Constructing Differentially 4-uniform Involutions over $\mathbb{F}_{2^{2k}}$ by using the Carlitz form

Jaeseong Jeong[1], Namhun Koo[2], Soonhak Kwon[1]

Email: wotjd012321@naver.com, nhkoo@ewha.ac.kr, shkwon@skku.edu
[1]Applied Algebra and Optimization Research Center, Sungkyunkwan University, Suwon, Korea
[2]Institute of Mathematical Sciences, Ewha Womans University, Seoul, Korea

Abstract

Differentially 4-uniform involutions on $\mathbb{F}_{2^{2k}}$ play important roles in the design of substitution boxes(S-boxes). Despite the active research on differentially 4-uniform permutation, there are very few studies on differentially 4-uniform involutions, especially over the field $\mathbb{F}_{2^n}$ with $4|n$. In this paper, we construct new classes of differentially 4-uniform involutions by using the Carlitz form. With this approach, we explicitly construct two new classes of differentially 4-uniform involutions over $\mathbb{F}_{2^n}$ with even n (expecially including $4|n$). We also show that our constructions have high nonlinearity and an optimal algebraic degree. With the help of computer, we show that our constructions are CCZ-inequivalent to the known 4-uniform involutions over $\mathbb{F}_{2^8}$.

1 Introduction

In block ciphers, substitution boxes (S-boxes) play important roles in resisting resist several attacks. To prevent various attacks, S-boxes should have good cryptographic properties, for example low differential uniformity, high nonlinearity, and high algebraic degree. In the recent book [5], the readers could find more details about Boolean cryptographic functions and profound developments on the related criteria. For the efficient implementation, S-boxes are often chosen to be permutations over $\mathbb{F}_{2^n}$ with even n. A function having the lowest differential uniformity is called almost perfect nonlinear (APN) function. However, finding APN permutations over even dimensions, called the Big APN problem, is very difficult. Indeed, only one APN permutation over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, was found [4], and the case for $\mathbb{F}_{2^8}$ is completely open. Therefore a natural tradeoff is to choose differentially 4-uniform permutation S-boxes. In this approach, constructions of differentially 4-uniform permutation have been studied extensively [2, 3, 7, 11, 12, 15–17, 20, 22–32].

An involution $\mathcal{I}$ is a permutation satisfying $\mathcal{I} = \mathcal{I}^{-1}$ where $\mathcal{I}^{-1}$ is the compositional inverse of $\mathcal{I}$. (for details, see also [10]) Due to this property, an involution S-box can be used on both encryption and decryption, which leads to an advantage on the efficient design of the system. Because of this advantage of implementation, the construction of differentially 4-uniform involutions is crucial in the block cipher. For example, the Advanced Encryption Standard(AES) uses the multiplicative inverse function, which is a differentially 4-uniform involution having maximal nonlinearity and algebraic degree [18]. Since the inverse function has good cryptographic properties, modifications of the inverse function are often used in the construction of new differentially 4-uniform involutions. For example, some differentially 4-uniform involutions are constructed by modifying few points of the inverse function [11, 13, 17, 21]. However finding differentially 4-uniform involutions over $\mathbb{F}_{2^n}$ with $4|n$ is rather difficult, and very few examples are known so far. (See [11].)

The Carlitz rank, first introduced in [1], is the concept based on the known result that all permutations can be expressed by compositions of the inverse function and linear permutations. In the case of a finite field of odd characteristic, differential uniformity of permutations with

Carlitz rank 1 or 2 can be found in [9]. In the case of even characteristic, differential uniformity of permutations with Carlitz rank 1,2 or 3 can be found in [13].

In this paper, we give new classes of differentially 4-uniform involutions over $\mathbb{F}_{2^{2k}}$ obtained by using permutations of Carlitz rank greater than 3. Our method provides plenty of examples of 4-uniform involutions over $\mathbb{F}_{2^n}$ with $4|n$, which were not known so far. We also study other cryptographic properties such as nonlinearity and algebraic degree, and give some theoretical bounds. Moreover, we present numerical results about our construction, for example the number of our involutions, differential spectrum and nonlinearity.

2 Construction of differentially 4-uniform involutions on $\mathbb{F}_{2^{2k}}$

Throughout the rest of this paper, we let Inv_n denote the multiplicative inverse function on $\mathbb{F}_{2^n}$, that is $Inv_n(x) = x^{-1}$ on $\mathbb{F}_{2^n}$ (as usual $0^{-1} \stackrel{\text{def}}{=} 0$). If n is clear from the context, then we omit the subscript, that is we use Inv instead of Inv_n. We consider the rational transform $r : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$,

$$r(x) = \frac{ax+b}{cx+d} = \frac{a}{c} + \frac{ad+bc}{c(cx+d)}$$

as a permutation on $\mathbb{F}_{2^n}$ where $a, b, c, d \in \mathbb{F}_{2^n}$ and $c \neq 0$, by defining $r(\frac{d}{c}) = \frac{a}{c}$. We define a finite field analogue of continued fraction of real numbers as:

$$[a_1, a_2, \ldots, a_{m-2}, a_{m-1}, a_m] = ((\cdots(a_m^{-1} + a_{m-1})^{-1} + \cdots)^{-1} + a_2)^{-1} + a_1$$

For any permutation $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, F can be represented as

$$F(x) = [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x] = ((\cdots((a_0 x + a_1)^{-1} + a_2)^{-1} + \cdots)^{-1} + a_m)^{-1} + a_{m+1}$$

where $m \geq 0$, $a_0, a_2, \ldots a_m \in \mathbb{F}_{2^n}^*$ and $a_1, a_{m+1} \in \mathbb{F}_{2^n}$. In other words, any permutation can be expressed by compositions of inverse function and linear permutations $ax + b$ ($a \neq 0$), and we call this expression *Carlitz form.* The above expression is not unique in general. However, there is the least $m \geq 0$ among all possible expressions of F. The *Carlitz rank* of F, denoted by $\mathrm{crk}(F)$, is the least nonnegative integer m satisfying the above expression. We summarize some basic properties of the Carlitz form. (For details, see [1, 8, 9])

Proposition 2.1. *Let $F(x) = [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x]$ be a permutation of the Carlitz form on $\mathbb{F}_{2^n}$ and R be the rational transform*

$$R(x) = \frac{\alpha_{m+1} x + \beta_{m+1}}{\alpha_m x + \beta_m} \tag{1}$$

where

$$\alpha_{k+1} = a_{k+1}\alpha_k + \alpha_{k-1}, \;\; \beta_{k+1} = a_{k+1}\beta_k + \beta_{k-1} \quad (1 \leq k \leq m)$$

with the initial conditions $\alpha_0 = 0, \alpha_1 = a_0$ and $\beta_0 = 1, \beta_1 = a_1$. Then the followings are satisfied:

(i) $\alpha_{k+1}\beta_k + \alpha_k\beta_{k+1} = a_0$ *for* $1 \leq k \leq m$.

(ii) $F(x) = R(x)$ *for all* $x \notin \{\frac{\beta_i}{\alpha_i} \;:\; \alpha_i \neq 0,\ 1 \leq i \leq m\}$.

By Proposition 2.1-(ii), given a Carlitz form F and a rational transform R defined in (1), there exists a permutation π on $\mathbb{F}_{2^n}$ and the set P such that

$$F = R \circ \pi \text{ and } P = \{x \in \mathbb{F}_{2^n} : \pi(x) \neq x\} \tag{2}$$

where $\circ$ denotes the function composition and $P \subset \left\{\frac{\beta_i}{\alpha_i} \;:\; \alpha_i \neq 0,\ 1 \leq i \leq m\right\}$. It turns out that $\pi(P) = P$, and the explicit permutation structure of π on $\left\{\frac{\beta_i}{\alpha_i} \;:\; \alpha_i \neq 0,\ 1 \leq i \leq m\right\}$ can be found in [1, 8, 9, 13]. Let $\tau = (c_1, c_2, \ldots, c_m)$ denotes the cyclic permutation (cycle)

$$\tau(x) = \begin{cases} c_{i+1} & \text{if } x = c_i \text{ for } 1 \leq i \leq m \\ x & \text{otherwise} \end{cases}$$

where c_{m+1} is regarded as c_1.

For a given permutation F on $\mathbb{F}_{2^n}$, we define a permutation $\mathcal{I}_F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ as

$$\mathcal{I}_F \stackrel{\text{def}}{=} F \circ Inv \circ F^{-1}, \text{ that is } \mathcal{I}_F(x) = F\left(\frac{1}{F^{-1}(x)}\right)$$

where F^{-1} is the compositional inverse of F . Then $\mathcal{I}_F$ is an involution because $\mathcal{I}_F \circ \mathcal{I}_F = F \circ Inv \circ F^{-1} \circ F \circ Inv \circ F^{-1} = id$ where id is the identity function.

2.1 The first construction of differentially 4-uniform involution

Let $F(x) = [0, c, c^{-1}, d, x]$ be a permutation on $\mathbb{F}_{2^n}$ with even n. Then it follows that

$$F(x) = \begin{cases} 0, & x = d^{-1} =: p_1 \\ c^{-1}, & x = (c+d)^{-1} =: p_2 \\ c^{-2}(c+d) + c^{-2}x^{-1} =: R(x), & x \notin P = \{p_1, p_2\} \end{cases}$$

that is $F = R \circ \pi$ where $\pi = (p_1, p_2)$.

From the setting of the above F with $P = \{p_1, p_2\}$, we are ready to state our first (explicit) construction of differentially 4-uniform involutions.

Construction 1. *Let F be defined as above and suppose that all elements of $Q = P \cup P^{-1} = \{p_1, p_2, p_1^{-1}, p_2^{-1}\}$ are distinct with $p_1 p_2^{-1} \notin \mathbb{F}_4$. If the following 5 trace conditions are satisfied,*

$$\mathrm{Tr}(1/(p_2+p_1^{-1})) = \mathrm{Tr}(1/(p_1+p_2^{-1})) = \mathrm{Tr}(1/((p_1+p_1^{-1})(p_2+p_2^{-1}))) = \mathrm{Tr}(p_2/p_1) = \mathrm{Tr}(p_1/p_2) = 1,$$

then $\mathcal{I}_F$ is differentially 4-uniform involution on $\mathbb{F}_{2^n}$.

2.2 The second construction of differentially 4-uniform involution

Let $F(x) = [0, c, c^{-1}, d + d^2, d^{-1}, d, x]$ on $\mathbb{F}_{2^n}$ with even n. Then it follows that

$$F(x) = \begin{cases} c^{-2}d^2 + c^{-1} + c^{-2}d, & x = 0 \\ c^{-2}d^2 + c^{-1}, & x = d^{-1} =: p_1 \\ 0, & x = 1 \\ c^{-1}, & x = 1 + cd^{-2} =: p_2 \\ c^{-2}d^2 + c^{-1} + c^{-2}d^2x =: R(x) & x \notin P = \{0, 1, p_1, p_2\}, \end{cases}$$

that is $F = R \circ \pi$ where $\pi = (0, p_1)(1, p_2)$.

From the setting of the above F with $P = \{0, 1, p_1, p_2\}$, we are ready to state our second construction of differentially 4-uniform involutions.

Construction 2. *Let F be defined as above and suppose that all elements of $Q = P \cup P^{-1} = \{0, 1, p_1, p_2, p_1^{-1}, p_2^{-1}\}$ are distinct and $p_1, p_2 \notin \mathbb{F}_4$. If the following 10 trace conditions are satisfied,*

$$\mathrm{Tr}(1/(p_1+p_2)) = \mathrm{Tr}(1/(p_1+1)) = \mathrm{Tr}(1/((p_1+1)(p_1+p_2^{-1}))) = \mathrm{Tr}(1/(p_2(p_2+p_1^{-1}))) = \mathrm{Tr}(p_2/(p_2+1)^3) =$$
$$\mathrm{Tr}(p_1) = \mathrm{Tr}(1/(p_2+1)) = \mathrm{Tr}(1/(p_1^{-1}+p_2^{-1})) = \mathrm{Tr}(p_2/(p_1^{-1}+1)) = \mathrm{Tr}(1/(1+p_1^{-1}+p_2^{-1})) = 1,$$

then $\mathcal{I}_F$ is differentially 4-uniform involution on $\mathbb{F}_{2^n}$.

3 Nonlinearity and algebraic degree of proposed involutions

Theorem 3.1. *Let $F(x) = [a_{m+1}, a_m, a_{m-1}, \cdots, a_3, a_2, a_1 + a_0 x]$ on $\mathbb{F}_{2^n}$ with $\alpha_m \beta_m = 0$. Let $F = R \circ \pi$ and $Q = P \cup P^{-1}$. Then the nonlinearity of the involution $\mathcal{I}_F$ is*

$$nl(\mathcal{I}_F) \geq 2^{n-1} - 2^{\frac{n}{2}} - \#Q.$$

Corollary 3.2. *The involutions in Construction 1 and Construction 2 are of algebraic degree $n-1$.*

4 Numerical Results

In this section, we give some numerical results. With the help of software SageMath, we count the number of involutions satisfying the conditions in Construction 1 and Construction 2, respectively. The result is shown in Table 1:

n	N_1	D_1	N_2	D_2
4	0	0	0	0
6	144	$\approx 2^{-4.830}$	0	0
8	2112	$\approx 2^{-4.496}$	104	$\approx 2^{-9.300}$
10	29200	$\approx 2^{-5.166}$	910	$\approx 2^{-10.170}$
12	531648	$\approx 2^{-4.953}$	15972	$\approx 2^{-10.037}$
14	8423632	$\approx 2^{-4.994}$	271096	$\approx 2^{-9.952}$
16	133344640	$\approx 2^{-5.009}$	4106624	$\approx 2^{-10.030}$

Table 1: Number of involutions in Construction 1 and Construction 2

where N_i denotes the number of involutions in Construction i, $D_i = N_i/2^{2n}$ for $i \in \{1, 2\}$.

We checked that our constructions are (previously undiscovered) new involutions by computing CCZ-invariant quantities. It is well-known that the differential spectrum and the extended Walsh spectrum are invariant under CCZ-equivalence. By computing the differential spectrum and the extended Walsh spectrum, we count the number of CCZ-inequivalence classes. The result is shown in Table 2.

n	# Construction 1	# Construction 2
4	0	0
6	6	0
8	66	13
10	1495	94

Table 2: Number of CCZ-inequivalence involutions in Construction 1 and Construction 2

5 Conclusion

In this paper, we presented a new methodology for constructing differentially 4-uniform involutions by using permutations of low Carlitz rank, which enables us to find new classes of differentially 4-uniform involutions over $\mathbb{F}_{2^n}$ when n is even, especially when $4|n$ (not many 4-uniform involutions are known over $\mathbb{F}_{2^n}$ with $4|n$ so far). We applied our method explicitly to the following permutations.

$$F(x) = [0, c, c^{-1}, d, x] \text{ and } F(x) = [0, c, c^{-1}, d + d^2, d^{-1}, d, x],$$

and obtained new classes of differentially 4-uniform involutions $\mathcal{I}_F$ over $\mathbb{F}_{2^n}$ with $n \equiv 0, 2 \pmod 4$, where

$$\mathcal{I}_F(x) = [0, a_m, \ldots, a_2, a_2, \ldots, a_m, x] \quad (F(x) = [0, a_m, \ldots, a_2, x]).$$

The algebraic degree and a lower bound of nonlinearity of the proposed involutions have been given. The results show that they possess a high nonlinearity and an optimal algebraic degree.

The implementation results, via SAGE, show that there are many CCZ-inequivalent classes of our 4-uniform involutions, which means that our constructions are indeed new results. In particular, there exist many 4-uniform involutions in our constructions when n is multiple of 4.

References

[1] E. Aksoy, A. Cesmelioglu, W. Meidl and A. Topuzoğlu, On the Carlitz rank of permutation polynomials, Finite Fields and Their Applications, Vol. 15, pp. 428-440 (2009) DOI : 10.1016/j.ffa.2009.02.006

[2] C. Bracken, G. Leander, A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, *Finite Fields Appl.* 16(4) (2010) 231-242. DOI : 10.1016/j.ffa.2010.03.001

[3] C. Bracken, C. H. Tan, and Y. Tan, Binomial differentially 4 uniform permutations with high nonlinearity, *Finite Fields Appl.* 18(3) (2012) 537-546. DOI : 10.1016/j.ffa.2011.11.00

[4] 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

[5] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge (2021)

[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] C. Carlet, D. Tang, X. Tang, and Q. Liao, New Construction of Differentially 4-Uniform Bijections, *D. Lin et al. (Eds.): Inscrypt 2013, Lect. Notes Comput. Sci.* 8567 (2014) 22–38. DOI : 10.1007/978-3-319-12087-4 2

[8] A. Çesmelioğlu, W. Meidl and A. Topuzoğlu, On the cycle structure of permutation polynomials, Finite Fields and Their Applications, Vol. 14, pp. 593-614 (2008) DOI : 10.1016/j.ffa.2007.08.003

[9] A. Çesmelioğlu, W. Meidl and A. Topuzoğlu, Permutations of finite fields with prescribed properties, Journal of Computational and Applied Mathematics, Vol. 259, pp. 536-545 (2014) DOI : 10.1016/j.cam.2013.07.036

[10] P. Charpin, S. Mesnager, and S. Sarkar, Involutions Over the Galois Field F_{2^n}. *IEEE Trans. Inf. Theory* 62(4) (2016) 2266-2276

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

[12] S. Fu, X. Feng, and B Wu, Differentially 4-Uniform Permutations with the Best Known Nonlinearity from Butterflies, *IACR Transactions on Symmetric Cryptology* 2017(2) (2017) 228-249. DOI : 10.13154/tosc.v2017.i2.228-249

[13] J. Jeong, N. Koo, and S. Kwon, On the Boomerang Uniformity of Permutations of Low Carlitz Rank, a preprint, Available at : https://arxiv.org/abs/2009.08612

[14] G. Lachaud and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE Trans. Inf. Theory* 36(3) (1990) 686-692. DOI : 10.1109/18.54892

[15] Y. Leng, J. Chen, and T. Xie, More Low Differential Uniformity Permutations over $\mathbb{F}_{2^{2k}}$ with k Odd, *Mathematical Problems in Engineering* 2020, Article ID 7152657. DOI : 10.1155/2020/7152657

[16] Y. Li, and M. Wang, Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$, *Des. Codes Cryptogr.* 72(2) (2014) 249-264. DOI : 10.1007/s10623-012-9760-9

[17] Y. Li, M. Wang and Y. Yu, Constructing Differentially 4-uniform Permutations over $GF(2^{2k})$ from the Inverse Function Revisited, eprint.iacr.org/2013/731

[18] K. Nyberg, Differentially uniform mappings for cryptography, *In: Helleseth T. (eds) Advances in Cryptology — EUROCRYPT '93. Lect. Notes Comput. Sci.* 765 (1994) 55-64, Springer, Berlin, Heidelberg. DOI : 10.1007/3-540-48285-7_6

[19] J. Peng, and C. H. Tan, New differentially 4-uniform permutations by modifying the inverse function on subfields, *Cryptogr. Commun.* 9(3) (2017) 363-378. DOI : 10.1007/s12095-016-0181-x

[20] J. Peng, and C. H. Tan, New explicit constructions of differentially 4-uniform permutations via special partitions of $\mathbb{F}_{2^{2k}}$, *Finite Fields Appl.* 40 (2016) 73-89. DOI : 10.1016/j.ffa.2016.03.003

[21] J. Peng, C. H. Tan, and Q. Wang, A new family of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for odd k, *Sci. China Math.* 59(6) (2016) 1221-1234. DOI: 10.1007/s11425-016-5122-9

[22] J. Peng, C. H. Tan, Q. Wang, J. Gao, and H. Kan, More New Classes of Differentially 4-Uniform Permutations with Good Cryptographic Properties, *IEICE Trans. on Fundamentals* E101-A (6) (2018) 945-952. DOI: 10.1587/transfun.E101.A.945

[23] L. Qu, Y. Tan, C. Li, and G. Gong, More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$, *Des. Codes Cryptogr.* 78(2) (2016) 391-408. DOI :10.1007/s10623-014-0006-x

[24] L. Qu, Y. Tan, C.H. Tan and C. Li, Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method, *IEEE Trans. Inf. Theory* 59(7) (2013) 4675–4686. DOI : 10.1109/TIT.2013.2252420

[25] L. Shuai, and M. Li, A method to calculate differential uniformity for permutations, *Des. Codes Cryptogr.* 86(7) (2018) 1553-1563. DOI : 10.1007/s10623-017-0412-y

[26] L. Shuai, L. Wang, L. Miao, and X. Zhou, Differential uniformity of the composition of two functions, *Cryptogr. Commun.* 12(2) (2020) 205-220. DOI : 10.1007/s12095-019-00382-6

[27] Y. Sin, K. Kim, R. Kim, and S. Han, Constructing new differentially 4-uniform permutations from known ones, *Finite Fields Appl.* 63 (2020) 101646. DOI : 10.1016/j.ffa.2020.101646

[28] D. Tang, C. Carlet and X. Tang, Differentially 4-uniform bijections by permuting the inverse function, *Des. Codes Cryptogr.* 77(1) (2015) 117-141. DOI : 10.1007/s10623-014-9992-y

[29] Y. Xu, Y. Li, C Wu, and F. Liu, On the construction of differentially 4-uniform involutions, *Finite Fields Appl.* 47 (2017) 309-329. DOI : 1010.1016/j.ffa.2017.06.004

[30] Z. Zha, L. Hu, and S. Sun, Constructing new differentially 4-uniform permutations from the inverse function, *Finite Fields Appl.* 25 (2014) 64-78. DOI : 10.1016/j.ffa.2013.08.003

[31] Z. Zha, L. Hu, S. Sun, and J. Shan, Further results on differentially 4-uniform $\mathbb{F}_{2^{2m}}$, *Sci. China Math.* 58(7) (2015) 1577-1588. DOI : 10.1007/s11425-015-4996-2

[32] X. Zhu, X. Zeng, and Y. Chen, Some Binomial and Trinomial Differentially 4-Uniform Permutation Polynomials, *Int. J. Found. Comput. Sci.* 26(4) (2015) 487-497. DOI : 10.1142/S0129054115500276