More permutation polynomials with differential uniformity six

TU Ziran, ZENG Xiangyong and ZHANG Zhiyong

Citation: SCIENCE CHINA Information Sciences **61**, 038104 (2018); doi: 10.1007/s11432-017-9118-5

View online: http://engine.scichina.com/doi/10.1007/s11432-017-9118-5

View Table of Contents:http://engine.scichina.com/publisher/scp/journal/SCIS/61/3

Published by the Science China Press

SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

March 2018, Vol. 61 038104:1–038104:3
doi: 10.1007/s11432-017-9118-5

More permutation polynomials with differential uniformity six

Ziran TU[1], Xiangyong ZENG[2*] & Zhiyong ZHANG[3]

[1]*School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang* 471003*, China;*
[2]*Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan* 430062*, China;*
[3]*School of Information Engineering, Henan University of Science and Technology, Luoyang* 471003*, China*

Received 14 May 2017/Accepted 31 May 2017/Published online 25 August 2017

Citation Tu Z R, Zeng X Y, Zhang Z Y. More permutation polynomials with differential uniformity six. Sci China Inf Sci, 2018, 61(3): 038104, doi: 10.1007/s11432-017-9118-5

Differential analysis is one of the most important attacks threatening iterated block ciphers. To resist against differential attacks [1], the multi-output Boolean functions used in designing S-boxes should have low differential uniformity. For a positive integer n, the lowest differential uniformity of the functions from the finite field $\mathbb{F}_{2^n}$ (for a prime power q, $\mathbb{F}_q$ denotes the finite field with q elements, and $\mathbb{F}_q^*$ denotes $\mathbb{F}_q \setminus \{0\}$) to itself is 2, and these functions are called almost perfect nonlinear (APN). APN functions have been intensively studied in the last decades and researchers have made many interesting observations about them (the reader is referred to [2] and references therein). While the cubic map is an obvious APN permutation for odd dimension n, the existence of APN permutations for even dimension n has been a long-standing question. Very recently, the first example of APN permutation over $\mathbb{F}_{2^6}$ was found in [3], but the question on the existence of APN permutations in even dimension $n > 6$ still remains open. From the cryptographic point of view, permutations with low differential uniformity are therefore of great interest [4].

The inverse function over $\mathbb{F}_{2^8}$ is applied to design the S-box of the Advanced Encryption Standard (AES) [5], and it is a differentially 4-uniform permutation over $\mathbb{F}_{2^8}$. This motivates people to study the constructions of 4-uniform permutation polynomials with other desired properties, recent papers like [4]. can be referred. Further, some differentially 6 or 8-uniform monomials are considered [6, 7]. Simulations in [6] show that for $17 \leqslant n \leqslant 31$, all monomials over $\mathbb{F}_{2^n}$ differentially 6-uniform belong to the family

$$\left\{G_t(x) = x^{2^t-1},\ x \in \mathbb{F}_{2^n} :\ 1 < t < n\right\},$$

and some differentially 6-uniform power functions of this family are discussed in [6, 7].

Our purpose is to extend the study of 6-uniform functions and construct new differentially 6-uniform non-monomial functions. We propose a class of non-monomial permutations with differential uniformity at most 6, and the key idea is to use rational functions over finite fields. This can be regarded as a generalization of the construction of the inverse function over finite fields, and it is in fact a piecewise permutation [8].

Theorem 1. Let $n = 2m$ for a positive integer m and $\delta \in \mathbb{F}_{2^n}$ satisfying $\mathrm{Tr}_1^n(\delta) = 1$. Define $f(x) : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ as

$$f(x) = \begin{cases} \dfrac{1}{x^2 + x}, & \text{if } \mathrm{Tr}_1^n(\delta x) = 0, \\ \dfrac{1}{\delta x}, & \text{if } \mathrm{Tr}_1^n(\delta x) = 1, \end{cases}$$

* Corresponding author (email: xiangyongzeng@aliyun.com)
The authors declare that they have no conflict of interest.

where $\frac{1}{0}$ is defined to be 0. Then $f(x)$ is a permutation over $\mathbb{F}_{2^n}$ with $\Delta_f \leqslant 6$.

Proof. Firstly we investigate the permutation property of $f(x)$. Suppose $f(x) = f(y)$ for two distinct elements x and y of $\mathbb{F}_{2^n}$. When $\mathrm{Tr}_1^n(\delta x) = \mathrm{Tr}_1^n(\delta y) = 0$, we have $x^2+x = y^2+y$, then $x+y = 1$ due to $x \neq y$ and $\mathrm{Tr}_1^n(\delta x)+\mathrm{Tr}_1^n(\delta y) = \mathrm{Tr}_1^n(\delta) = 1$. This is impossible. The other two cases $\mathrm{Tr}_1^n(\delta x) = \mathrm{Tr}_1^n(\delta y) = 1$ and $\mathrm{Tr}_1^n(\delta x) \neq \mathrm{Tr}_1^n(\delta y)$ are similar. Then $f(x)$ permutes $\mathbb{F}_{2^n}$.

To determine the differential uniformity of $f(x)$, we need prove that for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, there are not more than six solutions in $\mathbb{F}_{2^n}$ of the differential equation

$$f(x) + f(x+a) = b. \tag{1}$$

When $b = 0$, obviously the above equation has no solutions in $\mathbb{F}_{2^n}$ because f is a permutation. Assume $b \neq 0$. Denote by $H_{ij} = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(\delta x) = i, \mathrm{Tr}_1^n(\delta(x+a)) = j\}$ and N_{ij} the number of solutions of (1) in H_{ij} for $i, j \in \{0, 1\}$. It suffices to prove that for any pair $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$,

$$\delta_f(a, b) = N_{00} + N_{01} + N_{10} + N_{11} \leqslant 6.$$

Observe that $N_{01} = N_{10}$ and Eq. (1) is equivalent to

$$\frac{1}{x^2+x} + \frac{1}{(x+a)^2+x+a} = b,\ x \in H_{00}, \tag{2}$$

$$\frac{1}{x^2+x} + \frac{1}{\delta(x+a)} = b,\ x \in H_{01}, \tag{3}$$

$$\frac{1}{\delta x} + \frac{1}{(x+a)^2+x+a} = b,\ x \in H_{10}, \tag{4}$$

$$\frac{1}{\delta x} + \frac{1}{\delta(x+a)} = b,\ x \in H_{11}. \tag{5}$$

Two cases $\mathrm{Tr}_1^n(\delta a) = 1$ and $\mathrm{Tr}_1^n(\delta a) = 0$ need to be distinguished.

(i) $\mathrm{Tr}_1^n(\delta a) = 1$. In this case, we have $N_{00} = N_{11} = 0$ since neither $\mathrm{Tr}_1^n(\delta x) = \mathrm{Tr}_1^n(\delta(x+a)) = 0$ nor $\mathrm{Tr}_1^n(\delta x) = \mathrm{Tr}_1^n(\delta(x+a)) = 1$ holds. Thus, it suffices to consider N_{01}. Note that $x = 0$ satisfies (3) if and only if $ab\delta = 1$. Further, neither $x = 1$ nor $x = a$ satisfies (3) since $x = 1$ satisfying (3) implies $1 = \mathrm{Tr}_1^n(\delta) = \mathrm{Tr}_1^n(\delta x) = 0$ while $x = a$ satisfying (3) implies $0 = \mathrm{Tr}_1^n(\delta(a+a)) = \mathrm{Tr}_1^n(\delta(x+a)) = 1$. If only the solutions not in $\{0, 1, a\}$ are considered, the equation $\frac{1}{x^2+x} + \frac{1}{\delta(x+a)} = b$ is equivalent to

$$x^2 + x + \delta(x+a) = b(x^2+x)\delta(x+a). \tag{6}$$

When $ab\delta \neq 1$, obviously $x = 0$ does not satisfy (3). The number of solutions to (6) is not more than 3 and then $N_2 \leqslant 3$. When $ab\delta = 1$, by multiplying (6) with a, we have

$$x^3 + x^2 + \delta ax + \delta a^2 = 0.$$

Suppose x_0, x_1, x_2 are three solutions of (6). By (3), we have $\mathrm{Tr}_1^n(\delta x_i) = 0$ for $i \in \{0, 1, 2\}$. From Vieta's theorem, $x_0 + x_1 + x_2 = 1$ and then $0 = \mathrm{Tr}_1^n(\delta x_0)+\mathrm{Tr}_1^n(\delta x_1)+\mathrm{Tr}_1^n(\delta x_2) = \mathrm{Tr}_1^n(\delta) = 1$, which is impossible. Thus Eq. (6) has at most two solutions. This together with $x = 0$ shows $N_2 \leqslant 3$.

(ii) $\mathrm{Tr}_1^n(\delta a) = 0$. Since $\mathrm{Tr}_1^n(\delta a) = 0$ contradicts with $\mathrm{Tr}_1^n(\delta a) = \mathrm{Tr}_1^n(\delta x) + \mathrm{Tr}_1^n(\delta(x+a)) = 1$ in (3) and (4), we have $N_{01} = N_{10} = 0$. Thus, it suffices to consider (2) and (5). Note (2) has $x = 0$, a as its two solutions if and only if $\frac{1}{a^2+a} = b$, we need consider the solutions of (2) not in $\{0, a\}$. The equation $\frac{1}{x^2+x} + \frac{1}{(x+a)^2+x+a} = b$ is equivalent to

$$a^2 + a = b(x^2+x)(x^2+x+a^2+a), \tag{7}$$

which has at most four solutions. Note that $x = 0$ or $x = a$ does not satisfy (7), otherwise we have $a^2 + a = 0$, which contradicts with $\frac{1}{a^2+a} = b \neq 0$. It can be observed that Eq. (7) has the set of solutions as the form $\{x_0, x_0+1, x_1, x_1+1\}$. However, from (2) the constraint $\mathrm{Tr}_1^n(\delta x_i) = \mathrm{Tr}_1^n(\delta(x_i + 1)) = 0$ for $i \in \{0, 1\}$ implies that $\mathrm{Tr}_1^n(\delta) = 0$, which is a contradiction. This shows

$$N_{00} \leqslant \begin{cases} 4, & \dfrac{1}{a^2+a} = b, \\ 2, & \dfrac{1}{a^2+a} \neq b. \end{cases}$$

Observe that Eq. (5) is equivalent to

$$\delta a = b\delta^2 x(x+a),$$

and then $N_{11} \leqslant 2$.

These analysis shows that for $b \neq 0$, the inequality

$$N_{00} + N_{01} + N_{10} + N_{11} \leqslant 6$$

holds.

Example 1. Let the finite field $\mathbb{F}_{2^4}$ be generated by the primitive polynomial $m(x) = x^4 + x + 1$ and ω be a root of $m(x)$. Take $\delta = \omega^{11}$ and then $\mathrm{Tr}_1^4(\delta) = 1$. So $f(x)$ defined by Theorem 1 is

$$f(x) = \begin{cases} \dfrac{1}{x^2+x}, & \text{if } \mathrm{Tr}_1^4(\omega^{11}x) = 0, \\ \dfrac{1}{\omega^{11}x}, & \text{if } \mathrm{Tr}_1^4(\omega^{11}x) = 1. \end{cases}$$

It can be verified that $f(x)$ permutes $\mathbb{F}_{2^4}$ with $\Delta(f) = 4$. If we take $\delta = \omega^3$, then $\Delta(f) = 6$.

Theorem 2. The algebraic degree of $f(x)$ is $n-1$.

Proof. By the definition of $f(x)$ in Theorem 1, we have

$$f(x) = \sum_{\mathrm{Tr}_1^n(\delta c)=0} \frac{1}{c^2+c}\left(1+(x+c)^{2^n-1}\right) + \sum_{\mathrm{Tr}_1^n(\delta c)=1} \frac{1}{\delta c}\left(1+(x+c)^{2^n-1}\right),$$

in which the coefficient of the term x^{2^n-1} is

$$\sum_{\mathrm{Tr}_1^n(\delta c)=0} \frac{1}{c^2+c} + \sum_{\mathrm{Tr}_1^n(\delta c)=1} \frac{1}{\delta c} = \sum_{c\in\mathbb{F}_{2^n}} f(c) = 0,$$

and the coefficient t_{2^n-2} of the term x^{2^n-2} is

$$t_{2^n-2} = \sum_{\mathrm{Tr}_1^n(\delta c)=0} \frac{c}{c^2+c} + \sum_{\mathrm{Tr}_1^n(\delta c)=1} \frac{c}{\delta c}.$$

Note that $\sum_{\mathrm{Tr}_1^n(\delta c)=1} \frac{c}{\delta c} = \sum_{\mathrm{Tr}_1^n(\delta c)=1} \frac{1}{\delta} = 0$, we have

$$\begin{aligned} t_{2^n-2} &= \sum_{\mathrm{Tr}_1^n(\delta c)=0,\, c\neq 0} \frac{c}{c^2+c} \\ &= \sum_{\mathrm{Tr}_1^n(\delta c)=0,\, c\neq 0} \frac{1}{c+1} = \sum_{\mathrm{Tr}_1^n(\delta c)=1,\, c\neq 1} \frac{1}{c} \\ &= 1+\sum_{\mathrm{Tr}_1^n(\delta c)=1} \frac{1}{c} = 1+\delta \sum_{\mathrm{Tr}_1^n(c)=1} \frac{1}{c}. \end{aligned}$$

It can be verified that

$$\prod_{\mathrm{Tr}_1^n(c^{-1})=1} (x+c) = x^{2^{n-1}} + \sum_{i=0}^{n-1} x^{2^{n-1}-2^i}. \quad (8)$$

Indeed, the left hand-side of (8) is the polynomial with all elements in $\{c \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(c^{-1}) = 1\}$ as its roots. Meanwhile, the equalities

$$\begin{aligned} \mathrm{Tr}_1^n(c^{-1}) = 1 &\Leftrightarrow \sum_{i=0}^{n-1} c^{-2^i} = 1 \\ &\Leftrightarrow \sum_{i=0}^{n-1} c^{2^{n-1}-2^i} = c^{2^{n-1}} \end{aligned}$$

indicate all elements in $\{c \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(c^{-1}) = 1\}$ also are roots of the polynomial $x^{2^{n-1}} + \sum_{i=0}^{n-1} x^{2^{n-1}-2^i}$. The equality (8) holds since the two polynomials both have algebraic degree 2^{n-1}. Note that $\sum_{\mathrm{Tr}_1^n(c)=1} \frac{1}{c} = \sum_{\mathrm{Tr}_1^n(c^{-1})=1} c$. Therefore, by Vieta's formula we have $\sum_{\mathrm{Tr}_1^n(c)=1} \frac{1}{c} = 1$ and then $t_{2^n-2} = 1+\delta \neq 0$ due to $\mathrm{Tr}_1^n(\delta) = 1$. By the definition of algebraic degree, we have $\deg(f) = n-1$ due to $wt(2^{n-1}-1) = n-1$.

Based on exponential sums and the knowledge of the function fields, the nonlinearity of the proposed permutation polynomials can be characterized.

Theorem 3. Let $n > 4$ be an even integer and $f(x)$ be a permutation constructed as in Theorem 1. Then we have

$$NL(f) \geqslant 2^{n-1} - 3\cdot 2^{\frac{n}{2}} - 1.$$

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 11401172, 61672212, 61370220).

Supporting information Appendix A. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. J Cryptol, 1991, 4: 3–72
2 Browning K, Dillon J, Kibler R, et al. APN polynomials and related codes. J Combin Inf Syst Sci, 2009, 34: 135–159
3 Browning K, Dillon J, McQuistan M, et al. An APN permutation in dimension six. In: Proceedings of the 9th Conference on Finite Fields and Applications FQ9, Dublin, 2010. 33–42
4 Bracken C, Leander G. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields Their Appl, 2010, 16: 231–242
5 Daemen J, Rijmen V. The design of rijndael. In: AES-The Advanced Encryption Standard. Berlin: Springer-Verlag, 2002. 221–227
6 Blondeau C, Canteaut A, Charpin P. Differential properties of $x \mapsto x^{2^t-1}$. IEEE Trans Inf Theory, 2011, 57: 8127–8137
7 Blondeau C, Perrin L. More differentially 6-uniform power functions. Designs Codes Cryptogr, 2014, 73: 487–505
8 Cao X, Hu L, Zha Z. Constructing permutation polynomials from piecewise permutations. Finite Fields Their Appl, 2014, 26: 162–174