for the same reason as in Case 1.

Subcase 2.2: $\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right)=1\right\}=2^k$.

Then for any $z\in\mathbb{F}_2^k$, $\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right)=1$. In this subcase, we will only consider those z satisfying $z, z+d\in U_i$, then for these z, we have

$$\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right).$$

Since for any $d\in\mathbb{F}_2^k$ appears at least $2l$ times in the multiset $\{*\ z_1+z_2|(z_1,z_2)\in U_i\times U_i\ *\}$ for any U_i, then there are at least $2l$ different $z_1\in U_i$ such that $z_2=z_1+d\in U_i$. This means for any $d\in\mathbb{F}_2^k$,

$$\#\{z|z,z+d\in U_i\}\geq 2l.$$

Thus for any $d\in\mathbb{F}_2^k$ and $t\in\mathbb{F}_{2^m}^*$ satisfying $t+L(d)\neq 0$, we have

$$\begin{aligned}&2^{k+1}-2\#\left\{z\in\mathbb{F}_2^k\middle|\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}\\ &-\#\{z\in\mathbb{F}_2^k|t=\phi(z)+\phi(z+d)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z)\}+\#\{z\in\mathbb{F}_2^k|t=\phi(z+d)\}\\ \leq\ & 2^{k+1}-2\#\left\{z\middle|z,z+d\in U_i,\mathrm{Tr}_m\left(\frac{\phi(z)t}{(t+\phi(z)+\phi(z+d))^2}\right)=1\right\}-0+2\\ =\ & 2^{k+1}-2\#\left\{z\middle|z,z+d\in U_i,\mathrm{Tr}_m\left(\frac{(L(z)+c_i)t}{(t+L(d))^2}\right)=1\right\}+2\\ =\ & 2^{k+1}-2\#\{z|z,z+d\in U_i\}+2\\ \leq\ & 2^{k+1}-4l+2.\end{aligned}$$

All in all, $\Delta\leq 2^{k+1}-4l+2$ according to Proposition 3.1. □

B. Appendix B

A differentially 14-uniform $(8,5)$-function: Let $F_{8,5}(x,z)=\phi(z)I(x)$, where $I(x)$ is the Inverse function on $\mathbb{F}_{2^5}$ and $\phi:\mathbb{F}_2^3\to\mathbb{F}_{2^5}$ is presented by Table I:

TABLE I

z	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$\phi(z)$	1	α	α^2	α^3	α^4	α^{10}	α^{24}	α^{11}

where α is a defining element of $\mathbb{F}_{2^5}$.

A differentially 30-uniform $(10,6)$-function: Let $F_{10,6}(x,z)=\phi(z)I(x)$, where $I(x)$ is the Inverse function on $\mathbb{F}_{2^6}$ and $\phi:\mathbb{F}_2^4\to\mathbb{F}_{2^6}$ is presented by Table II:

TABLE II

z	$(0,0,0,0)$	$(0,0,0,1)$	$(0,0,1,0)$	$(0,0,1,1)$
$\phi(z)$	1	α^2+1	α^3+1	$\alpha^3+\alpha^2+1$
z	$(0,1,0,0)$	$(0,1,0,1)$	$(0,1,1,0)$	$(0,1,1,1)$
$\phi(z)$	α^4+1	$\alpha^4+\alpha^2+1$	$\alpha^4+\alpha^3+1$	$\alpha^4+\alpha^3+\alpha^2+\alpha$
z	$(1,0,0,0)$	$(1,0,0,1)$	$(1,0,1,0)$	$(1,0,1,1)$
$\phi(z)$	α^5+1	$\alpha^5+\alpha^2+1$	$\alpha^5+\alpha^3+1$	$\alpha^5+\alpha^3+\alpha^2+\alpha$
z	$(1,1,0,0)$	$(1,1,0,1)$	$(1,1,1,0)$	$(1,1,1,1)$
$\phi(z)$	$\alpha^5+\alpha^4+\alpha$	$\alpha^5+\alpha^4+\alpha^2+1$	$\alpha^5+\alpha^4+\alpha^3+1$	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$

where α is a defining element of $\mathbb{F}_{2^6}$.

A differentially 58-uniform $(12,7)$-function: Let $F_{12,7}(x,z)=\phi(z)I(x)$, where $I(x)$ is the Inverse function on $\mathbb{F}_{2^7}$ and $\phi:\mathbb{F}_2^5\to\mathbb{F}_{2^7}$ is presented by Table III:

TABLE III

z	$(0,0,0,0,0)$	$(0,0,0,0,1)$	$(0,0,0,1,0)$	$(0,0,0,1,1)$
$\phi(z)$	1	$\alpha^2+\alpha$	α^3+1	$\alpha^3+\alpha^2+1$
z	$(0,0,1,0,0)$	$(0,0,1,0,1)$	$(0,0,1,1,0)$	$(0,0,1,1,1)$
$\phi(z)$	α^4+1	$\alpha^4+\alpha^2+1$	$\alpha^4+\alpha^3+1$	$\alpha^4+\alpha^3+\alpha^2+\alpha$
z	$(0,1,0,0,0)$	$(0,1,0,0,1)$	$(0,1,0,1,0)$	$(0,1,0,1,1)$
$\phi(z)$	$\alpha^5+\alpha$	$\alpha^5+\alpha^2+\alpha$	$\alpha^5+\alpha^3+1$	$\alpha^5+\alpha^3+\alpha^2+\alpha$
z	$(0,1,1,0,0)$	$(0,1,1,0,1)$	$(0,1,1,1,0)$	$(0,1,1,1,1)$
$\phi(z)$	$\alpha^5+\alpha^4+\alpha$	$\alpha^5+\alpha^4+\alpha^2+1$	$\alpha^5+\alpha^4+\alpha^3+\alpha$	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$
z	$(1,0,0,0,0)$	$(1,0,0,0,1)$	$(1,0,0,1,0)$	$(1,0,0,1,1)$
$\phi(z)$	$\alpha^6+\alpha$	$\alpha^6+\alpha^2+1$	$\alpha^6+\alpha^3+1$	$\alpha^6+\alpha^3+\alpha^2+1$
z	$(1,0,1,0,0)$	$(1,0,1,0,1)$	$(1,0,1,1,0)$	$(1,0,1,1,1)$
$\phi(z)$	$\alpha^6+\alpha^4+1$	$\alpha^6+\alpha^4+\alpha^2+1$	$\alpha^6+\alpha^4+\alpha^3+1$	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+1$
z	$(1,1,0,0,0)$	$(1,1,0,0,1)$	$(1,1,0,1,0)$	$(1,1,0,1,1)$
$\phi(z)$	$\alpha^6+\alpha^5+1$	$\alpha^6+\alpha^5+\alpha^2+1$	$\alpha^6+\alpha^5+\alpha^3+1$	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+1$
z	$(1,1,1,0,0)$	$(1,1,1,0,1)$	$(1,1,1,1,0)$	$(1,1,1,1,1)$
$\phi(z)$	$\alpha^6+\alpha^5+\alpha^4+1$	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+1$	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+1$	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$

where α is a defining element of $\mathbb{F}_{2^7}$.