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

Jaeseong Jeong, Chang Heon Kim, Namhun Koo, Soonhak Kwon, and Sumin Lee
Email: wotjd012321@naver.com, {chhkim,komaton,shkwon,dltnals816}@skku.edu
Applied Algebra and Optimization Research Center,
Sungkyunkwan University, Suwon, Republic of 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 $x^r h(x^{(q-1)/d})$ over a finite field of $q = 2^n$ elements, where r is a positive integer and d is a positive divisor of $q-1$. The computational cost of those formulas is proportional to d. We investigate differentially 4-uniform permutation polynomials of the form $x^r h(x^{(q-1)/3})$ and compute the boomerang spectrum and the extended Walsh spectrum of them using the suggested formulas when $4 \leq n \leq 10$ 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, Boomerang Spectrum, Extended Walsh Spectrum, Differentially 4-Uniform Permutation Polynomials

1 Introduction

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

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

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[21] 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 $F(x) = x^{q-2} \in \mathbb{F}_q[x]$ 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[24]. Recently, Cid et al.[8] introduced the boomerang connectivity table which contains the number of solutions of

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

for a permutation $F : \mathbb{F}_q \to \mathbb{F}_q$, 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 $a, b \in \mathbb{F}_q^*$, where the case $a = 0$ or $b = 0$ are excluded because $\beta_F(a, 0) = \beta_F(0, b) = q$ for all $a, b \in \mathbb{F}_q$. 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, 17, 20] about the boomerang uniformity of the known differentially 4-uniform permutations. In [3, 17, 20], 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 $x^r h(x^{(q-1)/d})$. Permutation polynomials of this form were first characterized by Wan and Lidl[25], and have since been widely studied[1, 2, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 22, 23, 26, 27, 29]. 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 $x^r h(x^{(q-1)/3})$ 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 $x^r h(x^{(q-1)/d})$ 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 $x^r h(x^{(q-1)/d})$. In section 4, we investigate cryptographic parameters of differentially 4-uniform permutations of the form $x^r h(x^{(q-1)/3})$ 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 $x^r h(x^{(q-1)/d})$

In this subsection, we focus on permutation polynomials of the form $x^r h(x^{(q-1)/d})$ introduced by Wan and Lidl[25]. We first introduce the following notations which are also used in [25].

Definition 1. *(Definition 1.1 of [25]) Let $d|(q-1)$ and g be a fixed primitive root of $\mathbb{F}_q$. Let $\omega = g^{(q-1)/d}$ be a primitive d-th root of unity in $\mathbb{F}_q$. A map $\psi : \mathbb{F}_q^* \mapsto (\mathbb{Z}/d\mathbb{Z})^+$ defined by*

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

where $Ind_g(a)$ is the residue class ($b \bmod (q-1)$) such that $a = g^b$.

Note that the following equation holds.

$$a^{(q-1)/d} = \omega^{\psi(a)}$$

With these notations, the following main theorem of [25] gives a characterization of permutation polynomials of the form $x^r h(x^{(q-1)/d})$.

Theorem 1. *(Theorem 1.2 of [25]) Let r be a positive integer, d be a positive divisor of $q-1$. Let $h(x) \in \mathbb{F}_q[x]$. Then the polynomial $F(x) = x^r h(x^{(q-1)/d})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied :*
(i) $\gcd(r, (q-1)/d) = 1$.
(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[22] introduced a simpler characterization of these permutation polynomials. Zieve[29] reproved this formula with comment that he discovered it before the publication of [22].

Theorem 2. *(Lemma 2.1 of [29]) Let r be a positive integer, d be a positive divisor of $q-1$ and $\mu_d = \{\alpha \in \mathbb{F}_q^* : \alpha^d = 1\}$. Let $h(x) \in \mathbb{F}_q[x]$. Then the polynomial $F(x) = x^r h(x^{(q-1)/d})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied :*
(i) $\gcd(r, (q-1)/d) = 1$.
(ii) $x^r h(x)^{(q-1)/d}$ *permutes* μ_d.

There are many results on the permutation polynomials of this form, and several recent studies[1, 2, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 23, 27] focus on the case $d = 2^{n/2} + 1$.

For any permutation polynomial, one can express the polynomial as the form $x^r h(x^{(q-1)/d})$ for some r and d (see also Section 1 of [26]). 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

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

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

2.2 Equivalent relations of Boolean functions

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

Definition 2. *Let F and G be functions defined on $\mathbb{F}_q$.*
*(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 $\mathbb{F}_q$. Denote $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_q\}$ and $\mathcal{G}_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_q\}$. 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 $\rightarrow$ Affine equivalence $\rightarrow$ EA equivalence $\rightarrow$ 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 $\mathbb{F}_q$. We denote $\beta_F(a, b)$ $(a, b \in \mathbb{F}_q)$ 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*

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

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

Definition 5. *We say that two permutations F and F' defined on $\mathbb{F}_q$ are **boomerang equivalent** if F' is affine equivalent to F or F^{-1}.*

Note that Boomerang equivalence is also an equivalence relation. It is known that F and F^{-1} are CCZ-equivalent, hence if F and F' are boomerang equivalent then they are also CCZ-equivalent. The authors of [17] consider the following system of equations.

Definition 6. *Let F be a permutation on $\mathbb{F}_q$ and $a, b \in \mathbb{F}_q$. 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

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

Then one has the following result on the boomerang uniformity[17].

Theorem 3. *(Theorem 2.3 of [17]) The notations are same as those in Definition 4 and 6. 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 $a,b \in \mathbb{F}_q$.

2.4 Other notions of Boolean functions

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

Definition 7 (Walsh Transform)**.** *Let $a,b \in \mathbb{F}_q$ and F be a function on $\mathbb{F}_q$. Then*

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

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

Definition 8 ((Extended) Walsh Spectrum)**.** *Let F a function defined on $\mathbb{F}_q$.*
*(i) The multiset $\Lambda_F = \{\lambda_F(a,b) : a \in \mathbb{F}_q, b \in \mathbb{F}_q^*\}$ is called the **Walsh spectrum** of F.*
*(ii) The multiset $\Lambda'_F = \{|\lambda_F(a,b)| : a \in \mathbb{F}_q, b \in \mathbb{F}_q^*\}$ is called the **extended Walsh spectrum** of F.*

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

Definition 9 (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 10 (Differential Spectrum)**.** *Let F be a function defined on $\mathbb{F}_q$. The multiset*

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

*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 $F(x) = x^r h(x^{(q-1)/d})$

Throughout this section, we fix $F(x) = x^r h(x^{(q-1)/d}) \in \mathbb{F}_q[x]$ for some $h(x) \in \mathbb{F}_q[x]$ where r is an integer and d is a divisor of $q-1$. 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 $F(x) = x^r h(x^{(q-1)/d})$ is proposed. First we prove the following lemma which is used in the proof of Theorem 4 and Theorem 6.

Lemma 1. *If $\psi(a) = \psi(a')$ equivalently $a^{(q-1)/d} = a'^{(q-1)/d}$, where $a, a' \in \mathbb{F}_q^*$, then*

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

for all $x \in \mathbb{F}_q$.

Proof. Since $\psi(a) = \psi(a')$, we get $\psi\left(\frac{a'}{a}\right) = 0$. Hence $\psi\left(\frac{a'}{a}x\right) = \psi\left(\frac{a'}{a}\right) + \psi(x) = \psi(x)$. 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 4. *Under the same condition as in Lemma 1 and for $b \in \mathbb{F}_q$,*

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

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 $\frac{a'}{a}y$ is a solution of

$$F(x) + F(x+a') = \left(\frac{a'}{a}\right)^r b. \tag{9}$$

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 (9). Therefore, $F(x)+F(x+a) = b$ and (9) have same number of solutions, which completes the proof. □

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

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

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

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

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

$$\delta_F(a',b) = \delta_F\left(a_i, \left(\frac{a_i}{a'}\right)^r b\right) \tag{10}$$

from Theorem 4. Since $g^i \in \Psi_i$ for each $0 \le i < d$, where g is a primitive root of $\mathbb{F}_q$,

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

can be an example of such set consisting of representative element of Ψ_i. Considering G_d as the representative set, (10) is rewritten as

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

and we also get the following corollary.

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

$$\delta_F = \max_{a \in G_d, b \in \mathbb{F}_q} \delta_F(a,b). \tag{12}$$

If we apply (1) for computing the differential uniformity, then we need to consider all $a \in \mathbb{F}_q^*$, while we only need to consider $a \in G_d$ using (12). Therefore our reduced search space is only $d/(q-1)$ 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*

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

Then we have

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

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

$$\{\delta_F(a,b) : a \in G_d, b \in \mathbb{F}_q^*\}$$

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

Remark 1. *A similar result to Corollary 2 was obtained in Theorem 6 of [7] where S_d, the multiplicative subgroup of order $d \mid (q-1)$, with the condition* $\gcd(d,(q-1)/d)=1$ *is used in [7]. However, since* $\gcd(d,(q-1)/d) \mid \psi(a)$ *for all $a \in S_d$, S_d is not a representative set of Ψ_i when* $\gcd(d,(q-1)/d)>1$. *G_d in (12) can be replaced by any representative set of Ψ_i and hence our result is a generalization of the result in [7]. Furthermore, the method in [7] could not find any differentially 4-uniform binomial of the form $x^r h(x^{(q-1)/d})$ for small $d>1$, while we find two differentially 4-uniform binomials up to CCZ-equivalence when $n=6$ (see Section 4.1).*

3.2 The boomerang uniformity

For β_F and β'_F, we can derive similar theorems and formulas to previous subsection. First we prove the following lemma.

Lemma 2. *Let r' be an integer with $rr' \equiv 1 \pmod{q-1}$ and let F be a permutation. Suppose $\psi(a)=\psi(a')$ where $a,a' \in \mathbb{F}_q^*$. Then, for all $x \in \mathbb{F}_q$,*
(i) $F\left(\left(\frac{a}{a'}\right)^{r'} x\right) = \frac{a}{a'}F(x)$.
(ii) $F^{-1}\left(\frac{a'}{a}x\right) = \left(\frac{a'}{a}\right)^{r'} F^{-1}(x)$.

Proof. (i) Since $\psi(a)=\psi(a')$ we obtain $\psi(a^{r'})=\psi(a'^{r'})$. By Lemma 1,

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

(ii) Let $y = \left(\frac{a'}{a}\right)^{r'} F^{-1}(x)$. Then $F^{-1}(x) = \left(\frac{a}{a'}\right)^{r'} y$. By (i) we obtain $x = F\left(\left(\frac{a}{a'}\right)^{r'} y\right) = \frac{a}{a'}F(y)$. Thus we get $F(y) = \frac{a'}{a}x$ and $y = F^{-1}\left(\frac{a'}{a}x\right)$, which completes the proof. □

Theorem 5. *Under the same condition as in Lemma 2,*

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

Proof. Let y be a solution of (2). Then,

$$\begin{aligned}\left(\frac{a'}{a}\right)^{r'} b &= \left(\frac{a'}{a}\right)^{r'} \left(F^{-1}(F(y)+a) + F^{-1}(F(y+b)+a)\right) \\ &= \left(\frac{a'}{a}\right)^{r'} F^{-1}(F(y)+a) + \left(\frac{a'}{a}\right)^{r'} F^{-1}(F(y+b)+a)\end{aligned}$$

By Lemma 2, we obtain

$$\left(\frac{a'}{a}\right)^{r'} b = F^{-1}\left(\frac{a'}{a}F(y)+a'\right) + F^{-1}\left(\frac{a'}{a}F(y+b)+a'\right).$$

By Lemma 1, we get

$$\left(\frac{a'}{a}\right)^{r'} b = F^{-1}\left(F\left(\left(\frac{a'}{a}\right)^{r'} y\right) + a'\right) + F^{-1}\left(F\left(\left(\frac{a'}{a}\right)^{r'} y + \left(\frac{a'}{a}\right)^{r'} b\right) + a'\right)$$

Thus $\left(\frac{a'}{a}\right)^{r'} y$ is a solution of

$$F^{-1}\left(F(x) + a'\right) + F^{-1}\left(F\left(x + \left(\frac{a'}{a}\right)^{r'} b\right) + a'\right) = \left(\frac{a'}{a}\right)^{r'} b. \tag{13}$$

This shows that there is a bijection between solutions of (2) and solutions of (13). Therefore, (2) and (13) have same number of solutions, which completes the proof. □

Since Theorem 5 is very similar to Theorem 4, we can use similar argument as in Section 3.1. The above theorem shows that, for fixed $a, a' \in \mathbb{F}_q^*$ with $\psi(a) = \psi(a')$, the following is satisfied

$$\{\beta_F(a,b) : b \in \mathbb{F}_q\} = \left\{\beta_F\left(a', \left(\frac{a'}{a}\right)^{r'} b\right) : b \in \mathbb{F}_q\right\} = \{\beta_F(a',b) : b \in \mathbb{F}_q\}.$$

The second equality comes from the fact that $b \mapsto \left(\frac{a'}{a}\right)^{r'} b$ is bijective. Let $a_i \in \Psi_i$ be a representative element for each $0 \le i < d$. Then for any $a' \in \Psi_i$ and $b \in \mathbb{F}_q$, we obtain

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

using Theorem 5. Letting $a_i = g^i$, we get the following formula similar to (11),

$$\beta_F(a',b) = \beta_F\left(g^i, \left(\frac{g^i}{a'}\right)^{r'} b\right). \tag{14}$$

Hence we get the following analogue to Corollary 1.

Corollary 3. *Let $F(x)$ be a permutation. Then the boomerang uniformity of F can be computed by*

$$\beta_F = \max_{a \in G_d, b \in \mathbb{F}_q^*} \beta_F(a,b). \tag{15}$$

For β'_F introduced in Definition 6, by using Lemma 1, we find the following result similar to Theorem 4.

Theorem 6. *Suppose $F(x)$ is a permutation. Let $a, a' \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. If $\psi(a) = \psi(a')$ equivalently $a^{(q-1)/d} = a'^{(q-1)/d}$, 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

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

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

$$\begin{cases} F(x + a') + F(y + a') = \left(\frac{a'}{a}\right)^r b \\ F(x) + F(y) = \left(\frac{a'}{a}\right)^r b \end{cases} \tag{16}$$

This shows that there is a bijection between the solutions of (4) and the solutions of (16). Therefore, (4) and (16) have same number of solutions, which completes the proof. □

Applying Theorem 3 and Theorem 6, we get the following.

Corollary 4. *The boomerang uniformity of F can be computed by*

$$\beta_F = \max_{a \in G_d, b \in \mathbb{F}_q^*} \beta'_F(a, b). \tag{17}$$

In Corollary 2, we used the formula (11) 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 11 (Boomerang Spectrum)**.** *For any permutation F on $\mathbb{F}_q$, the* ***boomerang spectrum*** *of F is defined as the multiset*

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

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

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

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

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

Then we see that

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

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

$$\{\beta_F(a,b) : a \in G_d, b \in \mathbb{F}_q^*\}$$

first and apply Corollary 5 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 7. *Let $b, b' \in \mathbb{F}_q^*$ and $a \in \mathbb{F}_q$. If $\psi(b) = \psi(b')$ equivalently $b^{(q-1)/d} = b'^{(q-1)/d}$, then*

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

Proof. By Lemma 2-(i),

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

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

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

which completes the proof. □

From Theorem 7, we get

$$\lambda_F(a,b) = \lambda_F\left(\left(\frac{g^i}{b}\right)^{r'} a, g^i\right). \tag{18}$$

Corollary 6. *For $c \in \Lambda_F$, we denote that*

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

Then we see that

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

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

$$\{\lambda_F(a,b) : a \in \mathbb{F}_q, b \in G_d\} \text{ and } \{|\lambda_F(a,b)| : a \in \mathbb{F}_q, b \in G_d\}$$

first and apply Corollary 6 to compute the multiplicity of each element in the above sets, respectively. The nonlinearity of $F(x)$ can also be efficiently computed using Theorem 7.

Corollary 7. *The nonlinearity of $F(x)$ is given as*

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_q, b \in G_d} |\lambda_F(a,b)|. \tag{19}$$

4 Cryptographic parameters of differentially 4-uniform permutations of the form $F(x) = x^r h(x^{(q-1)/d})$ for even n

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 [17]. Hence we consider the second smallest case $d = 3$ in this section since $3 \mid (2^n - 1)$ for every even n. We first investigate differentially 4-uniform permutations for this case, and compute the boomerang uniformity and the extended Walsh spectrum using the formulas obtained in previous sections for even $n \leq 10$. We denote our obtained permutation polynomials defined on $\mathbb{F}_{2^n}$ by $F_{n,t,i}(x)$ where t is the number of monomials in the expression $F_{n,t,i}(x)$.

4.1 Permutation binomials

We investigate the permutation binomials of the form

$$F(x) = x^r(x^{(q-1)/3} + g^k) \tag{20}$$

where $0 \leq k < q-1$, when $4 \leq n \leq 10$ is even. First we get the following linear equivalence among them.

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

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

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

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

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

thus $F(x)$ is linear equivalent to $x^{r'-(q-1)/3}(x^{(q-1)/3} + g^{q-1-k \cdot 2^i})$.
(ii) Let $k' \equiv k \cdot 2^j \pmod{q-1}$ 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 $F'(x) = (L_1 \circ F \circ L_2)(x)$. □

For each even n with $4 \leq n \leq 10$, we first find the set of representative (r, k) up to linear equivalence in Proposition 1.

- Check whether $F(x)$ is a permutation or not using Theorem 2.
- If $F(x)$ is a permutation, then check whether $F(x)$ is differentially 4-uniform or not using the formula (12).
- If $F(x)$ is differentially 4-uniform, then compute other cryptographic parameters including β_F using the formulas in Section 3

Unfortunately, there is no differentially 4-uniform permutation binomial of the form (20) when $n = 4, 8, 10$. 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.

i	(r,k)	$\mathcal{D}_{F_{6,2,i}}$	$\mathcal{B}_{F_{6,2,i}}$	$\Lambda'_{F_{6,2,i}}$
1	(20,7)	$\{0^{2457}, 2^{1134}, 4^{441}\}$	$\{0^{1953}, 2^{1386}, 4^{378}, 6^{378}, 8^{126}\}$	$\{0^{1512}, 8^{2016}, 16^{504}\}$
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 $n = 6$

Recently, Li et al.[19] showed that, if $F(x) = x^r h(x^{(q-1)/d})$ is a permutation polynomial, then F^{-1}, the inverse function of F, is of the form $F^{-1}(x) = x^{r'} h'(x^{(q-1)/d})$ for some $h'(x)$ where $rr' \equiv 1 \pmod{(q-1)/d}$. We confirm that $F_{6,2,1}$ is linear equivalent to its inverse, and $F_{6,2,2}$ is linear equivalent to $F^{-1}_{6,2,3}$.

4.2 Permutation trinomials

We investigate the permutation trinomials of the form

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

where $0 \leq k, l < q-1$, when $4 \leq n \leq 10$ is even. We have the following linear equivalence among those polynomials.

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

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

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

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

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

Proof. If $F(x)$ is of the form (21), then the exponents of monomials of $F(x)$ belong in the same class under modulo $(q-1)/3$. Thus we may write $F(x) = x^r h(x^{(q-1)/3})$ for some $h(x) \in \mathbb{F}_q[x]$ where $0 \le r < (q-1)/3$.
(i) We have $(F(x))^{2^i} = x^{2^i \cdot r}(x^{2^{i+1} \cdot (q-1)/3} + g^{k \cdot 2^i} x^{2^i \cdot (q-1)/3} + g^{l \cdot 2^i})$. Thus we can express $(F(x))^{2^i} = x^{r'}h'(x^{(q-1)/3})$ for some $h'(x) \in \mathbb{F}_q[x]$, and $F(x)$ is linear equivalent to $x^{r'}h'(x^{(q-1)/3})$.
(ii) Write $(k', l') \equiv (k \cdot 2^j, l \cdot 2^j) \pmod{q-1}$ 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 $F'(x) = (L_1 \circ F \circ L_2)(x)$.
(iii) Let $L_3(x) = gx$, $L_4(x) = g^{(q-1)/3-r}x$, $L_5(x) = g^2 x$, and $L_6(x) = g^{2(q-1)/3-2r}x$. Then $F_1(x) = (L_4 \circ F \circ L_3)(x)$ and $F_2(x) = (L_6 \circ F \circ L_5)(x)$. □

For each even n with $4 \le n \le 10$, we investigate the polynomials of the form (21) for

- $0 < r < (q-1)/3$ in a representative set of each $C_r = \{r \cdot 2^i \pmod{(q-1)/3} : 0 \le i < n\}$,
- (k, l) in a representative set considering Proposition 2-(ii) and (iii).

We apply the same algorithm with Section 4.1.

4.2.1 $n = 4$

When $n = 4$, it is enough to consider the case $r = (q-1)/3 - 1 = 4$ by Proposition 2-(i). We obtain the following differentially 4-uniform permutation trinomials with corresponding boomerang spectrum in Table 2.

i	(k, l)	$\mathcal{B}_{F_{4,3,i}}$
1	(12,1)	$\{0^{105}, 2^{80}, 4^{30}, 6^5, 10^5\}$
2	(7,7)	$\{0^{110}, 2^{75}, 4^{25}, 6^{10}, 10^5\}$
3	(12,8)	$\{0^{100}, 2^{85}, 4^{30}, 6^5, 8^5\}$

Table 2: The boomerang spectrum of differentially 4-uniform permutations $F_{4,3,i}$ when $n = 4$

Note that $F_{4,3,1}$ and $F_{4,3,2}$ are involutions, and $F_{4,3,3}$ is linear equivalent to its inverse. We also note that all $F_{4,3,i}$'s are EA-equivalent. It is not difficult to see their EA-equivalence since

the monomial $g^l x^r$ in each $F_{4,3,i}$ can be ignored under EA-equivalence from $r = 4$ and we can apply Proposition 2-(iii). Therefore we found an example where the boomerang uniformity is not preserved under EA-equivalence. We also remark that the boomerang uniformity of permutations when $n = 4$ was completely investigated in [3].

4.2.2 $n = 6$

When $n = 6$, we get differentially 4-uniform permutation trinomials only for $r = (q-1)/3-1 = 20$. Table 3 contains cryptographic parameters of those differentially 4-uniform permutation trinomials.

i	(k,l)	$\mathcal{D}_{F_{6,3,i}}$	$\mathcal{B}_{F_{6,3,i}}$	$\Lambda'_{F_{6,3,i}}$
1	(11,0)	$\{0^{2457}, 2^{1134}, 4^{441}\}$	$\{0^{1848}, 2^{924}, 4^{882}, 6^{189}, 8^{105}, 10^{21}\}$	$\{0, 4, 8, 12, 16, 20, 24\}$
2	(8,1)	$\{0^{2394}, 2^{1260}, 4^{378}\}$	$\{0^{1869}, 2^{1050}, 4^{756}, 6^{210}, 8^{84}\}$	$\{0, 4, 8, 12, 16, 24\}$
3	(28,5)	$\{0^{2394}, 2^{1260}, 4^{378}\}$	$\{0^{1932}, 2^{987}, 4^{714}, 6^{252}, 8^{63}, 10^{21}\}$	$\{0, 4, 8, 12, 16, 20, 24\}$
4	(14,7)	$\{0^{2457}, 2^{1134}, 4^{441}\}$	$\{0^{1890}, 2^{1008}, 4^{819}, 8^{126}, 10^{126}\}$	$\{0, 4, 8, 12, 16, 20\}$
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 3: Differentially 4-uniform permutation trinomials $F_{6,3,i}$ when $n = 6$

Note that $F_{6,3,5}$ and $F_{6,3,6}$ are involutions, and $F_{6,3,1}$ is linear equivalent to its inverse. We can see that all $F_{6,3,i}$'s are CCZ-inequivalent considering their differential spectra and extended Walsh spectra. The multiplicity of each element in $\Lambda'_{F_{6,3,i}}$ is not shown in Table 3 because it is enough to see CCZ-inequivalence of $F'_{6,3,i}s$ without the multiplicity. Note that $\mathcal{D}_{F_{6,3,i}}$ for each $1 \leq i \leq 4$ is same to $\mathcal{D}_{F_{6,2,j}}$ for some j. However, since $\Lambda_{F_{6,3,i}} \neq \Lambda_{F_{6,2,j}}$, they are not CCZ-equivalent.

4.2.3 $n = 8$

When $n = 8$, we get differentially 4-uniform permutation trinomials of the form (21) for $r \in \{3, 57, 84\}$. First for $r = (q-1)/3 - 1 = 84$, we obtain one permutation trinomial of the form (21) up to boomerang equivalence. We also obtain 5 differentially 4-uniform permutation trinomials of the form (21) for both $r = 3$ and $r = 57$. Table 4 contains cryptographic parameters of differentially 4-uniform permutation trinomials of the form (21) up to linear equivalence in Proposition 2. Since $3 \cdot 57 \equiv 1 \pmod{(q-1)/3}$, each differentially 4-uniform permutation trinomial for $r = 57$ is linear equivalent to the inverse of a differentially 4-uniform permutation trinomial for $r = 3$. Hence we omit the case $r = 57$ in Table 4.

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 $F_{8,3,5}$.

4.2.4 $n = 10$

Unfortunately, when $n = 10$, we cannot find any differentially 4-uniform permutation trinomials of the form (21). When $n = 4, 6, 8$, there are differentially 4-uniform permutation trinomials

i	(r,k,l)	$\mathcal{D}_{F_{8,3,i}}$	$\mathcal{B}_{F_{8,3,i}}$	$\Lambda'_{F_{8,3,i}}$
1	(84,159,1)	$\{0^{37230}, 2^{23460}, 4^{4590}\}$	$\{0^{31450}, 2^{20655}, 4^{9435}, 6^{2635}, 8^{680}, 10^{170}\}$	$\{4j : 0 \le j \le 11\}$
2	(3,48,1)	$\{0^{36975}, 2^{23970}, 4^{4335}\}$	$\{0^{32555}, 2^{20145}, 4^{7990}, 6^{3655}, 8^{510}, 10^{170}\}$	$\{0^{24140}, 16^{33235}, 32^{7820}, 48^{85}\}$
3	(3,182,3)	$\{0^{35955}, 2^{26010}, 4^{3315}\}$	$\{0^{32555}, 2^{22950}, 4^{6290}, 6^{2805}, 8^{170}, 10^{255}\}$	$\{0^{22950}, 16^{34680}, 32^{7650}\}$
4	(3,155,13)	$\{0^{35190}, 2^{27540}, 4^{2550}\}$	$\{0^{32130}, 2^{25840}, 4^{4845}, 6^{1615}, 8^{510}, 10^{85}\}$	$\{0^{21420}, 16^{36720}, 32^{7140}\}$
5	(3,123,15)	$\{0^{35190}, 2^{27540}, 4^{2550}\}$	$\{0^{31875}, 2^{25755}, 4^{5440}, 6^{1785}, 8^{85}, 12^{85}\}$	$\{0^{21420}, 16^{36720}, 32^{7140}\}$
6	(3,39,29)	$\{0^{35955}, 2^{26010}, 4^{3315}\}$	$\{0^{32470}, 2^{23035}, 4^{6205}, 6^{2890}, 8^{340}, 10^{85}\}$	$\{0^{22950}, 16^{34680}, 32^{7650}\}$

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

of the form (21) when

- $r = (q-1)/3 - 1$ or
- r is the Kasami APN exponent, that is, $r = 3 = 2^2 - 2 + 1$ or $r = 57 = 2^6 - 2^3 + 1$.

The above two cases are linear equivalent when $n = 4$. There are differentially 4-uniform functions for $r = 3$ but they are not permutations since $\gcd(r, (q-1)/3) = \gcd(3, 21) = 3$ when $n = 6$. Hence we conjecture that there are differentially 4-uniform permutation trinomials of the form (21) when $r = (q-1)/3 - 1$ or r is a Kasami APN exponent for all even n. But there is no differentially 4-uniform permutation trinomial of the form (21) for $r \in \{3, 57, 340\}$ when $n = 10$, which shows that this conjecture is false.

It takes 642967 seconds(about 7.44 days) for this experiment using SageMath performed on Intel Core i7-4770 3.40GHz with 8GB memory for the case $n = 10$, while the same experiment for $n = 8$ requires only 20 minutes. Therefore, it seems computationally infeasible to do the same experiment for $n = 12$ with our current computation power.

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 5 for details. This is the case $d = 2^{n/2} + 1$ and we denote $m = n/2$ in Table 5 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 5, which are too long to be expressed in Table 5.

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 on permutation. 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 [28], and the boomerang uniformity was investigated in [17]. 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 5 is the minimal

Polynomial	Introduced in	6	8	10
$x^{(2^n-1)/(2^t-1)+1}+\alpha x$ ($n=2^st$, $t=$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 [18]	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 [18]	–	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 [18]	–	16	–
$F_{25}(x)$	Theorem 3.25 in [18]	16	16	36
$F_{27}(x)$	Theorem 3.27 in [18]	16	16	34

Table 5: Differential uniformity of some permutation polynomials for even $6 \le n \le 10$

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 $6 \le n \le 10$, where is 3 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)

References

[1] D. Bartoli, and L. Quoos, Permutation polynomials of the type $x^r g(x^s)$ over $\mathbb{F}_{q^{2n}}$, *Des. Codes Cryptogr.* 86(8) (2018) 1589-1599 https://doi.org/10.1007/s10623-017-0415-8

[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, C. Li, and S. Fu, New permutation trinomials constructed from fractional polynomials, *Acta. Arith.* 183 (2018) 101-116 http://dx.doi.org/10.4064/aa8461-11-2017

[17] K. Li, L. Qu, B. Sun, and C. Li, New Results about the Boomerang Uniformity of Permutation Polynomials, *a preprint*, available at https://arxiv.org/abs/1901.10999 (2019)

[18] 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

[19] 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

[20] 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)

[21] 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

[22] 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

[23] Z. Tu, X. Zeng, C. Li, and T. Helleseth, A class of new permutation trinomials, *Finite Fields Appl.* 50 (2018) 178-195 https://doi.org/10.1016/j.ffa.2017.11.009

[24] 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

[25] 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

[26] 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

[27] Z. Zha, L. Hu, and S. Fan, Further results on permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.* 45 (2017) 43-52 https://doi.org/10.1016/j.ffa.2016.11.011

[28] 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

[29] 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