IEICE TRANS. FUNDAMENTALS, VOL.E103–A, NO.6 JUNE 2020

LETTER

A New Construction of $(m + k, m)$-Functions with Low Differential Uniformity*

Tailin NIU[†], **Xi CHEN**[†], ***Nonmembers***, **Longjiang QU**[†,††a)], ***Member***, ***and*** **Chao LI**[†], ***Nonmember***

SUMMARY $(m + k, m)$-functions with good cryptographic properties when $1 \leq k < m$ play an important role in several block ciphers. In this paper, based on the method introduced by Carlet et al. in 2018, we construct infinite families of $(m + k, m)$-functions with low differential uniformity by constructing a class of pairwise disjoint special subsets in $\mathbb{F}_2^k$. Such class of subsets U_i are chosen to generate multisets such that all elements in $\mathbb{F}_2^k$ appears as many times as possible in each of these multisets. We construct explicitly such kind of special subsets by linearized polynomials, and provide differentially Δ-uniform $(m + k, m)$-functions with $\Delta < 2^{k+1}$, $k \leq m - 2$. Specifically when $k = m - 2$, the differential uniformity of our functions are lower than the function constructed by Carlet et al. The constructed functions provide more choices for the design of Feistel ciphers.

key words: *substitution boxes, Feistel structures, differential uniformity*

1. Introduction

Substitution boxes (S-boxes) play an important role in many block ciphers since they are the only nonlinear component and 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 $\mathbb{F}_2^m$, which are also called (n, m)-*functions* [14]. Permutations with $n = m$ are widely used in the Substitution-Permutation-Network (SPN) structure as S-boxes such as the AES [11], Serpent [1], PRESENT [3], MISTY [16], LED [13] and Kuznyechik [12]. Studies on (n, n)-permutations with good cryptographic properties were very active in the last decade, please refer to [2], [5], [6], [9], [20]–[24] and the references therein. However, (n, m)-functions with $m < n$ or even $m > n$ can also be used in the Feistel structure as S-boxes. For example, the DES cipher has eight S-boxes each mapping 6 bits to 4 bits. Compared with (n, n)-permutations, little theoretical work has been done on (n, m)-functions with good cryptographic properties when $\frac{n}{2} < m < n$.

In order to prevent various attacks on the cipher, such (n, m)-functions are required to have low differential uniformity [19], high nonlinearity [19] and high algebraic degree [17]. Since we mainly focus on the case $n > m$ here, we let $n = k + m$ with $k \geq 1$. According to Nyberg's results [10], [18], the differential uniformity of $(m+k, m)$-functions with $m > k \geq 1$ is bounded below by $2^k + 2$, which is called *Nyberg's bound*. An (n, n)-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 achieve Nyberg's bound which is 4. Very recently, Carlet et al. [8] introduced a method to construct $(m+k, m)$-functions $(1 \leq k \leq m - 1)$ of the form $F(x, z) = \phi(z)I(x)$ with differential uniformity $\Delta < 2^{k+1}$, where $I(x)$ is the (m, m)-inverse function and $\phi(z)$ is a (k, m)-function. Then for $k = m - 1$, they constructed an infinite family of $(m + k, m)$-functions achieveing Nyberg's bound, while for $k \leq m - 2$, they introduced a class of special subsets to construct infinite families of low differential uniformity functions (see Proposition 2.1 for details). However, for the latter case, they only gave one specific construction with $k = m - 2$ (see Proposition 2.2). As pointed out in [8], it is still an interesting question to construct explicit differentially Δ-uniform $(m + k, m)$-functions with $2 \leq k \leq m - 3$ and $\Delta < 2^{k+1}$.

In this paper, we construct special sets suitable for Proposition 2.1 by linearized polynomials. These sets lead to specific families of $(m + k, m)$-functions with differential uniformity $\Delta < 2^{k+1}$, high nonlinearity and not too low algebraic degree when $k \leq m - 2$. Thus we partly answer the above interesting quesiton. Even when $k = m - 2$, our constructions have better cryptographic properties than the function constructed in [8]. The constructed functions in this paper provide more choices for the design of Feistel ciphers.

2. Preliminaries

In this section, we give some necessary definitions and notions related to (n, m)-functions and then recall the previous results.

2.1 Necessary Definitions

Let $\mathbb{F}_{2^n}$ be an extension field of the finite field $\mathbb{F}_2$. Let $\Gamma(x) \in \mathbb{F}_2[x]$ be a primitive monic polynomial of degree n and α be a root of $\Gamma(x)$ in its splitting field. Then

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

Manuscript received March 16, 2019.
Manuscript revised January 10, 2020.

[†]The authors are with the Department of Mathematics, National University of Defense Technology, Changsha, 410073, China.
[††]The author is also with the State Key Laboratory of Cryptology, Beijing, 100878, China.

*This work is supported by the Nature Science Foundation of China (NSFC) under Grant 11531002, 61722213, National Key R&D Program of China (No. 2017YFB0802001), and the Open Foundation of State Key Laboratory of Cryptology.

a) E-mail: ljqu_happy@hotmail.com (Corresponding author)

DOI: 10.1587/transfun.2019EAL2030

For any $a = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in \mathbb{F}_{2^n}$, the mapping $a \to \vec{a} := (a_0, a_1, \cdots, a_{n-1})^{\mathrm{T}}$ is a bijection from $\mathbb{F}_{2^n}$ to the linear space $\mathbb{F}_2^n$. Thus, the finite field $\mathbb{F}_{2^n}$ is also viewed as the linear space $\mathbb{F}_2^n$ over $\mathbb{F}_2$ [15, Definition 1.83]. Throughout this note, we will switch between these two points of view without explanation if the context is clear. The set of all nonzero elements of $\mathbb{F}_{2^n}$ (resp. $\mathbb{F}_2^n$) is denoted by $\mathbb{F}_{2^n}^*$ (resp. $\mathbb{F}_2^{n*}$). In the note, we always define $I(0) = 0$ for the multiplicative inverse function $I(x) = 1/x$. For the convenience and clarity, the zero vector in a linear space V is denoted by 0_V. We use $\mathrm{Span}(A)$ to denote the linear span of a set A in $\mathbb{F}_2^n$. A polynomial of the form

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{2^i}$$

with coefficients in $\mathbb{F}_{2^n}$ is called a *linearized polynomial* over $\mathbb{F}_{2^n}$. If $L(x)$ permutes $\mathbb{F}_{2^n}$, the unique polynomial $L^{-1}(x)$ over $\mathbb{F}_{2^n}$ such that $L\left(L^{-1}(x)\right) \equiv L^{-1}(L(x)) \equiv x \pmod{x^{2^n} - x}$ is called *the compositional inverse* of $L(x)$.

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

$$\begin{aligned} F(x) &= (f_1(x), \ldots, f_m(x)) \\ &= \left(\sum_{P \subseteq \{1,2,\ldots,n\}} b_{1,P} \Big(\prod_{i \in P} x_i \Big), \ldots, \sum_{P \subseteq \{1,2,\ldots,n\}} b_{m,P} \Big(\prod_{i \in P} x_i \Big) \right) \\ &= \sum_{P \subseteq \{1,2,\ldots,n\}} a_P \Big(\prod_{i \in P} x_i \Big), \end{aligned} \tag{1}$$

where $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, a_P = (b_{1,P}, \ldots, b_{m,P}) \in \mathbb{F}_2^m$ and the algebraic normal form of $f_j(x)$ (the j-th coordinate function of $F(x)$, $1 \le j \le m$) is defined by $\sum_{P \subseteq \{1,2,\ldots,n\}} b_{j,P} \Big(\prod_{i \in P} x_i \Big)$.

The *algebraic degree* of an (n, m)-function is defined by the global degree of its ANF:

$$d^\circ(F) = \max \{\#P, \text{ where } a_P \neq 0\},$$

where $\#P$ denotes the cardinality of a set P.

Let F be an (n, m)-function. The *differential uniformity* of F is defined as:

$$\Delta_F = \max_{a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^m} \# \left\{ x \in \mathbb{F}_2^n \mid F(x + a) + F(x) = b \right\}.$$

The *Walsh transform* $F^{\mathcal{W}} : \mathbb{F}_2^n \times \mathbb{F}_2^{m*} \to \mathbb{C}$ of F is defined by:

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

where "$\cdot$" denotes the inner product in $\mathbb{F}_2^n$.

The *nonlinearity* of F is defined as

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

The nonlinearity of (n, m)-functions is bounded above by $2^{n-1} - 2^{n/2-1}$ according to the Parseval identity $\sum_{u \in \mathbb{F}_2^n} F^{\mathcal{W}}(u, v)^2 = 2^{2n}$ and the fact that the maximum value of a list of real numbers must not be less than their average.

2.2 Previous Results

Very recently, Carlet et al. [8] proposed a new method to construct infinite families of $(m + k, m)$-functions with low differential uniformity.

Proposition 2.1. *[8, Proposition 4.6] Let m, l be positive integers and $1 \le k \le m - 2$. Let U_i $(1 \le i \le m - k - 1)$ be disjoint sets in $\mathbb{F}_2^k$ satisfying $\sum_{i=1}^{m-k-1} \#U_i \le 2^{k-2} - l$ 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

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

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

According to Proposition 2.1, the problem of constructing $(m + k, m)$-functions with low differential uniformity $\Delta < 2^{k+1}$ was transformed to the problem of constructing these suitable special sets. Furthermore, the differential uniformity of such functions are highly depending on the properties of the constructed sets.

In the case $k = m - 2$, these pairwise disjoint sets U_i become one set U_1. According to Proposition 2.1, an infinite family of $(2m - 2, m)$-functions with $\Delta \le 2^{m-1} - 2^{m-6} + 2$ and algebraic degree $m + 5$ for any $m \ge 8$ was constructed.

Proposition 2.2. *[8, Proposition 4.7] Let $m \ge 8$ 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 $z_i, 1 \le i \le 6$ 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 $\Delta \le 2^{m-1} - 2^{m-6} + 2$ and the algebraic degree of F is $m + 5$.

Let

$$U_1 = \left\{ (x, 0_{\mathbb{F}_2^3}, y) | x \in \mathbb{F}_2^3, y \in \mathbb{F}_2^{m-8} \right\} \bigcup \left\{ (0_{\mathbb{F}_2^3}, x, y) | x \in \mathbb{F}_2^3, y \in \mathbb{F}_2^{m-8} \right\}.$$

Then the $\phi(z)$ in Proposition 2.2 can be expressed by

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

3. Construction of Special Sets

In this section, we generalize the set $U_1 \subseteq \mathbb{F}_2^{m-2}$ in Proposition 2.2 and construct pairwise disjoint special sets $U_i \subseteq \mathbb{F}_2^k$, where k is not necessary equal to $m-2$. We first give a useful basic lemma.

Lemma 3.1. *For $j = 1, 2$, let k_j, l_j be positive integers satisfying $k_j \geq 4$, and A_j be a set with elements in $\mathbb{F}_2^{k_j}$ such that any element in $\mathbb{F}_2^{k_j}$ appears at least $2l_j$ times in the multiset $\{* z_1 + z_2 | (z_1, z_2) \in A_j \times A_j *\}$. Define*

$$A = \{(x, y) \mid x \in A_1, y \in A_2\} \subseteq \mathbb{F}_2^{k_1+k_2}.$$

Then any element in $\mathbb{F}_2^{k_1+k_2}$ appears at least $4l_1l_2$ times in the multiset

$$\{* z_1 + z_2 \mid (z_1, z_2) \in A \times A *\}.$$

Proof: According to the assumption, $x' \in \mathbb{F}_2^{k_1}$ has at least $2l_1$ orderly addictive decompositions in A_1. Thus for each orderly addictive decomposition of $y' \in \mathbb{F}_2^{k_2}$ in A_2, the element $(x', y') \in \mathbb{F}_2^{k_1+k_2}$ has at least $2l_1$ orderly addictive decompositions. Since $y' \in \mathbb{F}_2^{k_2}$ have at least $2l_2$ orderly addictive decompositions in A_2, we obtain that $(x', y') \in \mathbb{F}_2^{k_1+k_2}$ has at least $4l_1l_2$ orderly addictive decompositions in A. □

We can generalize the set U_1 in Proposition 2.2. By linearized polynomials, we construct pairwise disjoint sets $U_i \subseteq \mathbb{F}_2^k$ in the following two propositions.

Proposition 3.2. *Let m, k, s, t be positive integers such that $1 \leq k \leq m-2$, $2 \leq t$ and $2 \leq s \leq 2^{t-1}$. Assume $L_{i,j}(x)$ are linearized polynomials over $\mathbb{F}_{2^t}$ satisfying that $(L_{i_1,j_1} + L_{i_2,j_2})(x)$ is a permutation for any $(i_1, j_1) \neq (i_2, j_2)$ (i.e., $i_1 \neq i_2$ or $j_1 \neq j_2$), where $1 \leq i \leq m-k-1, 1 \leq j \leq s$. Define the sets*

$$U_i' = \bigcup_{j=1}^{s} W_{i,j}',$$

where

$$W_{i,j}' = \left\{(x, L_{i,j}(x)) \mid x \in \mathbb{F}_2^{t*}\right\} \subseteq \mathbb{F}_2^{2t}.$$

Then U_i' $(1 \leq i \leq m-k-1)$ are pairwise disjoint sets in $\mathbb{F}_2^{2t}$, $\sum_{i=1}^{m-k-1} \#U_i' = (2^t-1)s(m-k-1)$ and for any U_i', all elements in $\mathbb{F}_2^{2t}$ appear at least $s(s-1)$ times in the multiset

$$T_i' = \left\{* z_1 + z_2 | (z_1, z_2) \in U_i' \times U_i' *\right\}.$$

Proof: We first show that U_i' $(1 \leq i \leq m-k-1)$ are pairwise disjoint sets in $\mathbb{F}_2^{2t}$ satisfying

$$\sum_{i=1}^{m-k-1} \#U_i' = (2^t-1)s(m-k-1).$$

Notice that $(L_{i_1,j_1} + L_{i_2,j_2})(x)$ is a permutation for any $(i_1, j_1) \neq (i_2, j_2)$. Then $L_{i_1,j_1}(x) = L_{i_2,j_2}(x)$ if and only if $x = 0$, and thus we have $W_{i_1,j_1}' \bigcap W_{i_2,j_2}' = \emptyset$. Therefore, $U_i' = \bigcup_{j=1}^{s} W_{i,j}'$ $(1 \leq i \leq m-k-1)$ are pairwise disjoint sets and $\sum_{i=1}^{m-k-1} \#U_i' = (2^t-1)s(m-k-1)$.

Secondly, we prove that any element $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least $s(s-1)$ times in the multiset T_i', where $x', x'' \in \mathbb{F}_2^t$. It is clear that $0_{\mathbb{F}_2^{2t}} \notin U_i'$. The rest of proof is divided into three cases.

Case 1: $(x', x'') = 0_{\mathbb{F}_2^{2t}}$.

Since $0_{\mathbb{F}_2^{2t}} = z + z$ holds for any $z \in U_i'$, $0_{\mathbb{F}_2^{2t}}$ appears at least $\#U_i'$ times in the multiset T_i'. Clearly we have $\#U_i' = (2^t-1)s \geq (s-1)s$, where the inequality holds since $2 \leq s \leq 2^{t-1}$.

Case 2: $(x', x'') \notin \left\{0_{\mathbb{F}_2^{2t}}\right\} \bigcup U_i'$.

We first prove that for any $j_1 \neq j_2$, $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least 2 times in the multiset

$$\left\{* z_1 + z_2 \mid (z_1, z_2) \in W_{i,j_1}' \bigcup W_{i,j_2}' \times W_{i,j_1}' \bigcup W_{i,j_2}' *\right\}.$$

Without lost of generality, we assume $j_1 = 1, j_2 = 2$ here. Since $(x', x'') \notin \left\{0_{\mathbb{F}_2^{2t}}\right\} \bigcup U_i'$, the addictive decomposition of (x', x'') into two elements in $W_{i,1}' \bigcup W_{i,2}'$ is equivalent to the following linear equation system:

$$\begin{cases} x_1 + x_2 = x' \\ L_{i,1}(x_1) + L_{i,2}(x_2) = x'', \end{cases} \tag{2}$$

where $x_1, x_2 \in \mathbb{F}_2^{t*}$ are unknowns. Plugging $x_1 = x_2 + x'$ and $x_2 = x_1 + x'$ into the second equation of Eq. (2) respectively, we obtain

$$\begin{cases} x_1 = (L_{i,1} + L_{i,2})^{-1}(L_{i,2}(x') + x'') \\ x_2 = (L_{i,1} + L_{i,2})^{-1}(L_{i,1}(x') + x''), \end{cases} \tag{3}$$

where $(L_{i,1} + L_{i,2})^{-1}(x)$ denotes the compositional inverse of $(L_{i,1} + L_{i,2})(x)$. Since $(x', x'') \notin \left\{0_{\mathbb{F}_2^{2t}}\right\} \bigcup U_i'$, we have $x_1, x_2 \neq 0_{\mathbb{F}_2^t}$ according to Eq. (3). Then we obtain two orderly addictive decompositions

$$\begin{aligned} (x', x'') &= (x_1, L_{i,1}(x_1)) + (x_2, L_{i,2}(x_2)) \\ &= (x_2, L_{i,2}(x_2)) + (x_1, L_{i,1}(x_1)), \end{aligned}$$

where $(x_1, L_{i,1}(x_1)) \in W_{i,1}'$ and $(x_2, L_{i,2}(x_2)) \in W_{i,2}'$. That is, $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least 2 times in the multiset

$$\left\{* z_1 + z_2 \mid (z_1, z_2) \in W_{i,1}' \bigcup W_{i,2}' \times W_{i,1}' \bigcup W_{i,2}' *\right\}.$$

After that, we prove $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least

$s(s-1)$ times in the multiset T'_i. Actually, there are $\binom{s}{2}$ combinations of $W'_{i,j_1} \bigcup W'_{i,j_2}$ for any $1 \le j_1 \ne j_2 \le s$. Notice that $U'_i = \bigcup_{j=1}^{s} W'_{i,j}$ and $W'_{i_1,j_1} \bigcap W'_{i_2,j_2} = \emptyset$ for any $(i_1, j_1) \ne (i_2, j_2)$. Thus we have $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least $2\binom{s}{2} = s(s-1)$ times in the multiset T'_i.

Case 3: $(x', x'') \in U'_i$.

Without lost of generality, assume that $(x', x'') \in W'_{i,1}$. On one hand, we show that $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least $2^t - 2$ times in the multiset

$$\left\{ * \, z_1 + z_2 \mid (z_1, z_2) \in W'_{i,1} \times W'_{i,1} \, * \right\}.$$

For any $z \in \mathbb{F}_2^{t*} \setminus \{x'\}$, it is clear that $(z, L_{i,1}(z))$, $(z + x', L_{i,1}(z + x')) \in W'_{i,1}$ are distinct and

$$(x', L_{i,1}(x')) = (z, L_{i,1}(z)) + (z + x', L_{i,1}(z + x')).$$

Thus $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least $2^t - 2$ times in the multiset $\{* \, z_1 + z_2 | (z_1, z_2) \in W'_{i,1} \times W'_{i,1} \, *\}$. On the other hand, since $(x', x'') \notin \left\{0_{\mathbb{F}_2^{2t}}\right\} \bigcup \bigcup_{j=2}^{s} W'_{i,j}$, clearly $(x', x'') \in \mathbb{F}_2^{2t}$ appears at least $(s-1)(s-2)$ times in the multiset

$$\left\{ * \, z_1 + z_2 \mid (z_1, z_2) \in \bigcup_{j=2}^{s} W'_{i,j} \times \bigcup_{j=2}^{s} W'_{i,j} \, * \right\}$$

similarly to Case 2. Thus (x', x'') appears at least $2^t - 2 + (s-1)(s-2) \ge s(s-1)$ times in the multiset T'_i, where the inequality holds since $2 \le s \le 2^{t-1}$.

All in all, U'_i $(1 \le i \le m-k-1)$ are pairwise disjoint in $\mathbb{F}_2^{2t}$, $\sum_{i=1}^{m-k-1} \#U'_i = (2^t - 1)s(m-k-1)$ and for any U'_i, any element in $\mathbb{F}_2^{2t}$ appears at least $s(s-1)$ times in the multiset T'_i. □

For each $1 \le i \le m-k-1$, if we let $A_1 = U'_i \subseteq \mathbb{F}_2^{2t}$, $A_2 = \mathbb{F}_2^{k-2t}$ in Lemma 3.1, then we have the following proposition.

Proposition 3.3. *For any $1 \le i \le m-k-1, 1 \le j \le s$, let $L_{i,j}$ be defined as in Proposition 3.2. Define the sets*

$$U_i = \bigcup_{j=1}^{s} W_{i,j},$$

where

$$W_{i,j} = \left\{ (x, L_{i,j}(x), y) \mid x \in \mathbb{F}_2^{t*}, y \in \mathbb{F}_2^{k-2t} \right\} \subseteq \mathbb{F}_2^k.$$

Then U_i $(1 \le i \le m-k-1)$ are pairwise disjoint sets in $\mathbb{F}_2^k$ satisfying $\sum_{i=1}^{m-k-1} \#U_i = 2^{k-2t}(2^t - 1)s(m-k-1)$ and such that, for any U_i, any element in $\mathbb{F}_2^k$ appears at least $2^{k-2t}s(s-1)$ times in the multiset $\{* \, z_1 + z_2 | (z_1, z_2) \in U_i \times U_i \, *\}$.

Remark 3.4. *Let $a_{i,j} \in \mathbb{F}_{2^t}$ $(1 \le i \le m-k-1, 1 \le j \le s)$ be pairwise distinct. Let $L_{i,j}(x) = a_{i,j}x^{2^d} + G(x) \in \mathbb{F}_{2^t}[x]$, where d is an integer and $G(x)$ is a linearized polynomial over $\mathbb{F}_{2^t}$. It is easy to verify that $(L_{i_1,j_1} + L_{i_2,j_2})(x)$ is a permutation for any $(i_1, j_1) \ne (i_2, j_2)$.*

4. Low Differential Uniformity $(m + k, m)$-Functions

Now we use the new construction of special sets to build low differential uniformity $(m + k, m)$-functions in the form $F(x, z) = \phi(z)I(x)$, where k is not necessarily equal to $m-2$. The following theorem is a generalization of Proposition 2.2.

Theorem 4.1. *Let m, k, t, s, d be integers satisfying $1 \le k \le m-2, 1 \le t \le \lfloor k/2 \rfloor, 2 \le s \le \min\left\{2^{t-1}, 2^t/(m-k-1)\right\}$. Assume $a_{i,j} \in \mathbb{F}_2^t$ satisfying $a_{i_1,j_1} \ne a_{i_2,j_2}$ for any $(i_1, j_1) \ne (i_2, j_2)$. Let*

$$U_i = \bigcup_{j=1}^{s} W_{i,j} \subseteq \mathbb{F}_2^k,$$

where for any $1 \le i \le m-k-1, 1 \le j \le s$,

$$W_{i,j} = \left\{ (x, a_{i,j}x^{2^d} + G(x), y) \mid x \in \mathbb{F}_2^{t*}, y \in \mathbb{F}_2^{k-2t} \right\} \subseteq \mathbb{F}_2^k$$

and $G(x)$ is a fixed linearized polynomial over $\mathbb{F}_{2^t}$.
Consider the function $F : \mathbb{F}_2^{m+k} \to \mathbb{F}_2^m$ in the form $F(x, z) = \phi(z)I(x)$. Here $I(x)$ is the (m, m)-inverse function and $\phi : \mathbb{F}_2^k \to \mathbb{F}_{2^m}$ is defined as follows:

$$\phi(z) = \begin{cases} \left(z, 0_{\mathbb{F}_2^{m-k}}\right) + e_{m+1-i}, & when \quad z \in U_i; \\ \left(z, 0_{\mathbb{F}_2^{m-k}}\right) + e_{k+1}, & when \quad z \in \mathbb{F}_2^k \setminus \bigcup_{i=1}^{m-k-1} U_i, \end{cases}$$

where $e_1, e_2, ..., e_m$ denote the standard basis of $\mathbb{F}_2^m$. Then F is a differentially Δ-uniform function with $\Delta \le 2^{k+1} - 4l_{m,k}(s,t) + 2$ and the algebraic degree of F is at least m, where $l_{m,k}(s,t)$

$$= \min\left\{2^{k-2} - 2^{k-2t}(2^t - 1)s(m-k-1), 2^{k-2t-1}s(s-1)\right\}$$

is a positive integer.

Proof: Since $s \le 2^t/(m-k-1)$, there are enough distinct $a_{i,j} \in \mathbb{F}_2^t$ to constitute U_i. Let $L_{i,j}(x) = a_{i,j}x^{2^d} + G(x)$ in Proposition 3.3 and we obtain that $(L_{i_1,j_1} + L_{i_2,j_2})(x)$ is a permutation for any $(i_1, j_1) \ne (i_2, j_2)$ according to Remark 3.4. Furthermore, according to Proposition 3.3, we have

$$\sum_{i=1}^{m-k-1} \#U_i = 2^{k-2t}(2^t - 1)s(m-k-1) \le 2^{k-2} - l_{m,k}(s,t)$$

and for any U_i, any element in $\mathbb{F}_2^k$ appears at least

$$2^{k-2t}s(s-1) \ge 2l_{m,k}(s,t)$$

times in the multiset $\{* \, z_1 + z_2 \mid (z_1, z_2) \in U_i \times U_i \, *\}$.

Thus we only need to prove the last condition in Proposition 2.1, i.e., $\mathrm{Rank}\{\phi(z)|z \in \mathbb{F}_2^k\} = m$. For clarity, here we use $e_1^{(m)}, e_2^{(m)}, ..., e_m^{(m)}$ denote the standard basis of $\mathbb{F}_2^m$ and $e_1^{(k)}, e_2^{(k)}, ..., e_k^{(k)}$ denote the standard basis of $\mathbb{F}_2^k$. Firstly, we prove $e_{k+1}^{(m)}, e_{k+2}^{(m)}, \ldots, e_m^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$. Notice that $0_{\mathbb{F}_2^k} \in \mathbb{F}_2^k \setminus \bigcup_{i=1}^{m-k-1} U_i$, we have $\phi(0_{\mathbb{F}_2^k}) = e_{k+1}^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$. Then for each $1 \le i \le m-k-1$, let $\beta_i \in U_i$. Since $\beta_i \in U_i$ appears at least $2^{k-2t}s(s-1) \ge 1$ times in the multiset $\{* z_1 + z_2 \mid (z_1, z_2) \in U_i \times U_i *\}$, there exists $\theta_i, \eta_i \in U_i$ such that $\beta_i = \theta_i + \eta_i$. Thus for any $1 \le i \le m-k-1$, we have

$$\begin{aligned} e_{m+1-i}^{(m)} &= \left(\beta_i, 0_{\mathbb{F}_2^{m-k}}\right) + e_{m+1-i}^{(m)} + \left(\theta_i, 0_{\mathbb{F}_2^{m-k}}\right) + e_{m+1-i}^{(m)} \\ &\quad + \left(\eta_i, 0_{\mathbb{F}_2^{m-k}}\right) + e_{m+1-i}^{(m)} \\ &= \phi(\beta_i) + \phi(\theta_i) + \phi(\eta_i) \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}, \end{aligned}$$

i.e., $e_{k+2}^{(m)}, \ldots, e_m^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$. Secondly, we prove $e_1^{(m)}, e_2^{(m)}, \ldots, e_k^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$. For each $1 \le j \le k$, if there exists $1 \le i_j \le m-k-1$ such that $e_j^{(k)} \in U_{i_j}$, then we have $e_j^{(m)} = \phi(e_j^{(k)}) + e_{m+1-i_j}^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$, where $\phi(e_j^{(k)}) + e_{m+1-i_j}^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$ holds since $e_{k+1}^{(m)}, e_{k+2}^{(m)}, \ldots, e_m^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$. Otherwise, we have $e_j^{(k)} \in \mathbb{F}_2^k \setminus \bigcup_{i=1}^{m-k-1} U_i$ and $e_j^{(m)} = \phi(e_j^{(k)}) + e_{k+1}^{(m)} \in \mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$. Thus all the standard basis of $\mathbb{F}_2^m$ are contained in $\mathrm{Span}\left\{\phi(z)\,|z \in \mathbb{F}_2^k\right\}$. This means $\mathrm{Rank}\{\phi(z)|z \in \mathbb{F}_2^k\} = m$.

All in all, F is a differentially Δ-uniform function with $\Delta \le 2^{k+1} - 4l_{m,k}(s,t) + 2$ according to Proposition 2.1. Since the algebraic degree of $I(x)$ is $m-1$, the algebraic degree of the $(m+k, m)$-function $F(x,z) = \phi(z)I(x)$ is at least m. □

Remark 4.2. *Any parameters t and s satisfying $l_{m,k}(s,t) \ge 1$ can be used to build differentially Δ-uniform $(m+k, m)$-functions with $\Delta \le D_{m,k}(s,t) = 2^{k+1} - 4l_{m,k}(s,t) + 2$, where*

$$\begin{aligned} l_{m,k}(s,t) &= \min\{f_{m,k}(s,t), g_{m,k}(s,t)\} \\ f_{m,k}(s,t) &= 2^{k-2} - 2^{k-2t}(2^t - 1)s(m-k-1), \\ g_{m,k}(s,t) &= 2^{k-2t-1}s(s-1). \end{aligned}$$

Algorithm 1 provides a fast way to obtain the minimal value of $D_{m,k}(s,t)$ for fixed m, k. For any fixed t, regard $f_{m,k}(s,t)$ and $g_{m,k}(s,t)$ as functions with independent variable s. Since $f_{m,k}(s,t)$ monotonically decreases while $g_{m,k}(s,t)$ increases as s increases from 2 to c, $l_{m,k}(s,t)$ will be possible to reach its maximum only when s is the boundary point or near the positive solution of the equation $f_{m,k}(s,t) = g_{m,k}(s,t)$. Thus only when $s \in H_t$ (see line 7 of Algorithm 1), the value of $D_{m,k}(s,t)$ will be possible to reach its minimal value for each m, k, t. Furthermore, we find most of the output $T_{m,k}$ is equal or close to $\lfloor k/2 \rfloor$ for each m, k.

Algorithm 1 The minimal value of $D_{m,k}(s,t)$

1: **Input** m, k.
2: $l_{m,k} := 0$;
3: **for** t in $[1..\lfloor k/2 \rfloor]$ **do**
4: $\quad c := \min\left\{2^{t-1}, 2^t/(m-k-1)\right\}$;
5: $\quad b := 1/2 - (2^t - 1)(m-k-1)$; $s_1 := b + \sqrt{2^{2t-1} + b^2}$;
6: $\quad H_t' := \{2, c, \lceil s_1 \rceil, \lfloor s_1 \rfloor\}$; $H_t := \left\{x \in H_t' \mid 2 \le x \le c\right\}$;
7: $\quad$ **for** s in H_t **do**
8: $\quad\quad$ **if** $l_{m,k}(s,t) \ge l_{m,k}$ **then**
9: $\quad\quad\quad l_{m,k} := l_{m,k}(s,t)$; $S_{m,k} := s$; $T_{m,k} := t$;
10: $\quad\quad$ **end if**
11: $\quad$ **end for**
12: **end for**
13: **if** $l_{m,k} \ge 1$ **then**
14: $\quad D_{m,k} := 2^{k+1} - 4l_{m,k} + 2$;
15: $\quad$ **Output** $D_{m,k}, S_{m,k}, T_{m,k}$.
16: **end if**

According to Algorithm 1, we calculate by Magma [4] the minimal upper bound of differential uniformity of specific $(m+k, m)$-functions constructed by Theorem 4.1 when $m \le 24$ (see Table 1). Based on these results, we obtain specific differentially Δ-uniform $(m+k, m)$-functions with $\Delta < 2^{k+1}$, $k \le m-2$ but k is close to $m-2$. As far as the authors know, this is the first time when specific Δ-uniform $(m+k, m)$-functions with $\Delta < 2^{k+1}$, $k < m-2$ are constructed.

The existence of differentially Δ-uniform $(m+k, m)$-

Table 1 The minimal upper bound $D_{m,k}$ of differential uniformity of $(m+k, m)$-functions constructed by Theorem 4.1.

$D_{m,k}$ m \ k	$m-2$	$m-3$	$m-4$	$m-5$
8	2^7-2	—	—	—
9	2^8-6	—	—	—
10	2^9-14	—	—	—
11	$2^{10}-30$	2^9-2	—	—
12	$2^{11}-82$	$2^{10}-6$	—	—
13	$2^{12}-166$	$2^{11}-22$	—	—
14	$2^{13}-362$	$2^{12}-46$	$2^{11}-2$	—
15	$2^{14}-726$	$2^{13}-94$	$2^{12}-6$	$2^{11}-2$
16	$2^{15}-1622$	$2^{14}-190$	$2^{13}-38$	$2^{12}-6$
17	$2^{16}-3246$	$2^{15}-418$	$2^{14}-78$	$2^{13}-22$
18	$2^{17}-6494$	$2^{16}-838$	$2^{15}-178$	$2^{14}-46$
19	$2^{18}-12990$	$2^{17}-1858$	$2^{16}-358$	$2^{15}-110$
20	$2^{19}-26218$	$2^{18}-3718$	$2^{17}-838$	$2^{16}-222$
21	$2^{20}-52438$	$2^{19}-7562$	$2^{18}-1678$	$2^{17}-446$
22	$2^{21}-105338$	$2^{20}-15126$	$2^{19}-3442$	$2^{18}-894$
23	$2^{22}-210678$	$2^{21}-30502$	$2^{20}-6886$	$2^{19}-1858$
24	$2^{23}-422278$	$2^{22}-610006$	$2^{21}-13942$	$2^{20}-3718$

$D_{m,k}$ m \ k	$m-6$	$m-7$	$m-8$	$m-9$	$m-10$
17	—	—	—	—	—
18	$2^{13}-10$	—	—	—	—
19	$2^{14}-22$	$2^{13}-2$	—	—	—
20	$2^{15}-58$	$2^{14}-6$	$2^{13}-2$	—	—
21	$2^{16}-118$	$2^{15}-38$	$2^{14}-6$	$2^{13}-2$	—
22	$2^{17}-262$	$2^{16}-78$	$2^{15}-22$	$2^{14}-6$	—
23	$2^{18}-526$	$2^{17}-178$	$2^{16}-46$	$2^{15}-22$	—
24	$2^{19}-1198$	$2^{18}-358$	$2^{17}-142$	$2^{16}-46$	$2^{15}-10$

Table 2 The differential uniformity Δ and nonlinearity NL of $(14, 8)$-functions constructed by Theorem 4.1 with $G(x) = 0, d = 1$.

$a_{1,1}$ and $a_{1,2}$	Δ	NL	$a_{1,1}$ and $a_{1,2}$	Δ	NL
Proposition 2.2	114	7954	α^3, α^6	116	7988
α, α^6	114	7988	$1, \alpha^4$	116	7984
$0, \alpha^6$	114	7980	$0, 1$	116	7980
$1, \alpha^5$	114	7976	$0, \alpha^3$	116	7980
α^2, α^5	114	7976	α^3, α^4	116	7980
α, α^4	114	7976	$1, \alpha^3$	116	7972
$0, \alpha^2$	114	7972	$1, \alpha^2$	116	7964
α, α^2	114	7972	α^5, α^6	116	7964
α^3, α^5	114	7972	$1, \alpha$	116	7960
α, α^5	114	7964	α^4, α^5	116	7956
α^4, α^6	114	7964	$0, \alpha^4$	118	7984
$\alpha^2, \alpha^6,$	114	7960	$\alpha^2, \alpha^4,$	118	7980
$0, \alpha^5$	114	7956	$1, \alpha^6$	118	7976
			$0, \alpha$	118	7964
			$\alpha^2, \alpha^3,$	118	7964
			α, α^3	118	7960

functions with $k = m-2, m \geq 8, \Delta < 2^{k+1}$ is unknown before [8]. The following examples show that even when $k = m-2$, our constructions have better cryptographic properties than the function constructed in Proposition 2.2.

Example 1. *Let* $m = 8, k = 6, d = 0$ *and* $G(x) = 0$ *in Theorem 4.1. By Algorithm 1 we pick* $t = T_{8,6} = 3$ *and* $s = S_{8,6} = 2$. *Then we have* $W_{1,1} = \left\{(x, a_{1,1}x) | x \in \mathbb{F}_2^{3*}\right\}$, $W_{1,2} = \left\{(x, a_{1,2}x) | x \in \mathbb{F}_2^{3*}\right\}$ *and* $U_1 = W_{1,1} \bigcup W_{1,2}$, *where* $a_{1,1} \neq a_{1,2}$. *Thus* $(14, 8)$*-functions with low differential uniformity are obtained by all possible combinations of* $a_{1,1} \neq a_{1,2} \in \mathbb{F}_{2^3}$ *(see Table 2).*

The differential uniformity and nonlinearity of the $(14, 8)$*-function constructed by Theorem 4.1 with parameters* $a_{1,1} = \alpha, a_{1,2} = \alpha^6$ *achieve* 114 *and* $7988 = 2^{13} - 204$ *respectively. It is an improvement comparing with* $7954 = 2^{13} - 238$, *which is the nonlinearity of the function constructed in Proposition 2.2. Furthermore, most of these functions in Table 2 are pairwise CCZ inequivalent, since it is well known that CCZ equivalence preserves the differential uniformity and the nonlinearity [7].*

Example 2. *Let* $m = 12, k = 10$. *By Algorithm 1, we pick* $t = T_{12,10} = 5$ *and* $s = S_{12,10} = 7$. *Then Theorem 4.1 builds differentially* Δ*-uniform* $(22, 12)$*-functions with* $\Delta \leq 2^{11}-82$. *However, the function constructed in Proposition 2.2 is only* $\Delta \leq 2^{11} - 62$.

References

[1] E. Biham, R. Anderson, and L. Knudsen, "Serpent: A new block cipher proposal," Fast Software Encryption, pp.222–238, Springer, 1998.

[2] C. Blondeau and K. Nyberg, "Perfect nonlinear functions and cryptography," Finite Fields and Their Applications, vol.32, pp.120–147, 2015.

[3] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," International Workshop on Cryptographic Hardware and Embedded Systems, pp.450–466, Springer, 2007.

[4] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," J. Symb. Comput., vol.24, no.3-4, pp.235–265, 1997.

[5] L. Budaghyan, T. Helleseth, N. Li, and B. Sun, "Some results on the known classes of quadratic APN functions," International Conference on Codes, Cryptology, and Information Security, pp.3–16, Springer, 2017.

[6] A. Canteaut, S. Duval, and L. Perrin, "A generalisation of dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}," IEEE Trans. Inf. Theory, vol.63, no.11, pp.7575–7591, Nov. 2017.

[7] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for des-like cryptosystems," Des. Codes Cryptogr., vol.15, no.2, pp.125–156, 1998.

[8] C. Carlet, X. Chen, and L. Qu, "Constructing infinite families of low differential uniformity (n, m)-functions with $m > n/2$," Des. Codes Cryptogr., vol.87, no.7, pp.1577–1599, 2019.

[9] C. Carlet, "Vectorial Boolean functions for cryptography," Boolean Models and Methods in Mathematics, Computer Science, and Engineering, vol.134, pp.398–469, 2010.

[10] C. Carlet, "Open questions on nonlinearity and on APN functions," International Workshop on the Arithmetic of Finite Fields, pp.83–107, Springer, 2014.

[11] J. Daemen and V. Rijmen, "Rijndael, the advanced encryption standard," Dr. Dobb's Journal, vol.26, no.3, pp.137–139, 2001.

[12] V. Dolmatov, "GOST R 34.12-2015: Block cipher "Kuznyechik"," RFC, vol.7801, pp.1–14, 2016.

[13] J. Guo, T. Peyrin, A. Poschmann, and M.J.B. Robshaw, "The LED block cipher," Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Proceedings, pp.326–341, Nara, Japan, 2011.

[14] L.R. Knudsen and M. Robshaw, The Block Cipher Companion, Springer Science & Business Media, 2011.

[15] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

[16] M. Matsui, "New block encryption algorithm misty," International Workshop on Fast Software Encryption, pp.54–68, Springer, 1997.

[17] Y. Nawaz, K.C. Gupta, and G. Gong, "Algebraic immunity of s-boxes based on power mappings: Analysis and construction," IEEE Trans. Inf. Theory, vol.55, no.9, pp.4263–4273, 2009.

[18] K. Nyberg, "Perfect nonlinear S-boxes," Advances in Cryptology — EUROCRYPT'91, pp.378–386, Springer, 1991.

[19] K. Nyberg, "S-boxes and round functions with controllable linearity and differential uniformity," International Workshop on Fast Software Encryption, pp.111–130, Springer, 1994.

[20] J. Peng, C.H. Tan, Q. Wang, J. Gao, and H. Kan, "More new classes of differentially 4-uniform permutations with good cryptographic properties," IEICE Trans. Fundamentals, vol.E101-A, no.6, pp.945–952, June 2018.

[21] A. Pott, "Almost perfect and planar functions," Des. Codes Cryptogr., vol.78, no.1, pp.141–195, 2016.

[22] L. Qu, Y. Tan, C. Li, and G. Gong, "More constructions of differentially 4-uniform permutations on $\mathbb{F}_2^{2k}$," Des. Codes Cryptogr., vol.78, no.2, pp.391–408, 2016.

[23] L. Qu, Y. Tan, C.H. Tan, and C. Li, "Constructing differentially 4-uniform permutations over $\mathbb{F}_2^{2k}$ via the switching method," IEEE Trans. Inf. Theory, vol.59, no.7, pp.4675–4686, 2013.

[24] D. Tang, C. Carlet, and X. Tang, "Differentially 4-uniform bijections by permuting the inverse function," Des. Codes Cryptogr., vol.77, no.1, pp.117–141, 2015.