On cryptographic parameters of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$

Jaeseong Jeong[1], Chang Heon Kim[1], Namhun Koo[2], Soonhak Kwon[1], and Sumin Lee[1]

Email: wotjd012321@naver.com, {chhkim,shkwon,dltnals816}@skku.edu, nhkoo@ewha.ac.kr

[1]Department of Mathematics, Sungkyunkwan University, Suwon, Korea

[2]Institute of Mathematical Sciences, Ewha Womans University, Seoul, Korea

Abstract

The differential uniformity, the boomerang uniformity, and the extended Walsh spectrum etc are important parameters to evaluate the security of S(substitution)-box. In this paper, we introduce efficient formulas to compute these cryptographic parameters of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$ over a finite field of $q = 2^n$ elements, where r is a positive integer and d is a positive divisor of $2^n - 1$. The computational cost of those formulas is proportional to d. We investigate differentially 4-uniform permutation polynomials of the form $x^r h(x^{(2^n-1)/3})$ and compute the boomerang spectrum and the extended Walsh spectrum of them using the suggested formulas when $6 \le n \le 12$ is even, where $d = 3$ is the smallest nontrivial d for even n. We also investigate the differential uniformity of some permutation polynomials introduced in some recent papers for the case $d = 2^{n/2} + 1$.

Keywords. Permutation Polynomials, Differential Uniformity, Boomerang Uniformity, Extended Walsh Spectrum, Differentially 4-Uniform Permutation Polynomials

Mathematics Subject Classification(2020) 94A60, 06E30

1 Introduction

Throughout this paper, $\mathbb{F}_{2^n}$ is the finite field of 2^n elements, $\mathbb{F}_{2^n}^*$ is the subset of nonzero elements of $\mathbb{F}_{2^n}$. For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we denote $\delta_F(a, b)$ with $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$ by the number of solutions of the equation $F(x) + F(x + a) = b$ and

$$\delta_F = \max_{a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}} \delta_F(a, b). \tag{1}$$

In this case, F is said to be *differentially δ_F-uniform.* Constructing an S-box with good cryptographic properties for symmetric cipher is essential to the security of the symmetric cryptography, and Nyberg[20] suggested to choose an S-box with low differential uniformity to avoid differential cryptanalysis. We call F *almost perfect nonlinear* (APN) if F is differentially 2-uniform, which is the optimal case for δ_F. Though S-Box does not need to be invertible, invertible S-Box has many advantages in symmetric cryptography. Several APN permutations are known when n is odd, and the inverse function $F(x) = x^{2^n-2} \in \mathbb{F}_{2^n}[x]$ is always APN for odd n. However, the situation for even n is quite different. It is known that there is no APN permutation if $n = 2, 4$, and a single example of APN permutation[5] is known for $n = 6$. However, at this moment, the existence of APN permutations for even $n \geq 8$ is still unsettled, and it is referred as the *Big APN Problem.*

Another important tool for cryptanalysis is the boomerang attack introduced by Wagner[22]. Recently, Cid et al.[8] introduced the boomerang connectivity table which contains the number of solutions of

$$F^{-1}(F(x) + a) + F^{-1}(F(x + b) + a) = b \qquad (a, b \in \mathbb{F}_{2^n})$$

for a permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, which is denoted by $\beta_F(a, b)$ in this paper. The boomerang uniformity of F, β_F, is defined as the maximum of $\beta_F(a, b)$ for all $a, b \in \mathbb{F}_{2^n}^*$, where the case $a = 0$ or $b = 0$ are excluded because $\beta_F(a, 0) = \beta_F(0, b) = q$ for all $a, b \in \mathbb{F}_{2^n}$. The boomerang uniformity of an S-box is related to the success probability of the boomerang attack, hence an S-box is suggested to have low boomerang uniformity. In [8], it is shown that $\beta_F \geq \delta_F$, and $\beta_F = 2$ if and only if $\delta_F = 2$ (i.e., F is APN). In constructing an S-box, the cases $n = 4$ and $n = 8$ are most preferred for implementations. However, when $n = 4$, there is no APN permutation and it is also proved[3] that there is no permutation with $\beta_F = 4$. When $n = 8$, we do not know the existence of a permutation F with $\delta_F = 2$ or $\beta_F = 4$, and the authors of [8] say that construction of a permutation polynomial F with $\beta_F = 4$ would be quite difficult. The result in [8] also says that a permutation of boomerang uniformity 4 needs to be differentially 4-uniform, i.e., $\beta_F = 4$ implies $\delta_F = 4$. There are several results[3, 16, 19] about the boomerang uniformity of the known differentially 4-uniform permutations. In [3, 16, 19], some permutations having boomerang uniformity 4 are found when $n \equiv 2 \pmod 4$. However, when $n \equiv 0 \pmod 4$, the lowest boomerang uniformity in the list is 6. Hence constructing a permutation polynomial of boomerang uniformity 4 when $4 \mid n$ is still an open problem.

To construct a permutation with low boomerang uniformity, we investigate boomerang uniformity of the known permutation polynomials. In particular, we consider permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$. Permutation polynomials of this form were first characterized by Wan and Lidl[23], and have since been widely studied[2, 10, 11, 12, 13, 14, 15, 16, 17, 18, 21, 25, 27]. In this paper, we introduce efficient formulas to compute differential uniformity and boomerang uniformity of permutation polynomials of this form. These formulas are more efficient when d is small. Since $3 \mid (2^n - 1)$ for even n, we investigate permutation polynomials of the form $x^r h(x^{(2^n-1)/3})$ for even $n \leq 10$. We also consider other important cryptographic parameters like the extended Walsh spectrum, the nonlinearity, the differential spectrum, and the boomerang spectrum for these permutation polynomials.

The rest of this paper is organized as follows. In section 2, we recall some known results about permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$ and cryptographic properties including the boomerang uniformity and the extended Walsh spectrum. In section 3, we give efficient formulas for computing cryptographic parameters introduced in section 2 of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$. In section 4, we investigate cryptographic parameters of differentially 4-uniform permutations of the form $x^r h(x^{(2^n-1)/3})$ using our formulas obtained in section 3, and we also investigate the differential uniformity of permutations of the form $x^r h(x^{2^{n/2}-1})$ in some recent papers for even $n \leq 10$. Finally we give a concluding remark in section 5.

2 Preliminaries

2.1 Permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$

In this subsection, we focus on permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$ introduced by Wan and Lidl[23]. We first introduce the following notations which are also used in [23].

Definition 1. *(Definition 1.1 of [23]) Let $d|(2^n-1)$ and g be a fixed primitive root of $\mathbb{F}_{2^n}$. Let $\omega_d = g^{(2^n-1)/d}$ be a primitive d-th root of unity in $\mathbb{F}_{2^n}$. A map $\psi : \mathbb{F}_{2^n}^* \mapsto (\mathbb{Z}/d\mathbb{Z})^+$ defined by*

$$\psi(a) \equiv Ind_g(a) \pmod{d}$$

where $Ind_g(a)$ is the residue class (b mod (2^n-1)) such that $a = g^b$.

Note that the following equation holds.

$$a^{(2^n-1)/d} = \omega_d^{\psi(a)}$$

With these notations, the following main theorem of [23] gives a characterization of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$.

Theorem 1. *(Theorem 1.2 of [23]) Let r be a positive integer, d be a positive divisor of 2^n-1. Let $h(x) \in \mathbb{F}_{2^n}[x]$. Then the polynomial $F(x) = x^r h(x^{(2^n-1)/d})$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if the following conditions are satisfied :*
(i) $\gcd(r, (2^n-1)/d) = 1$.
(ii) $h(\omega^i) \neq 0$ for all $0 \leq i < d$.
(iii) $\psi\left(\dfrac{h(\omega^i)}{h(\omega^j)}\right) \not\equiv r(j-i) \pmod{d}$ *for all* $0 \leq i < j < d$.

Park and Lee[21] introduced a simpler characterization of these permutation polynomials. This result is also found in [1, 24, 27].

Theorem 2. *(Lemma 2.1 of [27]) Let r be a positive integer, d be a positive divisor of 2^n-1 and $\mu_d = \{\alpha \in \mathbb{F}_{2^n}^* : \alpha^d = 1\}$. Let $h(x) \in \mathbb{F}_{2^n}[x]$. Then the polynomial $F(x) = x^r h(x^{(2^n-1)/d})$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if the following conditions are satisfied :*
(i) $\gcd(r, (2^n-1)/d) = 1$.
(ii) $x^r h(x)^{(2^n-1)/d}$ permutes μ_d.

There are many results on the permutation polynomials of this form, and several recent studies [2, 10, 11, 12, 13, 14, 15, 16, 17, 18] focus on the case $d = 2^{n/2}+1$.

For any permutation polynomial, one can express the polynomial as the form $x^r h(x^{(2^n-1)/d})$ for some r and d (see also Section 1 of [25]). This can be explained as follows. Let $F(x) = \sum g^{c_i} x^{d_i}$ where $c_i \geq 0$ and d_i's are distinct. Note that if F has a constant term then $d_i = 0$ for some i. Letting

$$d'_F = \gcd_{i \neq j}(2^n-1, d_i - d_j)$$

and $d_F = (2^n-1)/d'_F$, we can write $F(x) = x^r h(x^{(2^n-1)/d_F})$ where $r = d_i$ for some i. When F is a monomial, we get $d'_F = 2^n-1$ and $d_F = 1$ which is the most efficient case.

2.2 Equivalent relations of Boolean functions

The followings definition contains some equivalence relations among the vectorial Boolean functions on finite fields.

Definition 2. *Let F and G be functions defined on $\mathbb{F}_{2^n}$.*
(i) F and G are ***linear equivalent*** *if $F = L_1 \circ G \circ L_2$ for some linear permutations L_1 and L_2.*
(ii) F and G are ***affine equivalent*** *if $F = A_1 \circ G \circ A_2$ for some affine permutations A_1 and A_2.*
(iii) F and G are ***extended affine(EA) equivalent*** *if $F = A_1 \circ G \circ A_2 + A_3$ for some affine permutations A_1 and A_2 and an affine function A_3.*

The following equivalence, called CCZ-equivalence, was introduced in [6].

Definition 3. *Let F and F' be functions defined on $\mathbb{F}_{2^n}$. Denote $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $\mathcal{G}_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$. Then F and F' are said to be* ***CCZ-equivalent*** *if there is an affine permutation $\mathcal{L} : \mathcal{G}_F \mapsto \mathcal{G}_{F'}$.*

The relation among the above mentioned equivalences are as follows; Linear equivalence → Affine equivalence → EA equivalence → CCZ-equivalence.

2.3 Boomerang uniformity

As mentioned in section 1, the boomerang uniformity of a permutation F is defined as follows.

Definition 4. *Let F be a permutation on $\mathbb{F}_{2^n}$. We denote $\beta_F(a,b)$ $(a, b \in \mathbb{F}_{2^n})$ by the number of solutions of the following equation*

$$F^{-1}(F(x)+a) + F^{-1}(F(x+b)+a) = b. \tag{2}$$

The ***boomerang uniformity*** *of F is defined by*

$$\beta_F = \max_{a,b \in \mathbb{F}_{2^n}^*} \beta_F(a,b). \tag{3}$$

The boomerang uniformity is preserved under affine equivalence but is not preserved under EA equivalence[3]. Furthermore F and F^{-1} have the same boomerang uniformity[3] where F^{-1} is the inverse permutation of F.

The authors of [16] consider the following system of equations.

Definition 5. *Let F be a permutation on $\mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$. We denote $\beta'_F(a,b)$ by the number of solutions (x, y) of the following system*

$$\begin{cases} F(x+a) + F(y+a) = b \\ F(x) + F(y) = b \end{cases} \tag{4}$$

We also denote β'_F by

$$\beta'_F = \max_{a,b \in \mathbb{F}_{2^n}^*} \beta'_F(a,b). \tag{5}$$

Then one has the following result on the boomerang uniformity[16].

Theorem 3. *(Theorem 2.3 of [16]) The notations are same as those in Definition 4 and 5. Then $\beta'_F = \beta_F$.*

The key idea of Theorem 3 is

$$\beta'_F(a, b) = \beta_{F^{-1}}(a, b). \tag{6}$$

Theorem 3 is useful when computing the boomerang uniformity of F because F^{-1} is not used in (4). However, since $\beta'_F(a, b) = \beta_{F^{-1}}(a, b) \neq \beta_F(a, b)$ in general, $\beta'_F(a, b)$ do not generate the boomerang connectivity table[8] of F, the table of $\beta_F(a, b)$ for all $a, b \in \mathbb{F}_{2^n}$.

2.4 Other notions of Boolean functions

In this subsection, we introduce some invariants of vectorial Boolean functions.

Definition 6 (Walsh Transform)**.** *Let $a, b \in \mathbb{F}_{2^n}$ and F be a function on $\mathbb{F}_{2^n}$. Then*

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

*is called the **Walsh transform** of F, where $Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$ for all $x \in \mathbb{F}_{2^n}$.*

Definition 7 ((Extended) Walsh Spectrum)**.** *Let F a function defined on $\mathbb{F}_{2^n}$.*
*(i) The multiset $\Lambda_F = \{\lambda_F(a, b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}^*_{2^n}\}$ is called the **Walsh spectrum** of F.*
*(ii) The multiset $\Lambda'_F = \{|\lambda_F(a, b)| : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}^*_{2^n}\}$ is called the **extended Walsh spectrum** of F.*

The nonlinearity can be defined using the notion of the Walsh transform.

Definition 8 (Nonlinearity)**.** *Let F be a function on $\mathbb{F}_{2^n}$ and*

$$\lambda_F = \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}^*_{2^n}} |\lambda_F(a, b)| \tag{7}$$

*be the maximum value in Λ'_F. Then the **nonlinearity** of F is defined by*

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2}\lambda_F. \tag{8}$$

Next we introduce another cryptographic parameter of Boolean functions related with the differential uniformity.

Definition 9 (Differential Spectrum)**.** *Let F be a function defined on $\mathbb{F}_{2^n}$. The multiset*

$$\mathcal{D}_F = \{\delta_F(a, b) : a \in \mathbb{F}^*_{2^n}, b \in \mathbb{F}_{2^n}\}$$

*is called the **differential spectrum** of F.*

It is known that if two functions F and F' are CCZ-equivalent then F and F' have the same extended Walsh spectrum, nonlinearity, and differential spectrum.

3 Efficient formulas for computing cryptographic parameters of $F(x) = x^r h(x^{(2^n-1)/d})$

Throughout this section, we fix $F(x) = x^r h(x^{(2^n-1)/d}) \in \mathbb{F}_{2^n}[x]$ for some $h(x) \in \mathbb{F}_{2^n}[x]$ where r is an integer and d is a divisor of $2^n - 1$. We will present efficient formulas for computing the differential uniformity, the differential spectrum, the boomerang uniformity, the Walsh transform, the extended Walsh spectrum, and the nonlinearity of $F(x)$. The introduced formulas are efficient for small d.

3.1 The differential uniformity

In this subsection, an efficient formula for δ_F of $F(x) = x^r h(x^{(2^n-1)/d})$ is proposed. First we introduce the the following result in [7].

Theorem 4. *(Theorem 6 of [7]) Let $\mu_d = \{\alpha \in \mathbb{F}_{2^n}^* : \alpha^d = 1\}$ be the cyclic subgroup of order d in $\mathbb{F}_{2^n}^*$. If $\gcd(d, (2^n-1)/d) = 1$ then differential uniformity of F can be computed by*

$$\delta_F = \max_{a \in \mu_d, b \in \mathbb{F}_{2^n}} \delta_F(a, b). \tag{9}$$

We would like to extend the above result to the case $\gcd(d, (2^n-1)/d) > 1$. First we prove the following lemma which is used in the proof of Theorem 5 and Theorem 8.

Lemma 1. *If $\psi\left(\frac{a'}{a}\right) = 0$ equivalently $\left(\frac{a'}{a}\right)^{(2^n-1)/d} = 1$ where $a, a' \in \mathbb{F}_{2^n}^*$, then*

$$F\left(\frac{a'}{a}x\right) = \left(\frac{a'}{a}\right)^r F(x)$$

for all $x \in \mathbb{F}_{2^n}$.

Proof. Since $\psi\left(\frac{a'}{a}\right) = 0$, we get $\psi\left(\frac{a'}{a}x\right) = \psi\left(\frac{a'}{a}\right) + \psi(x) = \psi(x)$. Since $F(x) = x^r h(\omega^{\psi(x)})$, we get

$$F\left(\frac{a'}{a}x\right) = \left(\frac{a'}{a}x\right)^r h\left(\omega^{\psi\left(\frac{a'}{a}x\right)}\right) = \left(\frac{a'}{a}\right)^r x^r h(\omega^{\psi(x)}) = \left(\frac{a'}{a}\right)^r F(x).$$

□

Theorem 5. *Under the same condition as in Lemma 1 and for $b \in \mathbb{F}_{2^n}$,*

$$\delta_F(a, b) = \delta_F\left(a', \left(\frac{a'}{a}\right)^r b\right).$$

Proof. Suppose that y is a solution of $F(x) + F(x + a) = b$. By Lemma 1,

$$\begin{aligned} F\left(\frac{a'}{a}y\right) + F\left(\frac{a'}{a}y + a'\right) &= F\left(\frac{a'}{a}y\right) + F\left(\frac{a'}{a}(y + a)\right) \\ &= \left(\frac{a'}{a}\right)^r (F(y) + F(y + a)) = \left(\frac{a'}{a}\right)^r b \end{aligned}$$

Thus $\dfrac{a'}{a}y$ is a solution of

$$F(x) + F(x + a') = \left(\frac{a'}{a}\right)^r b. \tag{10}$$

This shows that there is a bijection between the set of solutions of $F(x) + F(x + a) = b$ and the set of solutions of (10). Therefore, $F(x) + F(x + a) = b$ and (10) have same number of solutions, which completes the proof. □

The above theorem shows that for fixed $a, a' \in \mathbb{F}_{2^n}^*$ with $\psi(a) = \psi(a')$ the following is satisfied

$$\{\delta_F(a, b) : b \in \mathbb{F}_{2^n}\} = \left\{\delta_F\left(a', \left(\frac{a'}{a}\right)^r b\right) : b \in \mathbb{F}_{2^n}\right\} = \{\delta_F(a', b) : b \in \mathbb{F}_{2^n}\}.$$

The second equality comes from the fact that $b \mapsto \left(\dfrac{a'}{a}\right)^r b$ is bijective. Let a_i be any representative element of the set

$$\Psi_i = \{a \in \mathbb{F}_{2^n}^* : \psi(a) = i\}$$

for each $0 \le i < d$. Suppose that we have already computed $\delta_F(a_i, b)$ for all $b \in \mathbb{F}_{2^n}$ and $0 \le i < d$. Then for all $a' \in \Psi_i$ and $b \in \mathbb{F}_{2^n}$, we get

$$\delta_F(a', b) = \delta_F\left(a_i, \left(\frac{a_i}{a'}\right)^r b\right) \tag{11}$$

from Theorem 5. Since $g^i \in \Psi_i$ for each $0 \le i < d$, where g is a primitive root of $\mathbb{F}_{2^n}$,

$$R_d = \{g^i : 0 \le i < d\}$$

can be an example of such set consisting of representative element of Ψ_i. Considering R_d as the representative set, (11) is rewritten as

$$\delta_F(a', b) = \delta_F\left(g^i, \left(\frac{g^i}{a'}\right)^r b\right), \tag{12}$$

and we also get the following corollary.

Corollary 1. *The differential uniformity of F can be computed by*

$$\delta_F = \max_{a \in R_d, b \in \mathbb{F}_{2^n}} \delta_F(a, b). \tag{13}$$

If we apply (1) for computing the differential uniformity, then we need to consider all $a \in \mathbb{F}_{2^n}^*$, while we only need to consider $a \in R_d$ using (13). Therefore our reduced search space is only $d/(2^n - 1)$ of the original search space. In a similar way, we get another corollary which is useful for computing the differential spectrum of $F(x)$.

Corollary 2. *For $c \in \mathcal{D}_F$, let*

$$\mathcal{D}_{F,c} = \{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} : \delta_F(a, b) = c\},$$
$$\mathcal{D}_{F,c,d} = \{(a, b) \in R_d \times \mathbb{F}_{2^n} : \delta_F(a, b) = c\}.$$

Then we have

$$\#\mathcal{D}_{F,c,d} = \#\mathcal{D}_{F,c} \cdot d/(2^n - 1).$$

Hence we can compute the differential spectrum of F efficiently by computing the multiset

$$\{\delta_F(a,b) : a \in R_d, b \in \mathbb{F}_{2^n}^*\}$$

first and apply Corollary 2 to compute the multiplicity of each element in the above set.

Next we consider a special family of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$. For an integer k, we denote $\nu_d(k)$ such that $d^{\nu_d(k)} \mid k$ but $d^{\nu_d(k)+1} \nmid k$. Suppose that d is a prime and $\gcd(d, (2^n-1)/d) = d$, and then $\nu_d(2^n-1) > 1$. Now we consider the polynomials

$$G(x) = x^r(x^{(2^n-1)/d} + \xi). \tag{14}$$

where $\xi \in \mu_{d^{\nu_d(2^n-1)}} \setminus \mu_d$. First we prove that $G(x)$ is a permutation polynomial for some special cases.

Theorem 6. *Let $d = 3$ and $\gcd(3, (2^n-1)/3) = 3$, that is, $6|n$. If $\gcd(r, (2^n-1)/3) = 1$ and ξ is a primitive 9-th root of unity, then $G(x)$ is a permutation polynomial.*

Proof. By Theorem 2, it remains to show that $G'(x) = x^r(x+\xi)^{(2^n-1)/3}$ permutes μ_3. Since $\xi^6 + \xi^3 + 1 = 0$,

$$\begin{aligned}(\xi^2+\xi)^7 &= \xi^{14} + \xi^{13} + \xi^{12} + \xi^{11} + \xi^{10} + \xi^9 + \xi^8 + \xi^7 \\ &= \xi^{12} + \xi^9 + (\xi^6 + \xi^3 + 1)(\xi^8 + \xi^7) = \xi^3 + 1 = \xi^6\end{aligned}$$

and hence we get $(\xi^2+\xi)^{21} = 1$. Since $(2^n-1)/3$ is divisible by $(2^6-1)/3 = 21$ when $6|n$, we get

$$(\xi^2+\xi)^{(2^n-1)/3} = \xi^{(2^n-1)/3}(\xi+1)^{(2^n-1)/3} = 1. \tag{15}$$

For convenience, we denote $\omega_3 = \xi^3$. Observe that

$$\begin{aligned}G'(1) &= (\xi+1)^{(2^n-1)/3} \\ G'(\omega_3) &= \omega_3^r(\omega_3+\xi)^{(2^n-1)/3} = \omega_3^r(\xi^3+\xi)^{(2^n-1)/3} = \omega_3^r\xi^{(2^n-1)/3}(\xi^2+1)^{(2^n-1)/3} \\ &= \omega_3^r\xi^{(2^n-1)/3}\left((\xi+1)^{(2^n-1)/3}\right)^2 \underset{(15)}{=} \omega_3^r(\xi+1)^{(2^n-1)/3} \\ G'(\omega_3^2) &= \omega_3^{2r}(\omega_3^2+\xi)^{(2^n-1)/3} = \omega_3^{2r}(\xi^6+\xi^{10})^{(2^n-1)/3} = \omega_3^{2r}(\xi^6+\xi^{10})^{(2^n-1)/3} \\ &= \omega_3^{2r}(1+\xi^4)^{(2^n-1)/3} = \omega_3^{2r}\left((1+\xi)^{(2^n-1)/3}\right)^4 = \omega_3^{2r}(\xi+1)^{(2^n-1)/3}\end{aligned}$$

and hence if $\gcd(r, (2^n-1)/3) = 1$ then $G'(x)$ permutes μ_3, which completes the proof. □

We would like to show that the formula (13) in Corollary 1 for $G(x)$ can be further simplified. First we prove the following lemma.

Lemma 2. *Let $\rho \in \mathbb{F}_{2^n}$ be a primitive $d^{\nu_d(2^n-1)}$-th root of unity. If 2 is a primitive root mod* $\mathrm{Ord}(\xi)$*, then*

$$\delta_G(\rho^j, b) = \delta_G\left(1, \left(\rho^{-j(r+(2^n-1)/d)}b\right)^{2^{n-k_j}}\right)$$

for some integer k_j for every $0 < j < d$.

Proof. Let x be a solution of $b = G(x) + G(x + \rho^j)$, that is,

$$b = G(x) + G(x + \rho^j) = x^{r+(2^n-1)/d} + \xi x^r + (x + \rho^j)^{r+(2^n-1)/d} + \xi(x + \rho^j)^r$$

Substitute $x = \rho^j y$ into the above equation we get

$$\begin{aligned} b &= (\rho^j y)^{r+(2^n-1)/d} + \xi(\rho^j y)^r + (\rho^j y + \rho^j)^{r+(2^n-1)/d} + \xi(\rho^j y + \rho^j)^{i\cdot(2^n-1)/d-1} \\ &= \rho^{j(r+(2^n-1)/d)} \left(y^{r+(2^n-1)/d} + \xi\rho^{-j(2^n-1)/d} y^r + (y+1)^{r+(2^n-1)/d} + \xi\rho^{-j(2^n-1)/d}(y+1)^r \right) \end{aligned}$$

Hence we get

$$\rho^{-j(r+(2^n-1)/d)} b = y^{r+(2^n-1)/d} + \xi\rho^{-j(2^n-1)/d} y^r + (y+1)^{r+(2^n-1)/d} + \xi\rho^{-j(2^n-1)/d}(y+1)^r$$

Since $\rho^{-j(2^n-1)/d} \in \mu_d$, we get $\xi\rho^{-j(2^n-1)/d} \in \mu_{\mathrm{Ord}(\xi)} \setminus \mu_d$. Since 2 is a primitive root mod $\mathrm{Ord}(\xi)$, there is an integer k_j such that $\xi^{2^{k_j}} = \xi\rho^{-j(2^n-1)/d}$. Raising 2^{n-k_j}-th power to the last equation, we get

$$\left(\rho^{-j(r+(2^n-1)/d)} b\right)^{2^{n-k_j}} = (y^{2^{n-k_j}})^{r+(2^n-1)/d} + \xi(y^{2^{n-k_j}})^r + (y^{2^{n-k_j}}+1)^{r+(2^n-1)/d} + \xi(y^{2^{n-k_j}}+1)^r$$

Hence $z = y^{2^{n-k_j}} = (\rho^{-j}x)^{2^{n-k_j}}$ is a solution of $G(z) + G(z+1) = \left(\rho^{-j(r+(2^n-1)/d)} b\right)^{2^{n-k_j}}$. □

Theorem 7. *Under the same condition as in Lemma 2,*

$$\delta_G = \max_{b \in \mathbb{F}_{2^n}} \delta_G(1, b). \tag{16}$$

It is clear that we can set $R_d = \{1\}$ for computing the differential spectrum of $G(x)$ in Corollary 2.

3.2 The boomerang uniformity

For boomerang uniformity, we can derive similar theorem and formula to previous subsection. We only consider the case for β'_F.

Theorem 8. *Suppose $F(x)$ is a permutation. Let $a, a' \in \mathbb{F}^*_{2^n}$ and $b \in \mathbb{F}_{2^n}$.If $\psi\left(\frac{a'}{a}\right) = 0$ equivalently $\left(\frac{a'}{a}\right)^{(2^n-1)/d} = 1$, then*

$$\beta'_F(a, b) = \beta'_F\left(a', \left(\frac{a'}{a}\right)^r b\right).$$

Proof. Suppose that $(x, y) = (x_0, y_0)$ is a solution of (4). By Lemma 1, we get

$$\begin{aligned} F\left(\frac{a'}{a}x_0 + a'\right) + F\left(\frac{a'}{a}y_0 + a'\right) &= F\left(\frac{a'}{a}(x_0 + a)\right) + F\left(\frac{a'}{a}(y_0 + a)\right) \\ &= \left(\frac{a'}{a}\right)^r (F(x_0 + a) + F(y_0 + a)) = \left(\frac{a'}{a}\right)^r b, \end{aligned}$$

and also

$$F\left(\frac{a'}{a}x_0\right)+F\left(\frac{a'}{a}y_0\right)=\left(\frac{a'}{a}\right)^r(F(x_0)+F(y_0))=\left(\frac{a'}{a}\right)^r b.$$

Thus $(x,y)=\left(\frac{a'}{a}x_0,\frac{a'}{a}y_0\right)$ is a solution of

$$\begin{cases} F(x+a')+F(y+a')=\left(\frac{a'}{a}\right)^r b \\ F(x)+F(y)=\left(\frac{a'}{a}\right)^r b \end{cases} \tag{17}$$

This shows that there is a bijection between the solutions of (4) and the solutions of (17). Therefore, (4) and (17) have same number of solutions, which completes the proof. □

Applying Theorem 3 and Theorem 8, we get the following.

Corollary 3. *The boomerang uniformity of F can be computed by*

$$\beta_F=\max_{a\in R_d,b\in\mathbb{F}_{2^n}^*}\beta'_F(a,b). \tag{18}$$

In Corollary 2, we used the formula (12) to compute the differential spectrum efficiently. We can apply similar argument for the boomerang uniformity. We define the boomerang spectrum of a permutation F. Since $\beta_F(a,b)=q$ when $a=0$ or $b=0$, we exclude these cases in the definition of the boomerang spectrum.

Definition 10 (Boomerang Spectrum)**.** *For any permutation F on $\mathbb{F}_{2^n}$, the* ***boomerang spectrum*** *of F is defined as the multiset*

$$\mathcal{B}_F=\{\beta_F(a,b):a,b\in\mathbb{F}_{2^n}^*\}.$$

It is shown[3] that if two permutations F and F' defined on $\mathbb{F}_{2^n}$ are boomerang equivalent, then $\mathcal{B}_F=\mathcal{B}_{F'}$. If we denote

$$\mathcal{B}'_F=\{\beta'_F(a,b):a,b\in\mathbb{F}_{2^n}^*\},$$

then we can easily see that $\mathcal{B}'_F=\mathcal{B}_F$ from (6). Note that the boomerang spectra of some S-boxes including AES(Advanced Encryption Standards) S-box were investigated in [8]. Now we have the following analogue to Corollary 2.

Corollary 4. *Suppose $F(x)$ is a permutation. For $c\in\mathcal{B}_F$, we denote that*

$$\mathcal{B}'_{F,c}=\{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}:\beta'_F(a,b)=c\}$$
$$\mathcal{B}'_{F,c,d}=\{(a,b)\in R_d\times\mathbb{F}_{2^n}:\beta'_F(a,b)=c\}$$

Then we see that

$$\#\mathcal{B}'_{F,c}=\#\mathcal{B}'_{F,c,d}\cdot(2^n-1)/d.$$

Hence we can compute the boomerang spectrum of F efficiently by computing the multiset

$$\{\beta_F(a,b):a\in R_d,b\in\mathbb{F}_{2^n}^*\}$$

first and apply Corollary 4 to compute the multiplicity of each element in the above set.

3.3 The extended Walsh spectrum

The result for the Walsh spectrum is similar, though the proof technique is slightly different from Section 3.1 and Section 3.2.

Theorem 9. *Let $b, b' \in \mathbb{F}_{2^n}^*$ and $a \in \mathbb{F}_{2^n}$. If $\psi\left(\frac{b'}{b}\right) = 0$ equivalently $\left(\frac{b'}{b}\right)^{(2^n-1)/d} = 1$, then*

$$\lambda_F(a, b) = \lambda_F\left(\left(\frac{b'}{b}\right)^{r'} a, b'\right).$$

where $rr' \equiv 1 \pmod{(2^n-1)/d}$.

Proof. By Lemma 1,

$$ax + bF(x) = \left(\frac{b'}{b}\right)^{r'}\left(\frac{b}{b'}\right)^{r'} ax + b' \cdot \frac{b}{b'}F(x) = \left(\frac{b'}{b}\right)^{r'} a\left(\left(\frac{b}{b'}\right)^{r'} x\right) + b'F\left(\left(\frac{b}{b'}\right)^{r'} x\right).$$

Since $\{(b/b')^{r'} x : x \in \mathbb{F}_{2^n}\} = \mathbb{F}_{2^n}$, we obtain

$$\begin{aligned}
\lambda_F(a, b) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax+bF(x))} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr\left((b'/b)^{r'} a\left((b/b')^{r'} x\right) + b'F\left((b/b')^{r'} x\right)\right)} \\
&= \sum_{(b/b')^{r'} x \in \mathbb{F}_{2^n}} (-1)^{Tr\left((b'/b)^{r'} a\left((b/b')^{r'} x\right) + b'F\left((b/b')^{r'} x\right)\right)} \\
&= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr\left((b'/b)^{r'} ax + b'F(x)\right)} = \lambda_F\left(\left(\frac{b'}{b}\right)^{r'} a, b'\right)
\end{aligned}$$

which completes the proof. □

From Theorem 9, we get

$$\lambda_F(a, b) = \lambda_F\left(\left(\frac{g^i}{b}\right)^{r'} a, g^i\right). \tag{19}$$

Corollary 5. *For $c \in \Lambda_F$, we denote that*

$$\Lambda_{F,c} = \{(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^* : \lambda_F(a, b) = c\},\ \Lambda_{F,c,d} = \{(a, b) \in \mathbb{F}_{2^n} \times R_d : \lambda_F(a, b) = c\},$$
$$\Lambda'_{F,|c|} = \{(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^* : \lambda'_F(a, b) = |c|\},\ \Lambda'_{F,|c|,d} = \{(a, b) \in \mathbb{F}_{2^n} \times R_d : \lambda'_F(a, b) = |c|\}$$

Then we see that

$$\#\Lambda_{F,c} = \#\Lambda_{F,c,d} \cdot (2^n - 1)/d \text{ and } \#\Lambda'_{F,|c|} = \#\Lambda'_{F,|c|,d} \cdot (2^n - 1)/d.$$

Hence we can compute the Walsh spectrum and the extended Walsh spectrum of $F(x)$ efficiently by computing the multisets

$$\{\lambda_F(a, b) : a \in \mathbb{F}_{2^n}, b \in R_d\} \text{ and } \{|\lambda_F(a, b)| : a \in \mathbb{F}_{2^n}, b \in R_d\}$$

first and apply Corollary 5 to compute the multiplicity of each element in the above sets, respectively. The nonlinearity of $F(x)$ can also be efficiently computed using Theorem 9.

Corollary 6. *The nonlinearity of $F(x)$ is given as*

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in R_d} |\lambda_F(a,b)|. \tag{20}$$

4 Numerical results for even n

4.1 A complete investigating for the case $d = 3$ when $n \leq 12$

It is well studied about the permutations of low boomerang uniformity including APN permutations over $\mathbb{F}_{2^n}$ for odd n. But the same topic on even n is not well studied yet. Especially there is no known permutation polynomial of the boomerang uniformity at most 4 over $\mathbb{F}_{2^n}$ when $4 \mid n$. Since a permutation of the boomerang uniformity 4 is differentially 4-uniform, it is worth to investigate the boomerang uniformity of differentially 4-uniform permutations. The boomerang uniformity of power permutation F with $\delta_F = 4$ is considered in [16]. Hence we consider the second smallest case $d = 3$ in this section since $3 \mid (2^n - 1)$ for every even n. A complete investigating is the most inefficient method, but it is also the most obvious method. And we can expect to offset this inefficiency by applying our formulas proposed in section 3.

4.1.1 Permutation binomials

We investigate the permutation binomials of the form

$$F(x) = x^r(x^{(2^n-1)/3} + g^k) \tag{21}$$

where $0 \leq k < 2^n - 1$, when $4 \leq n \leq 10$ is even.

■ **Reducing target space**

As already mentioned in Section 2, it is known that the differential uniformity and the extended Walsh spectrum are invariant under CCZ-equivalence and the boomerang uniformity is invariant under affine equivalence and inversion. Therefore, if we know that some polynomials have this equivalence, it is sufficient to investigate one of them as a representative. We first introduce a corollary of the result about compositional inverse of $F(x)$ in [18].

Theorem 10. *([18]) Let $F(x) = x^r h(x^{(2^n-1)/d})$. Then the compositional inverse of F can be expressed as*

$$F^{-1}(x) = x^{r'} h'(x^{(2^n-1)/d})$$

where $rr' \equiv 1 \pmod{(2^n-1)/d}$ and for some $h'(x) \in \mathbb{F}_{2^n}[x]$.

Next we get the following linear equivalence.

Proposition 1. *Let $F(x) = x^r(x^{(2^n-1)/3} + g^k)$.*
(i) Let $r' \equiv r \cdot 2^i \pmod{2^n - 1}$ be an element of the cyclotomic coset of $r \pmod{2^n-1}$. Then $F(x)$ is linear equivalent to

$$\begin{cases} x^{r'}(x^{(2^n-1)/3} + g^{k'}) \text{ for even } i \\ x^{r'-(2^n-1)/3}(x^{(2^n-1)/3} + g^{k'}) \text{ for odd } i \end{cases}$$

for some k'.
(ii) If k' is contained in the same cyclotomic coset with k, then $F'(x) = x^r(x^{(2^n-1)/3} + g^{k'})$ is linear equivalent to $F(x)$.

Proof. (i) We have $(F(x))^{2^i} = x^{2^i \cdot r}(x^{2^i \cdot (2^n-1)/3} + g^{k \cdot 2^i}) = x^{r'}(x^{(-1)^i \cdot (2^n-1)/3} + g^{k \cdot 2^i})$. If i is even, then $F(x)$ is linear equivalent to $x^{r'}(x^{(2^n-1)/3} + g^{k \cdot 2^i})$. If i is odd, then

$$(F(x))^{2^i} = x^{r'}(x^{-(2^n-1)/3} + g^{k \cdot 2^i}) = g^{k \cdot 2^i} x^{r'-(2^n-1)/3}(x^{(2^n-1)/3} + g^{2^n-1-k \cdot 2^i}),$$

thus $F(x)$ is linear equivalent to $x^{r'-(2^n-1)/3}(x^{(2^n-1)/3} + g^{2^n-1-k \cdot 2^i})$.
(ii) Let $k' \equiv k \cdot 2^j \pmod{2^n - 1}$ for some $0 \le j < n$. For $L_1(x) = x^{2^j}$ and $L_2(x) = x^{2^{n-j}}$, we can see that $F'(x) = (L_1 \circ F \circ L_2)(x)$. □

A detail process to select a target space for our experiments is in Algorithm 1. By Proposition 1, we consider a representative set of cyclotomic cosets mod $(2^n - 1)/3$. We also apply Theorem 10 in step 6-7. Note that r_{alr} and k_{alr} indicate whether there is an element that has equivalence mentioned in Proposition 1 or Theorem 10 in C_r and C_k, respectively.

Algorithm 1

Input : An even integer n

Output : Target space

```
 1: $C_r \leftarrow \{\}, C_k \leftarrow \{\}$
 2: for odd $k$ from 1 to $(2^n-1)/3$ do
 3:   $r_{alr} \leftarrow 0, k_{alr} \leftarrow 0, i \leftarrow 0$
 4:   while $k_{alr} = 0$ and $i < n$ do
 5:     $k' \leftarrow k \cdot 2^i \pmod{(2^n-1)/3}$
 6:     if $\gcd(k', (2^n-1)/3) = 1$ do
 7:       Compute $0 < r' < (2^n-1)/3$ such that $k'r' \equiv 1 \pmod{(2^n-1)/3}$
 8:     if $k'$ or $r'$ belong to $C_r$ do
 9:       $r_{alr} = 1$
10:     if $k'$ belong to $C_k$ do
11:       $k_{alr} = 1$
12:     $i \leftarrow i + 1$
13:   if $\gcd(k, (2^n-1)/3) = 1$ and $r_{alr} = 0$ do
14:     add $k$ in $C_r$
15:   if $k_{alr} = 0$ do
16:     add $k$ in $C_k$
17: return $\{r + i(2^n-1)/d : r \in C_r, 0 \le i < d\} \times C_k$
```

Remark 1. *By Theorem 10, when $r \equiv -1 \pmod{(2^n - 1)/3}$, the inverse of $x^r h(x^{(2^n-1)/3})$ is also of the form $x^r h'(x^{(2^n-1)/3})$, that is, $r' = r$. But we do not consider this property when we generate a target space by Algorithm 1. In our experimental results if two permutation polynomials have the same differential and boomerang spectrum and the same extended Walsh spectrum, then we investigate that one is linear equivalent to the inverse of the another. Note that some permutations are linear equivalent to their own inverse, for example $F_{6,2,1}(x)$ below.*

■ Our experiments

For each even n with $6 \leq n \leq 12$, we have the following experiments for all (r, k) in target space generated by Algorithm 1.

- Check whether $F(x)$ is a permutation or not. Note that we can use Theorem 2.
- If $F(x)$ is a permutation, then check whether $F(x)$ is differentially 4-uniform or not using the formula (13).
- If $F(x)$ is differentially 4-uniform, then compute other cryptographic parameters including β_F using the formulas in Section 3.

Unfortunately, as already mentioned in [7], there is no differentially 4-uniform permutation binomial of the form (21) when $n = 4, 8, 10, 12$. However, we find the following 3 differentially 4-uniform permutation binomials in $\mathbb{F}_{2^6}$. Cryptographic parameters of those differentially 4-uniform permutation binomials are described in Table 1. We denote these binomials as $F_{6,2,i}(x)$.

i	(r, k)	$\mathcal{D}_{F_{6,2,i}}$	$\mathcal{B}_{F_{6,2,i}}$	$\Lambda'_{F_{6,2,i}}$
1	(20,7)	$\{0^{2268}, 2^{1512}, 4^{252}\}$	$\{0^{1953}, 2^{1386}, 4^{378}, 6^{378}, 8^{126}\}$	$\{0^{1512}, 8^{2016}, 16^{504}\}$
2	(41,7)	$\{0^{2394}, 2^{1260}, 4^{378}\}$	$\{0^{1890}, 2^{882}, 4^{882}, 6^{252}, 12^{63}\}$	$\{0^{819}, 4^{1386}, 8^{1008}, 12^{504}, 16^{189}, 20^{126}\}$
3	(62,7)	$\{0^{2394}, 2^{1260}, 4^{378}\}$	$\{0^{1890}, 2^{882}, 4^{882}, 6^{252}, 12^{63}\}$	$\{0^{819}, 4^{1386}, 8^{1008}, 12^{504}, 16^{189}, 20^{126}\}$

Table 1: Differentially 4-uniform binomials $F_{6,2,i}$ when $n = 6$

According to Remark 1, we confirm that $F_{6,2,1}$ is linear equivalent to its inverse, and $F_{6,2,2}$ is linear equivalent to $F^{-1}_{6,2,3}$. Note that all $F_{6,2,i}(x)$ are of the form $G(x)$ in Eq. (14).

4.1.2 Permutation trinomials

We investigate the permutation trinomials of the form

$$F(x) = x^r(x^{2(2^n-1)/3} + g^k x^{(2^n-1)/3} + g^l) \tag{22}$$

where $0 \leq k, l < 2^n - 1$, when $6 \leq n \leq 12$ is even.

■ Reducing target space

Similar with the binomial case, we have the following linear equivalence among those polynomials.

Proposition 2. *Let* $F(x) = x^r(x^{2(2^n-1)/3} + g^k x^{(2^n-1)/3} + g^l)$.
(i) If $r' \equiv r \cdot 2^i \pmod{(2^n-1)/3}$ *for some* i, *then* $F(x)$ *is linear equivalent to* $x^{r'}h'(x^{(2^n-1)/3})$ *for some* $h'(x) \in \mathbb{F}_{2^n}[x]$.
(ii) Let $C_{k,l} = \{(k \cdot 2^i, l \cdot 2^i) \pmod{2^n-1} : 0 \leq i < n\}$ *and* $(k', l') \in C_{k,l}$. *Then*

$$F'(x) = x^r(x^{2(2^n-1)/3} + g^{k'} x^{(2^n-1)/3} + g^{l'})$$

is linear equivalent to $F(x)$.
(iii) Let

$$F_1(x) = x^r(x^{2(2^n-1)/3} + g^{k-(2^n-1)/3}x^{(2^n-1)/3} + g^{l+(2^n-1)/3}),$$
$$F_2(x) = x^r(x^{2(2^n-1)/3} + g^{k+(2^n-1)/3}x^{(2^n-1)/3} + g^{l-(2^n-1)/3}).$$

Then $F_1(x)$ and $F_2(x)$ are linear equivalent to $F(x)$.

Proof. If $F(x)$ is of the form (22), then the exponents of monomials of $F(x)$ belong in the same class under modulo $(2^n-1)/3$. Thus we may write $F(x) = x^r h(x^{(2^n-1)/3})$ for some $h(x) \in \mathbb{F}_{2^n}[x]$ where $0 \leq r < (2^n-1)/3$.
(i) We have $(F(x))^{2^i} = x^{2^i \cdot r}(x^{2^{i+1}\cdot(2^n-1)/3} + g^{k\cdot 2^i}x^{2^i\cdot(2^n-1)/3} + g^{l\cdot 2^i})$. Thus we can express $(F(x))^{2^i} = x^{r'}h'(x^{(2^n-1)/3})$ for some $h'(x) \in \mathbb{F}_{2^n}[x]$, and $F(x)$ is linear equivalent to $x^{r'}h'(x^{(2^n-1)/3})$.
(ii) Write $(k', l') \equiv (k \cdot 2^j, l \cdot 2^j) \pmod{2^n-1}$ for some $0 \leq j < n$. For $L_1(x) = x^{2^j}$ and $L_2(x) = x^{2^{n-j}}$, we can see that $F'(x) = (L_1 \circ F \circ L_2)(x)$.
(iii) Let $L_3(x) = gx$, $L_4(x) = g^{(2^n-1)/3-r}x$, $L_5(x) = g^2x$, and $L_6(x) = g^{2(2^n-1)/3-2r}x$. Then $F_1(x) = (L_4 \circ F \circ L_3)(x)$ and $F_2(x) = (L_6 \circ F \circ L_5)(x)$. □

Proposition 2 shows that we can select target space of (r, k, l) for our experiments by $C_r \times C_k \times \{0, \cdots, 2^n-2\}$, where C_r and C_k are in Algorithm 1. But the case $k = 0$ is not contained in this target space. (In the case of binomials, if $k = 0$ then $F(x)$ in Eq. (21) cannot be a permutation by Theorem 2. Hence we reject the case $k = 0$ from initial process for binomial case.) We generate C_l be a representative set of cyclotomic cosets mod $2^n - 1$. Then the target space of our experiments for trinomials is

$$C_r \times \left((C_k \times \{0, \cdots, 2^n-2\}) \cup (\{0\} \times C_l)\right).$$

■ Our experiments

For each even n with $6 \leq n \leq 12$, we have similar experiments in Section 4.1.1 for all (r, k, l) in target space mentioned above.

• The case $n = 6$

When $n = 6$, we get 11 differentially 4-uniform permutation trinomials only for $r = (2^n-1)/3 - 1 = 20$. We consider Remark 1 to get the following 6 CCZ-inequivalent differentially 4-uniform permutation trinomials. Table 2 contains cryptographic parameters of those differentially 4-uniform permutation trinomials, denoted by $F_{6,3,i}$. Note that $F_{6,3,5}$ and $F_{6,3,6}$ are involutions, they do not belong our target space but we find that our some permutation polynomials are linear equivalent to these involutions. Note that $F_{6,3,1}$ is linear equivalent to its inverse.

• The case $n = 8$

When $n = 8$, we get 7 differentially 4-uniform permutation trinomials. See Table 3 for details. We confirm that 2 permutation trinomials for $r = (2^n-1)/3 = 84$ are linear equivalent

i	(k,l)	$\mathcal{D}_{F_{6,3,i}}$	$\mathcal{B}_{F_{6,3,i}}$	$\Lambda'_{F_{6,3,i}}$
1	(0,11)	$\{0^{2457}, 2^{1134}, 4^{441}\}$	$\{0^{1848}, 2^{924}, 4^{882}, 6^{189}, 8^{105}, 10^{21}\}$	$\{0, 4, 8, 12, 16, 20, 24\}$
2	(1,8)	$\{0^{2394}, 2^{1260}, 4^{378}\}$	$\{0^{1869}, 2^{1050}, 4^{756}, 6^{210}, 8^{84}\}$	$\{0, 4, 8, 12, 16, 24\}$
3	(5,28)	$\{0^{2394}, 2^{1260}, 4^{378}\}$	$\{0^{1932}, 2^{987}, 4^{714}, 6^{252}, 8^{63}, 10^{21}\}$	$\{0, 4, 8, 12, 16, 20, 24\}$
4	(7,14)	$\{0^{2457}, 2^{1134}, 4^{441}\}$	$\{0^{1890}, 2^{1008}, 4^{819}, 8^{126}, 10^{126}\}$	$\{0, 4, 8, 12, 16, 20\}$
5	(13,13)	$\{0^{2331}, 2^{1386}, 4^{315}\}$	$\{0^{1974}, 2^{1239}, 4^{483}, 6^{105}, 8^{105}, 10^{42}, 12^{21}\}$	$\{0, 4, 8, 12, 16, 20, 24\}$
6	(61,31)	$\{0^{2520}, 2^{1008}, 4^{504}\}$	$\{0^{2037}, 2^{714}, 4^{777}, 6^{210}, 8^{84}, 10^{84}, 12^{63}\}$	$\{0, 4, 8, 12, 16, 20, 24\}$

Table 2: Differentially 4-uniform permutation trinomials $F_{6,3,i}$ when $n = 6$

to the inverse of each other, and hence we omit one of them in Table 3. Though $F_{8,3,3}$ and $F_{8,3,6}$ have the same differential spectrum and the same extended Walsh spectrum, we cannot confirm their CCZ-equivalence, nor the equivalence between $F_{8,3,4}$ and $F_{8,3,5}$. Nevertheless, we find at least 4 CCZ-inequivalent differentially 4-uniform trinomials for the case $n = 8$. Note that we apply $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x^2 + 1)$, the SageMath default finite field of 2^8 elements which is not exactly same with the base field of AES $\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$.

i	(r,k,l)	$\mathcal{D}_{F_{8,3,i}}$	$\mathcal{B}_{F_{8,3,i}}$	$\Lambda'_{F_{8,3,i}}$
1	(84,1,159)	$\{0^{37230}, 2^{23460}, 4^{4590}\}$	$\{0^{31450}, 2^{20655}, 4^{9435}, 6^{2635}, 8^{680}, 10^{170}\}$	$\{4j : 0 \leq j \leq 11\}$
2	(3,3,16)	$\{0^{36975}, 2^{23970}, 4^{4335}\}$	$\{0^{32555}, 2^{20145}, 4^{7990}, 6^{3655}, 8^{510}, 10^{170}\}$	$\{0^{24140}, 16^{33235}, 32^{7820}, 48^{85}\}$
3	(3,3,107)	$\{0^{35955}, 2^{26010}, 4^{3315}\}$	$\{0^{32555}, 2^{22950}, 4^{6290}, 6^{2805}, 8^{170}, 10^{255}\}$	$\{0^{22950}, 16^{34680}, 32^{7650}\}$
4	(3,13,155)	$\{0^{35190}, 2^{27540}, 4^{2550}\}$	$\{0^{32130}, 2^{25840}, 4^{4845}, 6^{1615}, 8^{510}, 10^{85}\}$	$\{0^{21420}, 16^{36720}, 32^{7140}\}$
5	(3,15,123)	$\{0^{35190}, 2^{27540}, 4^{2550}\}$	$\{0^{31875}, 2^{25755}, 4^{5440}, 6^{1785}, 8^{85}, 12^{85}\}$	$\{0^{21420}, 16^{36720}, 32^{7140}\}$
6	(3,29,39)	$\{0^{35955}, 2^{26010}, 4^{3315}\}$	$\{0^{32470}, 2^{23035}, 4^{6205}, 6^{2890}, 8^{340}, 10^{85}\}$	$\{0^{22950}, 16^{34680}, 32^{7650}\}$

Table 3: Differentially 4-uniform permutation trinomials $F_{8,3,i}$ when $n = 8$

- **The cases** $n = 10$ **and** $n = 12$

Unfortunately, when $n = 10$ and $n = 12$, we cannot find any differentially 4-uniform permutation trinomials of the form (22). It takes 405 seconds and 42822 seconds(about 12 hours) for thess experiments for the case $n = 10$ and $n = 12$, respectively, using SageMath performed on Intel Core i7-4770 3.40GHz with 8GB memory. Therefore, the same experiment for the case $n = 14$ seems to be possible in several days, but we do not run this experiment because expected experimental result is not optimistic like the cases $n = 10$ and $n = 12$.

4.1.3 Differentially 6-uniform permutation polynomials

Based on the experimental results in the above subsections, we can see that there is no APN permutation of the form $x^r h(x^{(2^n-1)/3})$ and differentially 4-uniform permutation polybomials of this form are very rare. Hence we also try the same experiments with the above subsections for differentially 6-uniform permutation binomials and trinomials of the form $x^r h(x^{(2^n-1)/3})$. We compute the differential spectrum and the extended Walsh specturm of differentially 6-uniform permutation polynomials of the form $x^r h(x^{(2^n-1)/3})$, and count the number of CCZ-inequivalent classes of differentially 6-uniform permutation binomials and trinomials that can be distinguished by differential spectrum or extended Walsh spectrum, when $6 \leq n \leq 12$. The results of these experiments are summarized in Table 4.

n	6	8	10	12
# of binomials F with $\delta_F = 6$	1	5	7	8
# of binomials F with $\delta_F = 6$ when $r \equiv -1$	1	2	5	7
# of trinomials F with $\delta_F = 6$	11	615	1779	1618
# of trinomials F with $\delta_F = 6$ when $r \equiv -1$	11	141	1005	1615

Table 4: The number of CCZ-inequivalent differentially 6-uniform permutation polynomials when $6 \leq n \leq 12$

In particular, we also indicate the number of differentially 6-uniform binomials and trinomials obtained in the case $r \equiv -1 \pmod{(2^n-1)/3}$ in the second row and the forth row of Table 4, respectively. We can see that many differentially 6-uniform permutation polynomials of this form are in the case $r \equiv -1 \pmod{(2^n-1)/3}$. Especially for $n = 12$, only one binomial and 3 trinomials are not in this case. Moreover, we can see that the number of differentially 6-uniform permutation polynomials for $r \equiv -1 \pmod{(2^n-1)/3}$ is significantly larger than the number of differentially 6-uniform permutation polynomials for $r \not\equiv -1 \pmod{(2^n-1)/3}$, when $n = 10, 12$. Hence we may conjecture that permutation polynomials of this form in the case $r \equiv -1 \pmod{(2^n-1)/3}$ have lower differential uniformity than the case $r \not\equiv -1 \pmod{(2^n-1)/3}$ in average. In next subsection we give some heuristic analysis for this conjecture.

4.2 Some Heuristic Analysis

In previous subsection, we can see that the differential uniformity for the case $r \equiv -1 \pmod{(2^n-1)/d}$ is relatively smaller than the case $r \not\equiv -1 \pmod{(2^n-1)/d}$. We can easily see that there are the following upper bound of the differential uniformity of F when $r \equiv -1 \pmod{(2^n-1)/d}$.

Theorem 11. *Let $F(x) = x^r h(x^{(2^n-1)/d})$ where $r \equiv -1 \pmod{(2^n-1)/d}$. Then $\delta_F \leq 2d^2+2$.*

Proof. For convenience we fix $r = 2^n - 2$. Let $F(x) = x^{2^n-2}h(x^{(2^n-1)/d})$ and denote

$$W_{a,i,j} = \{x \in \mathbb{F}_{2^n} : \psi(x) = i, \psi(x+a) = j\}$$

for $a \neq 0$ and $0 \leq i, j < d$. If $x \in W_{a,i,j}$ is a solution of $F(x) + F(x+a) = b$ then it is also a solution of $x^{2^n-2}h(\omega_d^i) + (x+a)^{2^n-2}h(\omega_d^j) = b$. Then, it is also a solution ofthe following quadratic equation

$$Q_{a,b,i,j}(x) = bx^2 + \Big(h(\omega_d^i) + h(\omega_d^j) + ab\Big)\, x + ah(\omega_d^i) = 0. \tag{23}$$

Since there are d^2 equations $Q_{a,b,i,j}(x) = 0 (0 \leq i, j < d)$, there are at most $2d^2$ possible solutions. When $b = F(a)$ there is an exceptional case that $x = 0, a$ are also solutions of $F(x) + F(x+a) = F(a)$ but $0, a \notin W_{a,i,j}$ for any $0 \leq i, j < d$. Together with solutions of Eq.(23) we get $\delta_F(a, F(a)) \leq 2d^2 + 2$. If $b \neq F(a)$, we get $\delta_F(a, b) \leq 2d^2$. □

By Theorem 11, we can express $F(x)+F(x+a)=b$ as a quadratic equation $Q_{a,b,i,j}(x)=0$ for each $0 \le i,j < d$ when $r \equiv 1 \pmod{(2^n-1)/3}$. Since we can express $F(x)=x^r h(\omega_d^{\psi(x)})$, if $i=j$ then $F(x)+F(x+a)=b$ can be expressed by $x^r+(x+a)^r = b \cdot \left(h(\omega_d^i)\right)^{-1}$ which is related with $\delta_{x^r}\left(a, b\left(h(\omega_d^i)\right)^{-1}\right)$. Hence if x^r has low differential uniformity, then the above equation has small number of solutions. But if $r \not\equiv -1 \pmod{(2^n-1)/3}$ and $i \neq j$ then it is not easy to apply the similar argument with $r \equiv -1 \pmod{(2^n-1)/3}$ and $i \neq j$. For example, it is well known that x^3 is APN for all n. For the case $r=3$, we get a quadratic equation for each case $i=j$, but we get a cubic equation for each case $i \neq j$. Hence we cannot apply same arguement in Theorem 11 for the case $r=3$.

Next we propose a heuristic analysis to compute an expected value of δ_F for the case $r \equiv -1 \pmod{(2^n-1)/3}$. If $b \neq F(a)$ then by Theorem 11 we can see that

$$\delta_F(a,b) = \sum_{i,j} |\{x \in \mathbb{F}_{2^n} : Q_{a,b,i,j}(x)=0\} \cap W_{a,i,j}|.$$

For each $0 \le i,j < d$, we first check whether $Q_{a,b,i,j}(x)=0$ is solvable or not. If $Q_{a,b,i,j}(x)=0$ is solvable, we check each solution is contained in $W_{a,i,j}$ or not. We assume that $W_{a,i,j}$'s are uniformly distributed in $\mathbb{F}_{2^n} \setminus \{0,a\}$ and hence we apply the probability that each element in $\mathbb{F}_{2^n} \setminus \{0,a\}$ is contained in each $W_{a,i,j}$ by $1/d^2$. Also, we assume that each quadratic equation $Q_{a,b,i,j}(x)=0$ is solvable with same probability $1/2$. We denote

$$\begin{aligned}
D_{a,b}(k) &= Pr\left(\sum_{0\le i,j<d} |\{x \in \mathbb{F}_q : Q_{a,b,i,j}(x)=0\} \cap W_{a,i,j}| = k\right)\\
U_{a,b}(k) &= Pr\left(\sum_{0\le i,j<d} |\{x \in \mathbb{F}_q : Q_{a,b,i,j}(x)=0\} \cap W_{a,i,j}| \le k\right) = \sum_{i=0}^{k/2} D_{a,b}(2i)
\end{aligned}$$

that are computed under these assumptions. Then, we can compute that

$$\begin{aligned}
&Pr(\delta_F \le k) = \prod_{a\in R_d, b\in\mathbb{F}_q} U_{a,b}(k)\\
&Pr(\delta_F = k) = Pr(\delta_F \le k) - Pr(\delta_F \le k-2) = \prod_{a\in R_d, b\in\mathbb{F}_q} U_{a,b}(k) - \prod_{a\in R_d, b\in\mathbb{F}_q} U_{a,b}(k-2)
\end{aligned} \tag{24}$$

We compare this heuristic analysis with actual experimental results in previous section for trinomials of the form $x^{(2^n-1)/3-1}h(x^{(2^n-1)/3})$. This heuristic analysis does not meet with actual experimental results (see Table 5 for $n=10$). But this analysis is not ridiculous because expected values given by (24) are somewhat similar with actual average(see Table 6).

We do not investigate for the cases $n \ge 14$ because it is expected to be difficult to compute. We apply the expected value of δ_F obtained by this heuristic analysis to guess existence of F with low differential uniformity. We summarize the expected value computed by (24) for $n \ge 14$ in Table 7. When $n=14$ or $n=16$, the expected value of δ_F is not much larger than the expected value of δ_F when $n=12$ in Table 6. Since there are 1626 differentially 6-uniform trinomials when $n=12$(see Table 4), we can expect there may exist differentially 6-uniform

k	4	6	8	10	12	14	16	18
Permutations	0	2136	2207	1850	1796	390	66	5
Actual Prob	0	0.2528	0.2612	0.2189	0.2125	0.0462	0.0078	0.0006
(24)	1.12×10^{-18}	0.0139	0.7127	0.2565	0.0162	0.0006	1.45×10^{-8}	1.83×10^{-7}

Table 5: Comparison of heuristic analysis and actual data for trinomials when $n = 10$

n	6	8	10	12
Average of δ_F	7.16	7.93	9.12	10.32
Expected value from (24)	6.52	7.53	8.55	9.56

Table 6: Comparison of expected value and actual average of δ_F for trinomials when $6 \leq n \leq 12$

permutation polynomials of the form $x^{(2^n-1)/3-1}h(x^{(2^n-1)/3})$ when $n = 14$ or $n = 16$. We also note that we obtain that the expected value of δ_F is larger than 18 when $n \geq 38$. Hence we guess that almost all permutation polynomials of this form archieve the upperbound of differential uniformity in Theorem 11.

n	14	16	18	20	22	24	26	28
Expected value from (24)	10.46	11.36	12.25	12.91	13.90	14.37	15.12	15.98

Table 7: Expected value of δ_F when $n \geq 14$

Next we consider $G(x)$ in Eq. (14) with $d = 3$ and $r \equiv -1 \pmod{(2^n-1)/3}$. We denote them by

$$G_{n,j,i}(x) = x^{i(2^n-1)/3-1}(x^{(2^n-1)/3} + \xi)$$

where $\xi \in \mu_{3^{\nu_d(2^n-1)}} \setminus \mu_3$ is a primitive 3^j-th root of unity and $0 \leq i < 3$. Note that we showed that each $G_{n,2,i}(x)$ is a permutation polynomial in Theorem 6. It can be applied for the case $j > 2$ if Eq. 15 holds, and we confirm that $G_{18,3,i}(x)$ is a permutation polynomial for each i.

By applying Theorem 2, (24) also can be simplified by

$$Pr(\delta_{G_{n,j,i}} = k) = \prod_{b \in \mathbb{F}_{2^n}} U_{1,b}(k) - \prod_{b \in \mathbb{F}_{2^n}} U_{1,b}(k-2) \tag{25}$$

We compare the expected value computed by Eq. (25) with actual differential uniformity of $G_{n,j,i}$ in Table 8. Expected value from (24) is less than expected value from (24), but is significantly larger than actual differential uniformity of $G_{n,j,i}$.

4.3 The case $d \neq 3$

We also investigate the differential uniformity of permutation polynomials of the form $x^r h(x^{n/2-1})$ discussed in some recent papers, see Table 9 for details. This is the case $d = 2^{n/2} + 1$ and we

(n,j,i)	(6,2,-)	(12,2,0)	(12,2,1)	(18,2,-)	(18,3,-)	(24,2,-)
$\delta_{G_{n,j,i}}$	4	6	8	8	8	8
Expected value from (25)	5.77	8.72	8.72	11.59	11.59	14.04

Table 8: Comparison of extended value and actual $\delta_{G_{n,j,i}}$

denote $m = n/2$ in Table 9 for convenience. Note that

$$F_{25}(x) = x^{2^n-2^m+2} + x^{2^n-3\cdot 2^m+4} + x^{2^n-5\cdot 2^m+6} + x^{2^n-7\cdot 2^m+8} + x^{7\cdot 2^m-5} + x^{5\cdot 2^m-3} + x^{3\cdot 2^m-1},$$
$$F_{27}(x) = x^{2^n-2^m+2} + x^{2^n-5\cdot 2^m+6} + x^{2^n-7\cdot 2^m+8} + x^{7\cdot 2^m-5} + x^{3\cdot 2^m-1}$$

in Table 9, which are too long to be expressed in Table 9.

Polynomial	Introduced in	6	8	10
$x^{(2^n-1)/(2^t-1)+1} + \alpha x$ $(n = 2^s t,\ t =\text{odd})$	Theorem 1.1 in [2]	4	lin.	4
$x^{3\cdot 2^m+1} + x^{2^m+3} + x^4$	Theorem 3.1 in [10]	–	16	34
$x^{3\cdot 2^m-1} + x^{2^{m+1}} + x^2$	Theorem 3.3 in [10]	–	16	34
$x^{2^{m+2}+1} + x^{2^m+4} + x^5$	Theorem 3.4 in [10]	16	–	64
$x^{2^{m+2}-1} + x^{3\cdot 2^m} + x^3$	Theorem 3.5 in [10]	16	–	44
$x^{3\cdot 2^m-2} + \alpha x$	Theorem B in [11]	10	–	34
$x^{2^{m+1}-1} + \alpha x^{2^m} + \gamma x$	Theorem 1.1 in [12]	8	16	32
$x^{s(2^m-1)+1} + x^{t(2^m-1)+1} + x$	Theorem 1 and 3 in [14]	16	10	64
$x^{2^{n-1}+2^{m-1}+1} + x^{2^m} + x$	Theorem 4.7 in [15]	–	16	34
$x^{2^{n-1}+2^{m-1}+1} + x^{2^m+2} + x$	Theorem 4.8 in [15]	8	–	10
$\alpha^{2^{m-1}} x^{2^n-2^m+1} + \alpha x^{2^{m+1}-1} + x$	Theorem 4.9 in [15]	14	32	62
$x^{3*2^m-2} + x^{2^{m+1}-1} + x^{2^n-2^m+1} + x^{2^n-2^{m+1}+2} + x$	Theorem 3.9 in [17]	16	32	104
$x^{2^m+1}x^2(x^{2^m-1} + x^{1-2^m})^{2^m-2^{m/2}-1}$	Theorem 3.13 in [17]	–	28	–
$x^{2^m+1}x^2(x^{2^m-1} + x^{2^n-2^m})^{2(2^{m+1}-2^{m/2}-1)/3}$	Theorem 3.15 in [17]	–	16	–
$F_{25}(x)$	Theorem 3.25 in [17]	16	16	36
$F_{27}(x)$	Theorem 3.27 in [17]	16	16	34

Table 9: Differential uniformity of some permutation polynomials for even $6 \leq n \leq 10$

We investigate the differential uniformity of those polynomials only when they are permutations, thus if the differential uniformity is omitted in the table, then the polynomial in that case is not a permutation. Please refer the cited papers for detailed conditions where each polynomial in the first column is a permutation polynomial. From the table, we see that the differential uniformity is not very low except the case in the first row when $n \equiv 2 \pmod 4$. However, since $n = 2t$ in this case, the polynomial is $x^{2^m+2} + \alpha x$. The differential uniformity of this polynomial was already investigated in [26], and the boomerang uniformity was investigated in [16]. We also computed the differential uniformity of these polynomial when $n = 12$, which is not the case $n \equiv 2 \pmod 4$, but we get $\delta_F = 88$. For the class of permutation polynomials in [14], there are several pairs (s,t) that the corresponding polynomial is a permutation, and the value in Table 9 is the minimal value of the differential uniformity of those permutation polynomials for each n. Overall, it is not very optimistic to get a permutation polynomial of low differential uniformity for the case $d = 2^m + 1$.

5 Conclusion

Compared with permutations having low differential uniformity, the permutations with low boomerang uniformity are not well studied yet. Since a permutation of the boomerang uniformity 4 is also differentially 4-uniform, the study of the boomerang uniformity of the known differentially 4-uniform permutations(see Table 1 in [9] for known differentially 4-uniform permutations) is important. Our research in this paper focuses on this topic. In this paper, we get efficient formulas for computing some cryptographic parameters (including boomerang and differential uniformity) of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$. The computational cost of our formulas is proportional to d. We tried our formulas to investigate differentially 4-uniform permutations for $d = 3$ with even $6 \leq n \leq 10$, where 3 is the least nontrivial factor dividing $2^n - 1$ for even n. For $n = 4, 8$, we computed the boomerang uniformity and the boomerang spectrum of differentially 4-uniform permutations using the suggested formula which turned out to be rather large. We also investigated the differential uniformity of some permutation polynomials for the case $d = 2^m + 1$ and found out that they are not suitable for S-box construction.

Acknowledgement This research was supported by the National Research Foundation of Korea (KRF) Grant funded by the Korea government (MSIP) (No. 2016R1A5A1008055) Namhun Koo was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1C1C2003888). Soonhak Kwon was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1F1A1058920 and No. 2021R1F1A1050721).

References

[1] A. Akbary, and Q. Wang, On Polynomials of the Form $x^r f(x^{(q-1)/l})$, *International Journal of Mathematics and Mathematical Sciences*, Vol. 2007, Article ID 23408. https://doi.org/10.1155/2007/23408

[2] S. Bhattacharya, and S. Sarkar, On some permutation binomials and trinomials over $\mathbb{F}_{2^n}$, *Des. Codes Cryptogr.* 82(1-2) (2017) 149-160 https://doi.org/10.1007/s10623-016-0229-0

[3] C. Boura, and A. Canteaut, On the Boomerang Uniformity of Cryptographic Sboxes. *IACR Transactions on Symmetric Cryptology*, 2018(3) (2018) 290-310. https://doi.org/10.13154/tosc.v2018.i3.290-310

[4] C. Boura, A. Canteaut, J. Jean, and V. Suder, Two notions of differential equivalence on Sboxes, *Des. Codes Cryptogr.* 87(2-3) (2019) 185-202 https://doi.org/10.1007/s10623-018-0496-z

[5] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe, An APN permutation in dimension six *9th, International conference on finite fields and applications; Finite fields: theory and applications, Dublin, in Comtemporary Mathematics*, 518 (2010) 33-42. http://doi.org/10.1090/conm/518

[6] C. Carlet, P. Charpin, and V. Zinoviev, Codes, Bent Functions, and Permutations Suitable For DES-like Cryptosystems, *Des. Codes Cryptogr.* 15(2) (1998) 125-156 https://doi.org/10.1023/A:1008344232130

[7] P. Charpin, and G.M. Kyureghyan, On sets determining the differential spectrum of mappings, *International Journal of Information and Coding Theory*, 4(2-3) (2017) 170-184, a recent revised version is available at https://hal.inria.fr/hal-01406589v3. https://doi.org/10.1504/IJICOT.2017.083844

[8] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, Boomerang Connectivity Table: A New Cryptanalysis Tool. *In: Nielsen J., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2018. Lecture Notes in Computer Science*, vol 10821, pp.683-714, Springer, Cham. https://doi.org/10.1007/978-3-319-78375-8_22

[9] S. Fu, and X. Feng, Involutory differentially 4-uniform permutations from known constructions, *Des. Codes Cryptogr.* 87(1) (2019) 31-56 https://doi.org/10.1007/s10623-018-0482-5

[10] R. Gupta, and R.K. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.* 41 (2016) 89-96 http://dx.doi.org/10.1016/j.ffa.2016.05.004

[11] X. Hou, Determination of a type of permutation trinomials over finite fields, II, *Finite Fields Appl.* 35 (2015) 16-35 http://dx.doi.org/10.1016/j.ffa.2015.03.002

[12] X. Hou, and S.D. Lappano, Determination of a type of permutation binomials over finite fields, *J. Number Theory* 147 (2015) 14-23 http://dx.doi.org/10.1016/j.jnt.2014.06.021

[13] N. Li, and T. Helleseth, Several classes of permutation trinomials from Niho exponents *Cryptogr. Commun.* 9 (2017) 693-705 https://doi.org/10.1007/s12095-016-0210-9

[14] N. Li, and T. Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, *Cryptogr. Commun.* 11 (2019) 129-136 https://doi.org/10.1007/s12095-018-0321-6

[15] K. Li, L. Qu, and X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, *Finite Fields Appl.* 43 (2017) 69-85 https://doi.org/10.1016/j.ffa.2016.09.002

[16] K. Li, L. Qu, B. Sun, and C. Li, New Results about the Boomerang Uniformity of Permutation Polynomials, *IEEE Trans. on Inf. Theory*, 65 (2019) 7542-7553 http://dx.doi.org/10.1109/TIT.2019.2918531

[17] K. Li, L. Qu, and Q. Wang, New constructions of permutation polynomials of the form $x^r hx(x^{q-1})$ over $\mathbb{F}_{q^2}$, *Des. Codes Cryptogr.* 86(10) (2019) 2379-2405 https://doi.org/10.1007/s10623-017-0452-3

[18] K. Li, L. Qu, and Q. Wang, Compositional inverses of permutation polynomials of the form $x^r h(x^s)$ over finite fields, *Cryptogr. Commun.* 11 (2019) 279-298 https://doi.org/10.1007/s12095-018-0292-7

[19] S. Mesnager, C. Tang, and M. Xiong, On the boomerang uniformity of (quadratic) permutations over $\mathbb{F}_{2^n}$, *a preprint*, available at https://arxiv.org/abs/1903.00501 (2019)

[20] K. Nyberg, Differentially uniform mappings for cryptography. *In: Helleseth T. (eds) Advances in Cryptology — EUROCRYPT '93. Lecture Notes in Computer Science* 765 (1994) 55-64, Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48285-7_6

[21] Y.H. Park, and J.B. Lee, Permutation polynomial and group permutation polynomials, *Bull. Aust. Math. Soc.* 63 (2001) 67-74 https://doi.org/10.1017/S0004972700019110

[22] D. Wagner, The Boomerang Attack. *In: Knudsen L. (eds) Fast Software Encryption 1999. Lecture Notes in Computer Science* 1636 (1999) 156-170 Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48519-8_12

[23] D. Wan, and R. Lidl, Permutation Polynomials of the Form $x^r f(x^{(q-1)/d})$ and Their Group Structure, *Monalshefte für Mathematik* 112 (1991) 149-163, Springer. https://doi.org/10.1007/BF01525801

[24] Q. Wang, Cyclotomic Mapping Permutation Polynomials over Finite Fields, *In: Golomb S.W., Gong G., Helleseth T., Song HY. (eds) Sequences, Subsequences, and Consequences. Lecture Notes in Computer Science*, vol 4893 (2007), pp. 119-128, Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-540-77404-4_11

[25] Q. Wang, Cyclotomy and permutation polynomials of large indices, *Finite Fields Appl.* 22 (2013) 57-69 https://doi.org/10.1016/j.ffa.2013.02.005

[26] X. Zhu, X. Zeng, and Y. Chen, Some Binomial and Trinomial Differentially 4-Uniform Permutation Polynomials, *International Journal of Foundations of Computer Science* 26(4) (2015) 487-497 https://doi.org/10.1142/S0129054115500276

[27] M.E. Zieve, On some permutation polynomial over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. *Proc. Am. Math. Soc.* 137 (2009) 2207-2216 https://doi.org/10.1090/S0002-9939-08-09767-0