SCIENCE CHINA
Information Sciences

• LETTER •

October 2020, Vol. 63 209101:1–209101:3
https://doi.org/10.1007/s11432-018-9741-6

Permutation polynomials $x^{2^{k+1}+3} + ax^{2^k+2} + bx$ over $F_{2^{2k}}$ and their differential uniformity

Jie PENG[1], Lijing ZHENG[2], Chunsheng WU[3] & Haibin KAN[4,5,6,7*]

[1]*Mathematics and Science College, Shanghai Normal University, Shanghai* 200234, *China;*
[2]*School of Mathematics and Physics, University of South China, Hengyang* 421001, *China;*
[3]*Department of Mathematics, Lianyungang Normal University, Lianyungang* 222006, *China;*
[4]*Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai* 200433, *China;*
[5]*Fudan-Zhongan Joint Laboratory of Blockchain and Information Security, Shanghai Blockchain Engineering Research Center, Shanghai* 200433, *China;*
[6]*Shanghai Institute for Advanced Communication and Data Science, Shanghai* 200433, *China;*
[7]*Shanghai Institute of Intelligent Electronics & Systems, Shanghai* 200433, *China*

Received 23 September 2018/Accepted 11 January 2019/Published online 25 August 2020

Citation Peng J, Zheng L J, Wu C S, et al. Permutation polynomials $x^{2^{k+1}+3}+ax^{2^k+2}+bx$ over $F_{2^{2k}}$ and their differential uniformity. Sci China Inf Sci, 2020, 63(10): 209101, https://doi.org/10.1007/s11432-018-9741-6

Dear editor,

A polynomial $f(x) \in F_q[x]$ is called a permutation polynomial (PP) over the finite field F_q if the associated mapping $f : c \mapsto f(c)$ from F_q to itself is bijective. A PP f is called a complete permutation polynomial if $f(x) + x$ is a PP. PPs over finite fields of even characteristic have wide applications, including cryptography, coding theory, and communication theory. In many block ciphers with substitution-permutation network structure, the substitution box is usually a PP over $F_{2^{2k}}$ for some positive integer k. To resist the differential attacks, the differential uniformity of this polynomial should be as low as possible. However, finding such polynomials is difficult. Even for most known differentially low uniform permutations over $F_{2^{2k}}$, their polynomial representations are difficult to obtain ([1–8]). Thus far, only a few classes of differentially low uniform PPs over $F_{2^{2k}}$ of few terms have been constructed. Monomial permutations with Gold exponents $2^i + 1$, Kasami exponents $2^{2i} - 2^i + 1$, Inverse exponents $2^n - 2$, and the Bracken-Leander exponents $2^{2k} + 2^k + 1$ are differentially 4-uniform. Moreover, when $k \geqslant 5$ is odd, monomials with exponents $2^{k+1} + 3$ and $2^k + 2^{\frac{k+1}{2}} + 1$ were conjectured by Blondeau et al. and finally verified by Xiong et al. [9] to be differentially 8-uniform permutations. A class of differentially 4-uniform permutation binomial, known as the Bracken-Tan-Tan function, was also determined. However, differentially low uniform permutation trinomials have not been found yet.

In this study, PPs of the form $x^{2^{k+1}+3}+ax^{2^k+2}+bx$ over $F_{2^{2k}}$ are determined. A class of permutation monomials, a class of permutation binomials, and two classes of permutation trinomials are obtained. All those monomials and binomials are shown to be differentially 8-uniform for $k \geqslant 5$. Moreover, there exists a subclass of complete permutation binomials. For the permutation trinomials, by simulations for small integers k, it seems that their differential uniformity is not very high, and is much better than that of previously found permutation trinomials.

Determination of the PPs. We find that $f(x) = x^{2^{k+1}+3} + ax^{2^k+2} + bx \in F_{2^{2k}}[x]$ permutes $F_{2^{2k}}$ if and only if $g(x) = x^5 + (b + \overline{b} + a\overline{a})x^3 + [(b + \overline{b} + a\overline{a})(a+\overline{a}) + a\overline{b} + b\overline{a}]x^2 + [(a+\overline{a})^4 + (b+\overline{b}+a\overline{a})(a+\overline{a})^2 + b\overline{b}]x$ permutates F_{2^k}, where x^{2^k} is denoted by $\overline{x}$ for any $x \in F_{2^{2k}}$. Furthermore, $g(x)$ permutates F_{2^k} if and only if $g(x) = x^5$ for $k \equiv 2 \pmod 4$, or $g(x) = x^5 + ax^3 + a^2x, a \in F_{2^k}$, for odd k.

* Corresponding author (email: hbkan@fudan.edu.cn)

This result allows determining all PPs of the form $x^{2^{k+1}+3}+ax^{2^k+2}+bx$ over $F_{2^{2k}}$. The monomial $f(x)=x^{2^{k+1}+3}$ permutes $F_{2^{2k}}$ if and only if $4\nmid k$. Other PPs with two or three terms are obtained in the following two theorems based on k being even or odd.

Theorem 1. Let k be a positive even integer and $a,b\in F_{2^{2k}}$ be not both zero. Then, $f(x)=x^{2^{k+1}+3}+ax^{2^k+2}+bx$ permutes $F_{2^{2k}}$ if and only if $k\equiv 2 \pmod 4$; b is a root of $x^2+t^{-2}\omega x+t^{-4}\omega=0$; and $a=tb$ for some $t\in F_{2^k}^*$, where $\omega\in F_{2^k}^*$ is a primitive 3rd root of unity.

Sketch of the proof. f permutes $F_{2^{2k}}$ if and only if $k\equiv 2 \pmod 4$, and a and b satisfy

$$\begin{cases} b+\overline{b}+a\overline{a}=0,\\ a\overline{b}+b\overline{a}=0,\\ (a+\overline{a})^4+b\overline{b}=0, \end{cases} \tag{1}$$

which implies that both a and b are nonzero. Hence $a=tb$ for some $t\in F_{2^k}^*$, and the following equation can be derived:

$$\begin{cases} b+\overline{b}=t^2b\overline{b},\\ t^4(b+\overline{b})^4=b\overline{b}. \end{cases} \tag{2}$$

By (2), it holds that $t^{12}(b\overline{b})^3+1=0$. Therefore, $b\overline{b}=t^{-4}\omega^i$ and $b+\overline{b}=t^{-2}\omega^i$, where $\omega\in F_{2^k}^*$ is of order 3 and $0\leqslant i\leqslant 2$. Consequently, b and $\overline{b}$ are exactly the roots in $F_{2^{2k}}$ of the following equation:

$$x^2+t^{-2}\omega^i x+t^{-4}\omega^i=0,\quad i=1,2. \tag{3}$$

Conversely, for any $t\in F_{2^k}^*$ and $i=1,2$, Eq. (3) has two different solutions in $F_{2^{2k}}\setminus F_{2^k}$, namely b and $\overline{b}$. Set $a=tb$; then, a and b satisfy (1). Therefore, f permutes $F_{2^{2k}}$.

Theorem 2. Let k be a positive odd integer and $a,b\in F_{2^{2k}}$ be not both zero. Then, $f(x)=x^{2^{k+1}+3}+ax^{2^k+2}+bx$ permutes $F_{2^{2k}}$ if and only if a and b satisfy one of the following two conditions:

(i) $a=0$ and $b=t\omega$, for any $t\in F_{2^k}^*$ and primitive 3rd root of unity ω in $F_{2^{2k}}$.

(ii) $a=t\omega$ and $b=t^2+\varepsilon\omega^2$ for any $t,\varepsilon\in F_{2^k}^*$ and primitive 3rd root of unity ω.

Sketch of the proof. Since k is odd, 1, ω is a basis for the vector space $F_{2^{2k}}$ over F_{2^k}. The polynomial f permutes $F_{2^{2k}}$ if and only if a and b satisfy

$$\begin{cases} (b+\overline{b}+a\overline{a})(a+\overline{a})+a\overline{b}+b\overline{a}=0,\\ (a+\overline{a})^4+(b+\overline{b}+a\overline{a})(a+\overline{a})^2+b\overline{b}=(b+\overline{b}+a\overline{a})^2. \end{cases} \tag{4}$$

Now, we consider the following cases.

Case 1: $a=0$. In this case, Eq. (4) becomes $b\overline{b}=(b+\overline{b})^2$, which means $b=t\omega$ or $b=t+t\omega=t\omega^2$ for some $t\in F_{2^k}^*$.

Case 2: $a\neq 0$. In this case, the first equation of (4) indicates $a+\frac{b}{\overline{a}}\in F_q$. Hence, there exists some element $\varepsilon\in F_q$ such that $b=\overline{a}(a+\varepsilon)$ and $b+\overline{b}=(a+\overline{a})\varepsilon$. Then, the second equation can be simplified as $a\overline{a}+(a+\overline{a})^2=0$, so that $a=t\omega$ or $t\omega^2$ for some $t\in F_{2^k}^*$. Therefore, in this case, all the solutions of (4) are

$$\begin{cases} a=t\omega,\\ b=t^2+\varepsilon t\omega^2, \end{cases} \quad\text{and}\quad \begin{cases} a=t\omega^2,\\ b=t^2+\varepsilon t\omega, \end{cases} \quad t\in F_{2^k}^*.$$

This completes the proof.

Theorem 2 provides a class of complete permutation binomials $f(x)=x^{2^{k+1}+3}+\omega x$ over $F_{2^{2k}}$, where ω is a primitive 3rd root of unity.

On the differential uniformity. For any polynomial f over F_{2^n}, the differential uniformity $\delta(f)$ of f is defined as

$$\delta(f)=\max_{a\in F_{2^n}^*,b\in F_{2^n}}\#\{x\in F_{2^n}\mid f(x+a)+f(x)=b\},$$

where $\#S$ represents the size of a set S. The function f is called differentially $\delta(f)$-uniform.

The monomial $f(x)=x^{2^{k+1}+3}$ is computed to be differentially 4-uniform when $k=3$. For $k\geqslant 5$ being odd, f was shown to be differentially 8-uniform in [9]. In fact, for the case $k\equiv 2 \pmod 4, k\geqslant 6$, f is also differentially 8-uniform.

Theorem 3. Let $f(x)=x^{2^{k+1}+3}$, and let $k\geqslant 5$ be a positive integer such that $4\nmid k$. Then, f is a differentially 8-uniform permutation over $F_{2^{2k}}$.

Proof. To prove this theorem, it suffices to prove that for any $b\in F_{2^{2k}}$, the equation

$$(x+1)^{2^{k+1}+3}+x^{2^{k+1}+3}=b \tag{5}$$

has at most eight solutions. Herein we only need to consider the case $k=2m$ with m odd. Let $\omega\in F_{2^k}^*$ be of order 3; then, $x^2+\omega x+1$ is irreducible over F_{2^k}. Let γ be one of its roots in $F_{2^{2k}}$; then, $1,\gamma$ is a basis of the vector space $F_{2^{2k}}$ over F_{2^k}. Denote by $\overline{x}=x^{2^k}$ for any $x\in F_{2^{2k}}$ as before. Let $x=y+z\gamma$ with $y,z\in F_{2^k}$; then, we have $\overline{x}=y+z\overline{\gamma}=y+z(\gamma+\omega)$, and thus

$$\overline{x}+x=\omega z \text{ and } \overline{x}x=y^2+\omega yz+z^2.$$

Set $x=y+z\gamma$ and $b=s+t\gamma$ with $y,z,s,t\in F_{2^k}$; then, Eq. (5) can be rewritten as

$$\begin{cases} y^4+y+\omega^2z^2(y^2+y+1)+z^4+1+s=0,\\ \omega^2z^3+z+t=0. \end{cases}$$

So $x \in F_{2^{2k}}$ is a solution of (5) if and only if $(y,z,u) \in F_{2^k}^3$ is a solution of

$$\begin{cases} \omega^2 z^3+z+t=0, \\ y^2+y+1+u=0, \\ u^2+(\omega^2 z^2+1)u+z^4+s=0, \end{cases} \tag{6}$$

where the first equation has at most three distinct solutions, and for each solution z, the third equation has at most two solutions u. Furthermore, for each solution u, there are at most two solutions y for the second equation. Hence, to prove that the number of solutions of (6) is at most 8, it suffices to prove that among the solutions of the first equation, at most two are such that the third equation also has solutions. For the case $t=0$, namely $b=s \in F_{2^k}$, the first equation becomes $\omega^2 z^3+z=0$, which has exactly two solutions, i.e., 0 and ω^2.

When $t \neq 0$, assume that the first equation has three solutions z_1, z_2, and z_3, for each of which the third equation has solutions; then, we have

$$\begin{aligned} 0=\mathrm{Tr}_1^k\left(\frac{{z_i}^4+s}{\omega {z_i}^4+1}\right) &= \mathrm{Tr}_1^k\left(\omega^2+\frac{\omega^2+s}{\omega {z_i}^4+1}\right) \\ &= 1+\mathrm{Tr}_1^k\left(\frac{\omega^2+s}{\omega {z_i}^4+1}\right), \end{aligned}$$

and thus $\mathrm{Tr}_1^k(\frac{\omega^2+s}{\omega {z_i}^4+1})=1$ for $1 \leqslant i \leqslant 3$. From the first equation, we can obtain $(\omega z_i)^2+1=\frac{t}{z_i}$; thus, for any $1 \leqslant i \leqslant 3$, $\mathrm{Tr}_1^k(\frac{z_i^2(\omega^2+s)}{t^2}) = \mathrm{Tr}_1^k(\frac{\omega^2+s}{(\omega z_i)^4+1}) = \mathrm{Tr}_1^k(\frac{\omega^2+s}{\omega {z_i}^4+1}) = 1$. Therefore, we have

$$\mathrm{Tr}_1^k\left(\frac{(z_1+z_2+z_3)^2(\omega^2+s)}{t^2}\right)=1,$$

which contradicts the fact that $z_1+z_2+z_3=0$. Hence the first equation of (6) has at most two solutions such that the third equation has solutions, so that the number of solutions of (6) is at most 8.

Next, we prove that there exists some (t,s) such that Eq. (6) has eight solutions. Note that the first equation of (6) can be written as $(\omega z)^3+\omega z+\omega t=0$. As a result of Lemma 3.1 of [9], we can choose some $t \in F_{2^k}$ such that this equation has three distinct roots z_1, z_2, and z_3 with $\mathrm{Tr}_1^k(\omega z_1)=\mathrm{Tr}_1^k((\omega z_1)^{-1})=\mathrm{Tr}_1^k(\omega z_2)=0$. Further, according to Lemma 3.3 of [9], we can find some $s \in F_{2^k}$ such that $\mathrm{Tr}_1^k(\frac{z_1^2}{t^2}(\omega^2+s)) = \mathrm{Tr}_1^k(\frac{z_2^2}{t^2}(\omega^2+s))=1$, so that for $i \in \{1,2\}$, the equation $u^2+(\omega^2 z_i^2+1)u+z_i^4+s=0$ has two roots u_{i1} and u_{i2} with $\mathrm{Tr}(u_{i1})=\mathrm{Tr}(u_{i2})=0$. Then, for each u_{ij}, the second equation of (6) has two roots in y. Besides, for $z=z_3$ it holds that $\mathrm{Tr}_1^k(\frac{z_3^2}{t^2}(\omega^2+s))=0$; thus, the third equation has no solution. Therefore, for $b=s+t\gamma \in F_{2^{2k}}$, Eq. (6) has exactly eight solutions. This completes the proof.

The differential uniformity of all the permutation binomials obtained by Theorem 2 with $k \geqslant 5$ is also 8. However, for permutation trinomials obtained by Theorems 1 and 2, determining their differential uniformity is difficult. Using the MAGMA software, their differential uniformity was computed when $k \leqslant 7$, revealing that their differential uniformity is better compared with that of all previously known permutation trinomials over $F_{2^{2k}}$, which have explicit polynomial representations. We conjecture that the differential uniformity is equal to 12 and 10, respectively for trinomials in Theorems 1 and 2 when $k \geqslant 5$.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61672166, 11701488), Shanghai Excellent Academic Leader (Grant No. 16XD1400200), Shanghai Innovation Plan of Science & Technology (Grant No. 16JC1402700), and Scientific Research Fund of Hunan Provincial Education Department (Grant No. 17B040).

References

1 Peng J, Tan C H. New explicit constructions of differentially 4-uniform permutations via special partitions of $F_{2^{2k}}$. Finite Fields Their Appl, 2016, 40: 73–89
2 Peng J, Tan C H. New differentially 4-uniform permutations by modifying the inverse function on subfields. Cryptogr Commun, 2017, 9: 363–378
3 Peng J, Tan C H, Wang Q C. A new family of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for odd k. Sci China Math, 2016, 59: 1221–1234
4 Peng J, Tan C H, Wang Q C. New secondary constructions of differentially 4-uniform permutations over. Int J Comput Math, 2017, 94: 1670–1693
5 Qu L J, Tan Y, Tan C H, et al. Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method. IEEE Trans Inform Theor, 2013, 59: 4675–4686
6 Tang D, Carlet C, Tang X. Differentially 4-uniform bijections by permuting the inverse function. Des Codes Cryptogr, 2015, 77: 117–141
7 Tu Z, Zeng X, Zhang Z. More permutation polynomials with differential uniformity six. Sci China Inf Sci, 2018, 61: 038104
8 Zha Z B, Hu L, Sun S W, et al. Further results on differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$. Sci China Math, 2015, 58: 1577–1588
9 Xiong M, Yan H, Yuan P. On a conjecture of differentially 8-uniform power functions. Des Codes Cryptogr, 2018, 86: 1601–1621