A New Class of Differentially 4-uniform Permutations from the Inverse Function

Jian Bai, Dingkang Wang

KLMM, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China

Abstract

Differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ with high nonlinearity and algebraic degree are often used in block ciphers and some stream ciphers as Substitution boxes. Recently,Chen et al.(An equivalent condition on the switching construction of differentially 4-uniform permutations on from the inverse function, International Journal of Computer Mathematics, DOI:10.1080/00207160.2016.1167884) presented a n equivalent condition on the switching construction. More precisely,they presented a sufficient and necessary condition on differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ of the form $G(x) = x^{-1} + f(x^{-1})$, where f is a Boolean function. However, the number of the satisfied functions is so enormous that it is difficult to find all the functions. In this paper,a new class of such functions are constructed. These functions may provide more options for the design of Substitute boxes.

Keywords: Differentially 4-uniform permutation, Substitute box, 4-Uniform BFI, Preferred Boolean function

1. Introduction

In the design of many block ciphers, permutations are often chosen as Substitution boxes(S-boxes) to bring confusion into ciphers. To prevent various attacks on the cipher, such permutations are required to have low differential uniformity, high algebraic degree and high nonlinearity. Furthermore, for software implementation, such functions are usually required to be defined on fields with even degrees, namely $\mathbb{F}_{2^{2k}}$. Throughout this paper, we always let $n = 2k$ be an even integer.

It is well known that the lowest differential uniformity of a function defined on $\mathbb{F}_{2^{2k}}$ can achieve is 2 and such functions are called *almost perfect nonlinear* (APN) functions. On this aspect, they are the most ideal options for the design of Substitution boxes. However, it is difficult to find APN permutations over $\mathbb{F}_{2^{2k}}$, which is called *BIG APN* Problem. Due to the lack of knowledge on APN permutations on $\mathbb{F}_{2^{2k}}$, a natural trade-off solution is to use differentially 4-uniform permutations as S-boxes. Recently, many constructions of differentially permutations were introduced [1]–[5], [7]–[13]. In 2013, Qu et al. used

Email addresses: baijian@amss.ac.cn (Jian Bai), dwang@mmrc.iss.ac.cn (Dingkang Wang)

the powerful switching method [6] to successfully construct many infinite families of such permutations from the inverse function [7],[8]. In 2015, Chen et al. proved an equivalent condition on this method. More precisely, they studied the functions with the form $G(x) = x^{-1} + f(x^{-1})$, where f is a Boolean function. They proved that G is a differentially 4-uniform permutation over $\mathbb{F}_{2^{2k}}$ if and only if f is a *4-uniform Boolean function with respect to the inverse function* (4-uniform BFI).Furthermore, they construct a family of differentially 4-uniform permutations which is a subclass of all the 4-uniform BFIs. The number of permutations in this family is about 2^{n-5}.

In this paper, we construct a new infinite family of differentially 4-uniform permutations which is a subclass of all the 4-uniform BFIs. The number of permutations in this family is at least $2^{2^{n-2}}$ which is far more than before. These functions may provide more choices for the design of Substitution boxes.

2. Necessary Definition and Useful Lemmas

In this section, we give necessary definitions and results which will be used in the paper.

Given two positive integers n and m, a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called an (n, m)-*function*. Particularly, when $m = 1$, F is called an n-variabke *Boolean function*, or a *Boolean function* with n variables. Clearly, a Boolean function may be regarded as a vector with elements on $\mathbb{F}_2$ of length 2^n by identifying $\mathbb{F}_{2^n}$ with a vector space $\mathbb{F}_2^n$ OF dimension n over $\mathbb{F}_2$. In the following, we will switch between these two points of view without explanation if the context is clear.

Let f be a nonzero Boolean function. Define the set $\mathrm{Supp}(f) = \{x \in \mathbb{F}_{2^n} | f(x) = 1\}$ and call it the *support set* of f. The value $|\mathrm{Supp}(f)|$ is called the *(Hamming) weight* of f. Denote by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2i}$ the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Note that for the multiplicative inverse function x^{-1}, we always define $0^{-1} = 0$ below.

Let F be an (n, m)-function. Then F can be expressed uniquely as a polynomial over $\mathbb{F}_{2^n}$ with degree at most $2^n - 1$. It is called a *Permutation Polynomial* if it induces a permutation over $\mathbb{F}_{2^n}$. Denote by $\mathbb{F}_{2^n}^*$ the set of all nonzero elements of $\mathbb{F}_{2^n}$. For any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, define

$$\delta_F(a, b) = \sharp\{x : x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\}.$$

Note that we denote the cardinality of S by $\sharp S$. The multiset $\{* \ \delta_F(a, b) : (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} *\}$ is called the *differential spectrum* of F. The value

$$\Delta_F \triangleq \max_{(a,b)\in\mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} \delta_F(a, b)$$

is called the *differential uniformity* of F, or we call F a *differentially* Δ_F*-uniform* function. In particular, we call F *almost perfect nonlinear*(APN) if $\Delta_F = 2$. It is easy to see that APN functions achieve the lowest possible differential uniformity for functions defined on fields with an even characteristic.

3. Construct New Differentially 4-uniform Permutations

In [4] the authors introduced a type of functions called 4-uniform boolean function with respect to the inverse function (4-uniform BFI for short), and proposed a method to construct infinite families of permutations whose differentially uniformity are at most 4 of the form $G(x) = x^{-1} + f(x^{-1})$.

Theorem 3.1. [4]. *Let n be an even integer and f be an n-variable Boolean function. Let ω be an element of $\mathbb{F}_{2^n}$ with order 3. Then f is a 4-uniform BFI if and only if $f(x) = f(x+1)$ holds for any $x \in \mathbb{F}_{2^n}$ and for any $z \in \mathbb{F}_{2^n} \backslash \mathbb{F}_4$, at least one of the following two equations holds.*

$$f(0) + f(z + z^{-1} + 1) + f(\omega z + (\omega z)^{-1} + 1) + f(\omega^2 z + (\omega^2 z)^{-1} + 1) = 0 \tag{1}$$

$$f(0) + f(z + z^{-1} + 1) + f(\omega(z + (z)^{-1} + 1)) + f(\omega^2(z + (z)^{-1} + 1)) = 0 \tag{2}$$

Theorem 3.2. [4]. *Let n be an even integer and f be an n-variable Boolean function. Then $G(x) = x^{-1} + f(x^{-1})$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ if and only if f is a 4-uniform BFI.*

Lemma 3.3. *Let n be an even integer and ω be an element of $\mathbb{F}_{2^n}$ with order 3. We call the set $A_\alpha = \alpha\mathbb{F}_4^* + \mathbb{F}_4 = \{\alpha, \alpha+1, \alpha+\omega, \alpha+\omega^2, \omega\alpha, \omega\alpha+1, \omega\alpha+\omega, \omega\alpha+\omega^2, \omega^2\alpha, \omega^2\alpha+1, \omega^2\alpha+\omega, \omega^2\alpha+\omega^2\}$ a space set, where $\alpha \in \mathbb{F}_{2^n} \backslash \mathbb{F}_4\}$. Then $\{A_\alpha | \alpha \in \mathbb{F}_{2^n} \backslash \mathbb{F}_4\}$ is a partition of $\mathbb{F}_{2^n} \backslash \mathbb{F}_4$.*

Proof. Clearly $\mathbb{F}_{2^n} \backslash \mathbb{F}_4 = \bigcup_{\alpha \in \mathbb{F}_{2^n} \backslash \mathbb{F}_4} A_\alpha$. Assume that $x \in A_\alpha \cap A_\beta$,then there exists $a_1, b_1 \in \mathbb{F}_4^*$ and $a_2, b_2 \in \mathbb{F}_4$ such that $x = a_1\alpha + a_2 = b_1\beta + b_2$.Therefore, we have $\alpha = a_1^{-1}b_1\beta + a_1^{-1}(a_2 + b_2) \in A_\beta$ and $\beta = b_1^{-1}a_1\alpha + b_1^{-1}(a_2 + b_2) \in A_\alpha$. It is easy to verify that $A_\alpha = A_\beta$. The proof is finished. □

Theorem 3.4. *Let n be an even integer. Assume $4 \nmid n$. Let A_α be the same with the definition in Lemma 1. First, given the values of $f(0)$ and $f(\omega)$. Second, for arbitrary space set A_α, given the values of $f(\alpha)$, $f(\alpha+\omega)$ and $f(\omega\alpha)$. Third, let*

$$f(\omega^2\alpha) = f(\alpha) + f(\omega\alpha) + f(0) + 1,$$

$$f(\omega^2\alpha + \omega) = f(\alpha + \omega) + f(\omega\alpha) + f(0) + 1,$$

$$f(\omega\alpha + \omega) = f(\alpha) + f(\alpha + \omega) + f(\omega\alpha).$$

In the end, define $f(x) = f(x+1)$ for every $x \in \mathbb{F}_{2^n}$. Then $f(x)$ is a 4-uniform BFI. Hence $G(x) = x^{-1} + f(x^{-1})$ is a differentially 4-uniform permutations in $\mathbb{F}_{2^n}$. The number of such differentially 4-uniform permutations is $2^{2^{n-2}+1}$.

Proof. By Lemma 1, the boolean function is well defined. It is easy to verify that for any $z \in \mathbb{F}_{2^n} \backslash \mathbb{F}_4$, equation (2) of Theorem 1 holds. We know that $f(x) = f(x+1)$ for any $x \in \mathbb{F}_{2^n}$ by the last step of the construction. Therefore, $f(x)$ in the theorem is a 4-uniform BFI by Theorem 1.

During the construction, we have $2+\frac{2^n-4}{12}\times 3 = 2^{n-2}+1$ independent values. Hence the number of such permutations is $2^{2^{n-2}+1}$.

We finish the proof. □

Theorem 3.5. *Let n be an even integer. Assume $4|n$. Let A_α be the same with the definition in Lemma 1. Let $z \in \mathbb{F}_{16}$ such that $z + z^{-1} = \omega$. First, given the values of $f(0)$ and $f(\omega)$. Second, for arbitrary space set $A_\alpha \in \{A_\alpha | \alpha \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{16}\}$, given the values of $f(\alpha)$, $f(\alpha+\omega)$ and $f(\omega\alpha)$. Third, let*

$$f(\omega^2\alpha) = f(\alpha) + f(\omega\alpha) + f(0) + 1,$$
$$f(\omega^2\alpha+\omega) = f(\alpha+\omega) + f(\omega\alpha) + f(0) + 1,$$
$$f(\omega\alpha+\omega) = f(\alpha) + f(\alpha+\omega) + f(\omega\alpha).$$

Then given the values of $f(z)$ and $f(\omega z)$, define

$$f(\omega^2 z) = f(z) + f(\omega z) + f(0) + 1,$$
$$f(\omega^2 z+\omega) = f(z) + f(\omega z) + f(\omega) + 1,$$
$$f(\omega z+\omega) = f(\omega z) + f(0) + f(\omega).$$
$$f(z+\omega) = f(z) + f(0) + f(\omega).$$

In the end, define $f(x) = f(x+1)$ for every $x \in \mathbb{F}_{2^n}$. Then $f(x)$ is a 4-uniform BFI. Hence $G(x) = x^{-1} + f(x^{-1})$ is a differentially 4-uniform permutations in $\mathbb{F}_{2^n}$. The number of such differentially 4-uniform permutations is $2^{2^{n-2}}$.

4. Concluding Remarks

In this paper, a new infinite family of differentially 4-uniform permutations is constructed. The structure of these functions is very simple and the number of these functions are much more than the constructions in [4]. For further research, it is interesting to find other subclasses of 4-uniform BFI. A more inmortant chanllenge is the *BIG APN* Problem.

[1] Bracken, C., Leander, G.: A highly nonlinear differentially 4 uniform power map- ping that permutes fields of even degree. Finite Fields Appl. 16(4), 231–242 (2010)

[2] C. Bracken, C.H. Tan and Y. Tan, Binomial differentially 4-uniform permutations with high nonlinearity. Finite Fields and Their Applications, Vol. 18, No. 3, pp. 537-546, 2012.

[3] C. Carlet, On known and new differentially uniform functions. Information Security and Privacy, Vol. 6812, pp. 1-15, 2011.

[4] X. Chen, Y.Z. Deng, M. Zhu and L.J. Qu, An Equivalent Condition on the Switching Construction of Differentially 4-uniform Permutations on $\mathbb{F}_{2^{2k}}$ from the Inverse Function. International Journal of Computer Mathematics, DOI:10.1080/00207160.2016.1167884.

[5] C. Carlet, More constructions of APN and differentially 4-uniform functions by concatenation. Science China Mathematics, Vol. 56, No. 7, pp. 1373-1384, 2013.

[6] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic. Advances in Mathematical Communications. Vol. 3, No. 1, pp. 59-81, 2009.

[7] L.J. Qu, Y. Tan, C. Li and G. Gong, More Constructions of Differentially 4-uniform Permutations on $\mathbb{F}_{2^{2k}}$. Designs, Codes and Cryptography, Vol. 78, No. 2, pp. 391-408, 2016.

[8] L.J. Qu, Y. Tan, C. Tan and C. Li, Constructing Differentially 4-Uniform Permutations over $\mathbb{F}_{2^{2k}}$ via the Switching Method. IEEE Transactions on Information Theory, Vol. 59, No. 7, pp. 4675-4686, 2013.

[9] Y.Q. Li, M.S. Wang and Y.Y. Yu, Constructing Differentially 4-uniform Permutations over $\mathbb{F}_{2^{2k}}$ from the Inverse Function Revisited. https://eprint.iacr.org/2013/731.pdf.

[10] D. Tang, C. Carlet and X.H. Tang, Differentially 4-Uniform Bijections by Permuting the Inverse Function. Designs, Codes and Cryptography, Vol. 77, No. 1, pp. 117-141, 2015.

[11] Y.Y. Yu, M.S. Wang and Y.Q. Li, Constructing differential 4-uniform permutations from know ones. Chinese Journal of Electronics, Vol. 22, No. 3, pp. 495-499, 2013.

[12] Z.B. Zha, L. Hu and S.W. Sun, Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields and Their Applications, Vol. 25, pp. 64-78, 2014.

[13] Z.B. Zha, L. Hu, S.W. Sun and J.Y. Shan, Further results on a class of differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$. Science China Mathematics, Vol. 58, No. 7, pp. 1577-1588, 2015.