New Construction of Differentially 4-Uniform Bijections

Claude Carlet[1], Deng Tang[1,2](✉), Xiaohu Tang[2], and Qunying Liao[3]

[1] LAGA, Department of Mathematics, University of Paris 8, CNRS, UMR 7539,
2 Rue de la Liberté, 93526 Saint-Denis Cedex 02, France
claude.carlet@univ-paris8.fr

[2] Provincial Key Lab of Information Coding and Transmission,
Institute of Mobile Communications, Southwest Jiaotong University,
Chengdu 610031, China
deng.tang@etud.univ-paris8.fr, xhutang@ieee.org

[3] Institute of Mathematics and Software Science, Sichuan Normal University,
Chengdu 610066, China
qunyingliao@sicnu.edu.cn

Abstract. Block ciphers use Substitution boxes (S-boxes) to create confusion into the cryptosystems. For resisting the known attacks on these cryptosystems, the following criteria for functions are mandatory: low differential uniformity, high nonlinearity and not low algebraic degree. Bijectivity is also necessary if the cipher is a Substitution-Permutation Network, and balancedness makes a Feistel cipher lighter. It is well-known that almost perfect nonlinear (APN) functions have the lowest differential uniformity 2 (the values of differential uniformity being always even) and the existence of APN bijections over $\mathbb{F}_{2^n}$ for even $n \geq 8$ is a big open problem. In real practical applications, differentially 4-uniform bijections can be used as S-boxes when the dimension is even. For example, the AES uses a differentially 4-uniform bijection over $\mathbb{F}_{2^8}$. In this paper, we first propose a method for constructing a large family of differentially 4-uniform bijections in even dimensions. This method can generate at least $\left(2^{n-3} - \lfloor 2^{(n-1)/2-1} \rfloor - 1\right) \cdot 2^{2^{n-1}}$ such bijections having maximum algebraic degree $n-1$. Furthermore, we exhibit a subclass of functions having high nonlinearity and being CCZ-inequivalent to all known differentially 4-uniform power bijections and to quadratic functions.

Keywords: Block cipher · Substitution box · Differential uniformity · CCZ-equivalence · Nonlinearity

1 Introduction and Preliminaries

In Shannon's terms [12], the generally accepted design principles for conventional ciphers are confusion and diffusion. These two design principles are very general

© Springer International Publishing Switzerland 2014
D. Lin et al. (Eds.): Inscrypt 2013, LNCS 8567, pp. 22–38, 2014.
DOI: 10.1007/978-3-319-12087-4_2

and informal. In practice, every block cipher uses Substitution boxes (S-boxes) to create confusion and uses some well chosen linear transformations (related to codes of large minimum distance) to bring diffusion into the cryptosystem. If the cipher is a Substitution-Permutation Network as in the AES, then we need the S-boxes to be bijections (to ensure invertibility).

Given two integers n and m, any S-box with n input bits and m output bits, which is often called an (n, m)-function or a vectorial Boolean function if the values n and m are omitted, can be viewed as a function G from the vectorial space $\mathbb{F}_2^n$ to the vectorial space $\mathbb{F}_2^m$. Particularly, G is called a Boolean function when $m = 1$. We denote by $\mathcal{B}_n$ the set of Boolean functions of n variables. The basic representation of any Boolean function $f \in \mathcal{B}_n$ is by its truth table, i.e.,

$$f = \big[f(0, 0, \cdots, 0), f(1, 0, \cdots, 0), \cdots, f(0, 1, \cdots, 1), f(1, 1, \cdots, 1)\big].$$

We say that a Boolean function $f \in \mathcal{B}_n$ is balanced if its truth table contains an equal number of ones and zeros, that is, if its Hamming weight equals 2^{n-1}, where the Hamming weight of f, denoted by $\mathrm{wt}(f)$, is the number of nonzero values in its truth table. Given two Boolean functions f and g on n variables, the Hamming distance between f and g is defined as $d_H(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|$.

Let G be an (n, m)-function, the Boolean functions $g_1(x), \cdots, g_m(x)$ defined by $G(x) = (g_1(x), \cdots, g_m(x))$ are called the coordinate functions of G. Further, the Boolean functions, which are the linear combinations, with non all-zero coefficients of the coordinate functions of G, are called component functions of G. The component functions of G can be expressed as $a \cdot G$ where $a \in \mathbb{F}_2^{m*}$. If we identify every element of $\mathbb{F}_2^m$ with an element of finite field $\mathbb{F}_{2^m}$, then the component functions of G can be expressed as $tr_1^n(\alpha G)$, where $\alpha \in \mathbb{F}_{2^n}^*$ and $tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. To resist the known attacks on each model of block cipher (and hopefully, to resist future attacks), the S-boxes used in ciphers should satisfy various design criteria simultaneously. The design criteria on S-boxes result in necessary properties of the component functions and of the vectorial function itself.

Let $x = (x_1, x_2, \cdots, x_n)$ and $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ both belong to $\mathbb{F}_2^n$ and let $x \cdot \alpha$ be any inner product, for instance the usual one, defined as $x \cdot \alpha = x_1\alpha_1 \oplus x_2\alpha_2 \oplus \cdots \oplus x_n\alpha_n$, then the Walsh transform of G at $(a, b) \in \mathbb{F}_2^{m*} \times \mathbb{F}_2^n$ is defined as

$$W_G(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot G(x) + b \cdot x}.$$

Usually, we call extended Walsh spectrum of G the multi-set of their absolute values. To resist linear cryptanalysis [10], S-boxes used in cryptosystems should have high nonlinearity. The nonlinearity $nl(G)$ of an (n, m)-function G is the minimum Hamming distance between all the component functions of G and all affine functions on n variables. According to the definition of Walsh transform, we have

$$\begin{aligned} nl(G) &= 2^{n-1} - \frac{1}{2} \max_{(a,b)\in\mathbb{F}_2^{m*}\times\mathbb{F}_2^n} |W_G(a,b)| \\ &= 2^{n-1} - \frac{1}{2} \max_{(\alpha,\beta)\in\mathbb{F}_{2^m}^*\times\mathbb{F}_{2^n}} |W_G(\alpha,\beta)|. \end{aligned}$$

It is well-known that the nonlinearity $nl(G)$ is upper-bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$ when $n = m$ and the best known value of $nl(G)$ is $2^{n-1} - 2^{\frac{n}{2}}$ when $n = m$ is even.

Any (n, m)-function G can be represented in univariate form:

$$G(x) = \sum_{i=0}^{2^n-1} a_i x^i, a_i \in \mathbb{F}_{2^n}.$$

The algebraic degree, denoted by $\deg(G)$, equals the maximal 2-weight of the exponent i such that $a_i \neq 0$, where the 2-weight of a given integer i is the number of ones in its binary expansion. It is known that the maximum algebraic degree of bijective functions in dimension n is $n-1$. Functions used as S-boxes should have high (or at least not low) algebraic degree to withstand the higher order differential attack [7] which is described by Knudsen when the degree is 2 but a degree 3 seems still insufficient and a degree at least 4 is safer.

The differential attack introduced by Biham and Shamir [1] is a powerful cryptanalytic method for attacking block ciphers. For measuring the ability of a given function to resist the differential attack [1], Nyberg [11] introduced a concept which is called differential δ-uniformity:

Definition 1. *An (n, m)-function G is called differentially δ-uniform if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, the equation $G(x) + G(x + a) = b$ has at most δ solutions.*

For every $a \in \mathbb{F}_2^{n*}$ and every $b \in \mathbb{F}_2^m$, if we denote by $\delta_G(a, b)$ the size of the set $\{x \in \mathbb{F}_2^n \,|\, G(x) + G(x + a) = b\}$, then we can see that δ equals the maximum value of $\delta_G(a, b)$. The multi-set $[\delta_G(a, b) \,|\, a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^m]$ is called the differential spectrum of G. The smaller δ is, the better is the contribution of G to a resistance to differential attack. When $m = n$, the smallest possible value of δ is 2 (since if x is a solution of equation $G(x)+G(x+a) = b$ then $x+a$ is also a solution, hence the values of δ are even); the functions achieving this value are called almost perfect nonlinear (APN) functions. APN functions have the lowest differential uniformity. Up to now, there is only one sporadic example of APN bijection for $n = 6$, found in [3] and it is a big open problem to know whether there exist APN bijections over $\mathbb{F}_{2^n}$ for even $n \geq 8$. So, for resisting differential attacks in even dimension, we need to choose differentially 4-uniform bijections as S-boxes (differential 4-uniformity is not optimal but it can withstand differential attacks in an efficient way; for example, the AES uses a differentially 4-uniform bijection with 8 input bits). For the convenience of the readers, we give in Sect. 2 a brief description of known APN bijections and differentially 4-uniform bijections in even dimensions.

These notions are preserved by extended affine equivalence (in brief, EA equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence): two (n, n)-functions G and H are called affine equivalent if one is equal to the other, composed on the left and on the right by affine permutations; they are called EA-equivalent if one is affine equivalent to the other, added with an affine function; they are called CCZ-equivalent if their graphs $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \,|\, y = G(x)\}$ and $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \,|\, y = H(x)\}$ are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $y = G(x) \Leftrightarrow L_2(x, y) = H(L_1(x, y))$ (where L_1 and L_2 are two affine functions from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ to $\mathbb{F}_2^n$). It is well-known that EA equivalence implies CCZ-equivalence, but the converse is false. Both EA and CCZ-equivalence preserve the differential spectrum and extended Walsh spectrum. But CCZ-equivalence does not respect the algebraic degree, while EA equivalence does.

Ideally, the dimension n of bijections used in cryptosystems should be a power of 2 for an efficient implementation in both hardware and software since it allows decomposing optimally the computation of the output in $\mathbb{F}_{2^n}$ into computations in subfields. This is also more convenient for the design of the whole cipher, for instance the number of input bits of the AES is 8. In practice, S-boxes used in cryptosystems should satisfy a tradeoff between security and efficient implementation simultaneously. Therefore, it is very interesting to construct bijections with good cryptographic properties in even dimensions. In the present paper, we construct a family of differentially 4-uniform bijections of even dimensions $n \geq 6$ by concatenating two $(n-1, n)$-functions. For every even $n \geq 6$, this family includes at least $\left(2^{n-3} - \lfloor 2^{(n-1)/2-1} \rfloor - 1\right) \cdot 2^{2^{n-1}}$ bijections, all of algebraic degree $n-1$. We also mathematically prove that, for any even $n \geq 8$, bijections in this family are CCZ-inequivalent to the Gold functions, the Kasami functions, the functions discussed in [2] and to quadratic functions. Further, we show a subclass of the family which has nonlinearity at least $2^{n-1} - 2\lfloor 2^{(n+1)/2} \rfloor - 4$ and is CCZ-inequivalent to all known differentially 4-uniform power bijections and to quadratic functions.

The paper is organized in the following way: Sect. 2 summarizes the known differentially 4-uniform bijections in even dimensions. A family of differentially 4-uniform bijections is presented in Sect. 3, and its algebraic degree, Walsh spectrum and CCZ-equivalence with known functions is studied. In Sect. 4, we give a subclass of differentially 4-uniform bijections with good cryptographic properties. Finally, Sect. 5 concludes the paper.

2 The Known Bijections with Low Differential Uniformity in Even Dimensions

Up to now, only a few classes of bijections with very low differential uniformity in even dimensions have been found, some of them are listed in [4,14]. We summarize them here for the convenience of the reader. It is clear that the functions

x^d and $x^{2^i d}$ are affine equivalent for every i, so we only list one value of d for each cyclotomic coset of 2 mod 2^n-1. Besides, we also omit d^{-1} when d is co-prime with 2^n-1 since arbitrary bijection is CCZ-equivalent to its compositional inverse.

- There is only one example of APN bijection on 6 variables, which is found by J. Dillon in [3], and the problem whether there exist APN bijections over $\mathbb{F}_{2^n}$ for even $n \geq 8$ is still open. This example is CCZ-equivalent to a quadratic function (which may represent a risk with respect to the higher order differential attack) and its expression is complex (this leads to inefficient implementation in both hardware and software).
- The inverse function x^{2^n-2} is differentially 4-uniform when n is even (and is APN when n is odd) [11]; it is used as the S-box of the AES with $n = 8$. It has best known nonlinearity $2^{n-1} - 2^{n/2}$ and maximum algebraic degree $n-1$. But the inverse function satisfies the bilinear relation $x^2 y = x$ where $y = x^{2^n-2}$, which is the core of the algebraic attacks and so may represent a thread.
- The Gold functions x^{2^i+1} such that $\gcd(i,n) = 2$ are differentially 4-uniform. Functions in this class are bijective when $\gcd(2^i+1, 2^n-1) = 1$, but they are quadratic and can not be used as S-boxes.
- The Kasami functions $x^{2^{2i}-2^i+1}$ such that n is divisible by 2 but not by 4 and $\gcd(i,n) = 2$ are differentially 4-uniform. Functions in this class have best known nonlinearity $2^{n-1} - 2^{n/2}$ (in fact, they have same Walsh spectrum as the Gold functions and we do not know whether this can represent a weakness) and are bijective when $\gcd(2^{2i} - 2^i + 1, 2^n - 1) = 1$. This class of functions never reaches the maximum algebraic degree $n-1$. Note that $2^{2i} - 2^i + 1 = \frac{2^{3i}+1}{2^i+1}$ and $2^i + 1$ is co-prime with $2^n - 1$ when n is divisible by 2 but not by 4 and $\gcd(i,n) = 2$. This means that the Kasami functions have the form $F(x) = Q_1(Q_2^{-1}(x))$ where Q_1 and Q_2 are quadratic permutations, which has some similarity with a function CCZ-equivalent to a quadratic function. Maybe this could be used in an extended higher order differential attack.
- The function $x^{2^{n/2+n/4+1}}$ is differentially 4-uniform [2] and has best known nonlinearity $2^{n-1} - 2^{n/2}$ as well. This class of functions is bijective if n is divisible by 4 but not by 8. It has algebraic degree 3 which is too low.
- In [8], the authors modified the method introduced in [4], initially designed for constructing differentially 4-uniform bijections in odd dimensions, to construct differentially 4-uniform bijections in even dimensions.They obtained three classes of differentially 4-uniform bijections with best known nonlinearity $2^{n-1} - 2^{n/2}$ and algebraic degree $(n+2)/2$. Those functions are interesting but the authors did not discuss whether they are CCZ-equivalent to power functions and quadratic functions.
- Recently, a construction has been introduced in [14] to build differentially 4-uniform bijections in even dimensions by adding some special Boolean functions to the inverse function. Based on it, the authors have discovered two infinite classes of differentially 4-uniform bijections. The first class of functions is of the form $x^{2^n-2} + tr_1^n(x^2(x+1)^{2^n-2})$, which has optimal algebraic

degree $n-1$ and the nonlinearity is no less than $2^{n-1}-2^{n/2+1}-2$. The second one is of the form $x^{2^n-2}+tr_1^n\big(x^{(2^n-2)d}+(x^{2^n-2}+1)^d\big)$, where $d=3(2^t+1)$, $2\le t\le n/2-1$. The latter has algebraic degree $n-1$ as well and the nonlinearity is at least $2^{n-2}-2^{n/2-1}-1$. The authors didn't mathematically prove whether their functions are CCZ-inequivalent to the inverse function (but we can easily check, with the help of computer, that those two classes of functions are CCZ-inequivalent to the inverse function for even $n=6,8,10,12$). These two classes of functions are interesting and they are worthy of a further investigation.

We can see from above that except for the inverse function (which has however a potential weakness), the Kasami functions (whose algebraic degree is enough to resist the higher order differential attack but which is not maximum, whose Walsh spectrum is the same as that of the Gold function and which seems related with quadratic functions - in a way which could not be used yet to design attacks, though), the functions proposed in [8] (which have not been proven CCZ-inequivalent to power functions) and the functions constructed in [14] (which have not been proven CCZ-inequivalent to the inverse function), there is no known bijection with low differential uniformity, which can be used as S-box. Hence, finding more bijections with all the desired features is very interesting from theoretical and practical viewpoints.

3 A Family of Differentially 4-Uniform Bijections

For any finite field $\mathbb{F}_{2^n}$ we define $0^{-1}=0$ by convention (we shall always use this convention in the sequel). Any finite field $\mathbb{F}_{2^n}$ can be viewed as an n-dimensional vector space over $\mathbb{F}_2$; each of its elements can be identified with a binary vector of length n, the element $0\in\mathbb{F}_{2^n}$ is identified with the all-zero vector. From now on, any given element $x=(x_1,\cdots,x_{n-1},x_n)\in\mathbb{F}_2^n$ can be identified with $(x',x_n)\in\mathbb{F}_{2^{n-1}}\times\mathbb{F}_2$, where $x'\in\mathbb{F}_{2^{n-1}}$ is identified with the vector $(x_1,\cdots,x_{n-1})\in\mathbb{F}_2^{n-1}$.

Construction 1. *Let $n\ge 6$ be an even number. For any element $c\in\mathbb{F}_{2^{n-1}}\setminus\{0,1\}$ such that $tr_1^{n-1}(c)=tr_1^{n-1}(1/c)=1$, we define an (n,n)-function F as follows:*

$$F(x_1,\cdots,x_{n-1},x_n)=\begin{cases}(1/x',f(x')), & \text{if } x_n=0\\ (c/x',f(x'/c)+1), & \text{if } x_n=1\end{cases}.$$

where $x'\in\mathbb{F}_{2^{n-1}}$ is identified with $(x_1,\cdots,x_{n-1})\in\mathbb{F}_2^{n-1}$ and f is an arbitrary Boolean function defined on $\mathbb{F}_{2^{n-1}}$.

3.1 Bijectivity

Theorem 1. *The function F defined in Construction 1 is bijective.*

Proof. We first prove that F is an injection. For any two elements $x, y \in \mathbb{F}_2^n$, if $x_n = y_n$ and $x \neq y$, then we can easily see that $F(x) \neq F(y)$ since $1/x', c/y'$ are two bijections on $\mathbb{F}_{2^{n-1}}$. If $x_n = y_n + 1$, then without loss of generality, we assume that $x_n = 0$ and $y_n = 1$. We can see that $F(x) = F(y)$ leads to $1/x' = c/y'$ which is equivalent to $y' = cx'$. Note that the last bit of $F(x)$ is $f(x')$ and the last bit of $F(y)$ equals $f(y'/c) + 1 = f(cx'/c) + 1 = f(x') + 1$, which does not equal $f(x')$. So F is an injection. Therefore, F is bijective. □

3.2 Differential 4-Uniformity

In this subsection, we will prove that F is differentially 4-uniform. For doing this, we first need a few preliminary results. The following lemma is well known.

Lemma 1. [9]. *Let n be a positive integer. For any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ let us define the polynomial $\mu(x) = ax^2 + bx + c \in \mathbb{F}_{2^n}[x]$, then the equation $\mu(x) = 0$ has 2 solutions if and only if $tr_1^n(b^{-2}ac) = 0$.*

The proof of the differential 4-uniformity of our functions will be based on the following lemma.

Lemma 2. *Let n be an even integer and $c \in \mathbb{F}_{2^{n-1}} \setminus \{0, 1\}$ such that $tr_1^{n-1}(c) = tr_1^{n-1}(1/c) = 1$, let us consider the following four equations defined on $\mathbb{F}_{2^{n-1}}$:*

$$1/x' + 1/(x' + a') = b' \tag{1}$$

$$c/x' + c/(x' + a') = b' \tag{2}$$

where $(a', b') \in \mathbb{F}_{2^{n-1}}^* \times \mathbb{F}_{2^{n-1}}$, and

$$1/x' + c/(x' + a') = b' \tag{3}$$

$$c/x' + 1/(x' + a') = b' \tag{4}$$

where $(a', b') \in \mathbb{F}_{2^{n-1}} \times \mathbb{F}_{2^{n-1}}$. Then the following statements hold:

(1) For $a'b' \neq 1$, (1) has two solutions on $\mathbb{F}_{2^{n-1}}$ if $b' \neq 0$ and $tr_1^{n-1}(1/(a'b')) = 0$ and has no solution otherwise. For $a'b' = 1$, (1) has two distinct solutions $0, a'$.

(2) For $a'b' \neq c$, (2) has two solutions on $\mathbb{F}_{2^{n-1}}$ if $b' \neq 0$ and $tr_1^{n-1}(c/(a'b')) = 0$ and has no solution otherwise. For $a'b' = c$, (2) has two distinct solutions $0, a'$.

(3) For any $x_0' \in \mathbb{F}_{2^{n-1}}$, x_0' is a solution of (3) if and only if $x_0' + a'$ is a solution of (4). Furthermore:
   - *for $a'b' \neq 0, 1, c$, both of (3) and (4) have two solutions if $tr_1^{n-1}(a'b'/(a'b' + c + 1)) = 0$ and have no solution otherwise;*
   - *for $a'b' = 1$, (3) has unique solution a' and (4) has unique solution 0;*
   - *for $a'b' = c$, (3) has unique solution 0 and (4) has unique solution a';*
   - *for $a'b' = 0$, both (3) and (4) have unique solution.*

Proof. Our proof mainly relies on Lemma 1.

(1) If $a'b' \neq 1$, which is equivalent to saying that both 0 and a' are not solutions of (1), then (1) is equivalent to $b'x'^2 + a'b'x' + a' = 0$. By Lemma 1, this new equation has two solutions if $b' \neq 0$ and $tr_1^{n-1}(1/(a'b')) = 0$. Note that (1) has no solution if $b' = 0$ since $a' \neq 0$. Therefore, for $a'b' \neq 1$, (1) has two solutions if $b' \neq 0$ and $tr_1^{n-1}(1/(a'b')) = 0$ and has no solution otherwise. If $a'b' = 1$ then $tr_1^{n-1}(1/(a'b')) = tr_1^{n-1}(1) = 1$ and therefore $b'x'^2 + a'b'x' + a' = 0$ has no solution. This implies that (1) has only two solutions $0, a'$ when $a'b' = 1$.

(2) If $a'b' \neq c$, which is equivalent to saying that both 0 and a' are not solutions of (2), then (2) is equivalent to $b'x'^2+a'b'x'+ca' = 0$, which, by Lemma 1, has two solutions if $b' \neq 0$ and $tr_1^{n-1}(c/(a'b')) = 0$ and has no solution otherwise since (2) has no solution for $b' = 0$. If $a'b' = c$ then $tr_1^{n-1}(c/(a'b')) = tr_1^{n-1}(1) = 1$, which implies that $b'x'^2 + a'b'x' + ca' = 0$ has no solution. Thus, (2) has only two solutions $0, a'$ for $a'b' = c$.

(3) We can directly check that, for any $x_0' \in \mathbb{F}_{2^{n-1}}$, if x_0' is a solution of (3) then $x_0' + a'$ is a solution of (4) and the converse is true.

If $a'b' \neq 1, c$ in (3), which is equivalent to saying that both 0 and a' are not solutions of (3), then (3) is equivalent to $b'x'^2 + (a'b' + c + 1)x' + a' = 0$. Note that $a'b' \neq 0$ gives $b' \neq 0$. Hence, for $a'b' \neq 0, 1, c$, $b'x'^2 + (a'b' + c + 1)x' + a' = 0$ has two solutions if $tr_1^{n-1}(a'b'/(a'b' + c + 1)^2) = 0$ and has no solution if $tr_1^{n-1}(a'b'/(a'b' + c + 1)^2) = 1$ by Lemma 1. Note that $a'b' = 1$ implies that $tr_1^{n-1}(a'b'/(a'b'+c+1)^2) = tr_1^{n-1}(1/c) = 1$ and $a'b' = c$ leads to $tr_1^{n-1}(a'b'/(a'b'+c+1)^2) = tr_1^{n-1}(c) = 1$. Hence, (3) has unique solution a' if $a'b' = 1$ and has unique solution 0 if $a'b' = c$. If $a'b' = 0$, we can easily check that (3) has unique solution for $b' \neq a' = 0$, $a' \neq b' = 0$ and $a' = b' = 0$, respectively. Then the statement for (4) is direct.

□

Now we are ready to prove our main theorem.

Theorem 2. *For any even $n \geq 6$, the bijection F defined in Construction 1 is differentially 4-uniform.*

Proof. Let us check that

$$F(x) + F(x + a) = b \tag{5}$$

has at most 4 solutions for every fixed $(a, b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^n$. Let us write $x = (x', x_n)$, $a = (a', a_n)$ and $b = (b', b_n)$. Then Eq. (5) is equivalent to

$$F(x', x_n) + F(x' + a', x_n + a_n) = (b', b_n), \tag{6}$$

s If $a_n = 0$ and $a' \neq 0$ then the solutions of Eq. (6) are constituted by $(x', 0)$ such that

$$1/x' + 1/(x' + a') = b', f(x') + f(x' + a') = b_n \tag{7}$$

and by $(x', 1)$ such that

$$c/x' + c/(x' + a') = b', f(x'/c) + f((x' + a')/c) = b_n. \tag{8}$$

If $a_n = 1$ then the solutions of Eq. (6) are constituted by $(x', 0)$ such that

$$1/x' + c/(x' + a') = b', f(x') + f((x' + a')/c) = b_n + 1 \tag{9}$$

and by $(x', 1)$ such that

$$c/x' + 1/(x' + a') = b', f(x'/c) + f((x' + a')) = b_n + 1. \tag{10}$$

For $a_n = 0$ and $a' \neq 0$, by (1) and (2) of Lemma 2, we can see that the sum of the numbers of solutions of Eqs. (7) and (8) is at most 4. Similarly, for $a_n = 1$, it follows from (3) of Lemma 2 that the sum of the numbers of solutions of Eqs. (9) and (10) is at most 4. This completes the proof. □

Remark 1. Given an integer n, let us define $T(n)$ as the number of $c \in \mathbb{F}_{2^n}$ such that $tr_1^n(c) = tr_1^n(1/c) = 1$. Then there are $T(n)-1$ elements $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $tr_1^n(c) = tr_1^n(1/c) = 1$ when n is odd, since $tr_1^n(0) = 0$ and $tr_1^n(1) = 1$. Let $K_n(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(1/x+ax)}$, where $a \in \mathbb{F}_{2^n}^*$, be the so-called Kloosterman sums on $\mathbb{F}_{2^n}$. Note that $K_n(1) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x+1/x)} = 2^n - 2\mathrm{wt}\big(tr_1^n(x) + tr_1^n(1/x)\big) = 2^n - 2\mathrm{wt}(tr_1^n(x)) - 2\mathrm{wt}(tr_1^n(1/x)) + 4T(n) = -2^n + 4T(n)$. We have $T(n) = 2^{n-2} + K_n(1)/4$, which is at least $2^{n-2} - \lfloor 2^{n/2-1} \rfloor$ according to Lemma 3 (see below). Hence, for any even $n \geq 6$, Construction 1 can generate $(T(n-1)-1) \cdot 2^{2^{n-1}} \geq (2^{n-3} - \lfloor 2^{(n-1)/2-1} \rfloor - 1) \cdot 2^{2^{n-1}}$ differentially 4-uniform bijections.

In fact, our method for constructing differentially 4-uniform bijections on n variables can be viewed as concatenating the value-tables of two almost bent bijections on $n-1$ variables and completing each value by concatenating it with the value of a Boolean function. Some work to find new infinite classes of APN or differentially 4-uniform functions (not bijective) has been done by concatenation method [5,6], but the concatenation was on two functions in n variables whose outputs have length $n/2$.

3.3 Algebraic Degree

We shall now show the algebraic degree of F.

Theorem 3. *For every even $n \geq 6$, F with any Boolean function $f \in \mathcal{B}_{n-1}$ has algebraic degree $n-1$.*

Proof. It is obvious that F has algebraic degree at most $n-1$ since F is bijective. So we only need to prove that F has algebraic degree at least $n-1$. Let $a_0 \in \mathbb{F}_{2^n}$ be an element which is identified with $(a', 0)$ such that $a' \neq 0$. Then the component function $a_0 \cdot F$ is identified with $tr_1^{n-1}(a'F(x', x_n))$. This implies that $a_0 \cdot F(x', x_n) = (1 + x_n)tr_1^{n-1}(a'/x') + x_n tr_1^{n-1}(a'c/x') = x_n tr_1^{n-1}((a' + a'c)/x') + tr_1^{n-1}(a'/x')$. Note that $a' + a'c \neq 0$ since $a' \neq 0$ and $c \neq 1$. So we have the component function $a_0 \cdot F$ has algebraic degree $n-1$ thanks to $tr_1^{n-1}((a' + a'c)/x')$ has degree $n-2$. Therefore, F has algebraic degree $n-1$. □

3.4 Walsh Transform

Theorem 4. *Let $n \geq 6$ be an integer and $f \in \mathcal{B}_{n-1}$ be the function defined in Construction 1. For any $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^n$, we have*

$$W_F(a,b) = \begin{cases} \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'/x'+b'x')} + \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'c/x'+b'x')}, & \text{if } a_n = 0, b_n = 0 \\ \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'/x'+b'x')} - \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'c/x'+b'x')}, & \text{if } a_n = 0, b_n = 1 \\ \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'/x'+b'x')+f(x')} - \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'c/x'+b'x')+f(x'/c)}, & \\ & \text{if } a_n = 1, b_n = 0 \\ \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'/x'+b'x')+f(x')} + \sum\limits_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'c/x'+b'x')+f(x'/c)}, & \\ & \text{if } a_n = 1, b_n = 1 \end{cases}$$

where a is identified with (a', a_n) and b is identified with (b', b_n), where $a', b' \in \mathbb{F}_{2^{n-1}}$.

Proof. Note that the linear function $(b_1, \cdots, b_{n-1}, b_n) \cdot (x_1, \cdots, x_{n-1}, x_n)$ can be identified with $tr_1^{n-1}(b'x') + b_n x_n$ and the component function $a \cdot F$, denoted by $g_a(x_1, \cdots, x_{n-1}, x_n)$, can be identified with $g_a(x', x_n)$, where $g_a(x', x_n)$ is defined as $g_a(x', x_n) = tr_1^{n-1}(a'/x') + a_n f(x')$ if $x_n = 0$ and $g_a(x', x_n) = tr_1^{n-1}(a'c/x') + a_n(f(x'/c) + 1)$ if $x_n = 1$. Therefore, we have

$$\begin{aligned} W_F(a,b) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot F + bx} \\ &= \sum_{(x', x_n) \in \mathbb{F}_{2^{n-1}} \times \{0\}} (-1)^{tr_1^{n-1}(a'/x') + a_n f(x') + tr_1^{n-1}(b'x') + b_n x_n} \\ &\quad + \sum_{(x', x_n) \in \mathbb{F}_{2^{n-1}} \times \{1\}} (-1)^{tr_1^{n-1}(a'c/x') + a_n(f(x'/c)+1) + tr_1^{n-1}(b'x') + b_n x_n} \\ &= \sum_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'/x'+b'x') + a_n f(x')} \\ &\quad + \sum_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(a'c/x'+b'x') + a_n f(x'/c) + b_n + a_n}. \end{aligned}$$

Then our assertion follows from above equality. □

Remark 2. By Theorem 4, we can see that the nonlinearity of F can take value 0 if the Boolean function f used in Construction 1 is an affine function.

3.5 CCZ-inequivalence

In this subsection, we will prove that, for any even $n \geq 8$, F is CCZ-inequivalent to the Gold functions, the Kasami functions, the functions discussed in [2] and to quadratic functions. With the help of computer, we checked that for even n ranging from 8 to 16, F is CCZ-inequivalent to the inverse function.

Here and subsequently, I denotes the inverse function. We need the nonlinearities of component functions of I.

Lemma 3 [13]**.** *For any positive integer n and arbitrary $a \in \mathbb{F}_{2^n}^*$, the Walsh spectrum of $tr_1^n(ax^{-1})$ defined on $\mathbb{F}_{2^n}$ can take any value divisible by 4 in the range $[-2^{n/2+1}+1, 2^{n/2+1}+1]$.*

We now study the CCZ-inequivalence of F.

Theorem 5. *For every even $n \geq 8$, F is CCZ-inequivalent to the Gold functions, the Kasami functions, the functions discussed in [2] and quadratic functions.*

Proof. Note that the extended Walsh spectrum is a CCZ-invariant parameter. It is well known that, for even n, the elements of the extended Walsh spectra of the Gold functions, the Kasami functions and the functions discussed in [2] belong to the set $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$ and that the elements of the extended Walsh spectrum of quadratic functions can be divisible by $2^{n/2}$ (indeed, the component functions of any quadratic function have algebraic degree at most 2. We know that the nonlinearity of any affine function is equal to 0 and the Walsh spectrum of any quadratic Boolean function is $\pm 2^{n/2}$ or $0, \pm 2^{n/2+l}$, where $l \geq 1$). Hence, for proving F is CCZ-inequivalent to those functions, we only need to prove that F has different extended Walsh spectrum compared to theirs. Let us take $a' = 1$ in Theorem 4. Then there must be an element $b_0' \in \mathbb{F}_{2^{n-1}}$ such that $\sum_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(1/x' + b_0' x')} = 4$, according to Lemma 3. Define $\lambda = \sum_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{tr_1^{n-1}(c/x' + b_0' x')}$. It follows from Theorem 4 that $4 + \gamma$ and $4 - \gamma$ belong to the extended Walsh spectra of F. We can see that, for even $n \geq 8$, $4 + \gamma$ and $4 - \gamma$ can not be divisible by $2^{n/2}$ simultaneously. This is the desired conclusion. □

Theorem 6. *Let $n \geq 8$ be an even integer. Define $f_3 \in \mathcal{B}_n$ on variables $x_1, \cdots, x_n$ as $f_3 = (1+x_n)f_1 + x_n f_2$, where $f_1, f_2 \in \mathcal{B}_{n-1}$ are defined as $f_1 = tr_1^{n-1}(1/x)$ and $f_2 = tr_1^{n-1}(c/x)$ where $c \in \mathbb{F}_{2^{n-1}} \setminus \{0, 1\}$ is such that $tr_1^{n-1}(c) = tr_1^{n-1}(1/c) = 1$. If $nl(f_3) < 2^{n-1} - 2^{n/2}$, then F with any $f \in \mathcal{B}_{n-1}$ is CCZ-inequivalent to the inverse function and therefore F is CCZ-inequivalent to all known differentially 4-uniform power functions and to quadratic functions.*

Proof. Let us take $a' = 1 \in \mathbb{F}_{2^{n-1}}$ and $a_n = 0$ in the function $g_a(x_1, \cdots, x_{n-1}, x_n)$ which is defined in the proof of Theorem 4. Then we can see that $g_a(x_1, \cdots, x_{n-1}, x_n)$ is equal to f_3 and so f_3 is a component function of F. If $nl(f_3) < 2^{n-1} - 2^{n/2}$, then we have $nl(F) < 2^{n-1} - 2^{n/2}$ and therefore F is CCZ-inequivalent to the inverse function since the nonlinearity is a CCZ-invariant parameter and $nl(I) = 2^{n-1} - 2^{n/2}$. The rest of proof follows from Theorem 5. □

Remark 3. By computer investigation, we checked that $nl(f_3) < 2^{n-1} - 2^{n/2}$ (but the nonlinearity of f_3 is very close to $2^{n-1} - 2^{n/2}$ and we will show below a class of highly nonlinear bijections by choosing a special Boolean function f in Construction 1) for even n ranging from 8 to 16, where f_3 is defined in Theorem 6. This implies that F is CCZ-inequivalent to all known differentially 4-uniform power functions and to quadratic functions when $8 \le n \le 16$.

4 A Class of Differentially 4-Uniform Bijections with Good Cryptographic Properties

Hereinafter, for any even integer $n \ge 6$, we define F_1 as the function F with $f(x') = tr_1^{n-1}(1/(x'+1))$. By Theorems 1 and 2, we can see that F_1 is a differentially 4-uniform bijection. It follows from Theorem 3 that F_1 has maximum algebraic degree $n-1$. In what follows, we will prove that the function F_1 has high nonlinearity and is CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions.

We first give a lower bound on the nonlinearity of F_1. For doing this, we need the following lemma.

Lemma 4 [14]. *Let n be a positive integer such that $n \ge 4$, then we have $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax+bx^{-1}+x^2(x+1)^{-1})}| \le 2\lfloor 2^{n/2+1}\rfloor + 4$ for any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.*

Note that $x^2(x+1)^{-1} = x + 1 + (x+1)^{-1}$. Then Lemma 4 is equivalent to:

Corollary 1. *For any $n \ge 4$, we have $|\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax+bx^{-1}+(x+1)^{-1})}| \le 2\lfloor 2^{n/2+1}\rfloor + 4$ for any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.*

We are now ready to give a lower bound on the nonlinearity of F_1.

Theorem 7. *For any even $n \ge 6$, we have $nl(F_1) \ge 2^{n-1} - 2\lfloor 2^{(n+1)/2}\rfloor - 4$.*

Proof. For any $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^n$, we identify a with (a', a_n) and b with (b', b_n). By Lemma 4, we have

$$W_F(a,b) = \begin{cases} \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}(a'/x'+b'x')} + \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}(a'c/x'+b'x')}, & \text{if } a_n = 0, b_n = 0 \\ \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}(a'/x'+b'x')} - \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}(a'c/x'+b'x')}, & \text{if } a_n = 0, b_n = 1 \\ \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}\left(a'/x'+1/(x'+1)+b'x'\right)} & \\ \quad - \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}\left(a'/x'+1/(x'+1)+b'cx'\right)}, & \text{if } a_n = 1, b_n = 0 \\ \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}\left(a'c/x'+1/(x'+1)+b'x'\right)} & \\ \quad + \sum\limits_{x'\in\mathbb{F}_{2^{n-1}}}(-1)^{tr_1^{n-1}\left(a'/x'+1/(x'+1)+b'cx'\right)}, & \text{if } a_n = 1, b_n = 1 \end{cases}.$$

Table 1. The exact values of $nl(F_1)$ on small number of variables

n	6	8	10	12
$2^{n-1}-2^{n/2}$	24	112	480	1984
$nl(F_1)$	20	94	436,438,440,442	1888,1892,1894,1896,1898,1900,1902
Our lower bound	6	80	418	1864

By Lemma 3 and Corollary 1, we have

$$|W_F(a,b)| \leq \begin{cases} 2\lfloor 2^{(n+1)/2} \rfloor, & \text{if } a_n = 0, b_n \in \mathbb{F}_2 \\ 4\lfloor 2^{(n+1)/2} \rfloor + 8, & \text{if } a_n = 1, b_n \in \mathbb{F}_2 \end{cases}.$$

This implies that $nl(F_1) \geq 2^{n-1} - 2\lfloor 2^{(n+1)/2} \rfloor - 4$. □

With the help of computer, we get the exact values of $nl(F_1)$ for even numbers of variables ranging from 6 to 12, which are given in the following table.

4.1 CCZ-inequivalence

We shall now show that F_1 is CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions.

To prove our main result, we need the following lemma.

Lemma 5. *Let $n \geq 7$ be an integer. For any $\gamma \in \mathbb{F}_{2^n}^*$ and $\beta_i, \alpha_i \in \mathbb{F}_{2^n}$ where $1 \leq i \leq 3$, we have*

$$|\sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n\left(\frac{\alpha_1}{x+\beta_1} + \frac{\alpha_2}{x+\beta_2} + \frac{\alpha_3}{x+\beta_3} + \gamma x\right)}| \leq 3\lfloor 2^{\frac{n}{2}+1} \rfloor + 6.$$

Proof. Define $S = \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \,|\, y^2 + y = \frac{\alpha_1}{x+\beta_1} + \frac{\alpha_2}{x+\beta_2} + \frac{\alpha_3}{x+\beta_3} + \gamma x\}$. Then we have

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(\frac{\alpha_1}{x+\beta_1} + \frac{\alpha_2}{x+\beta_2} + \frac{\alpha_3}{x+\beta_3} + \gamma x)} = |S| - 2^n, \tag{11}$$

since $tr_1^n(z) = 0$ if and only if there exists an element $y \in \mathbb{F}_{2^n}$ such that $z = y^2 + y$, and $y \mapsto y^2 + y$ is a 2-to-1 mapping. Let us consider the function field $K = \mathbb{F}_{2^n}(x,y)$ with defining equation

$$y^2 + y = \frac{\alpha_1}{x+\beta_1} + \frac{\alpha_2}{x+\beta_2} + \frac{\alpha_3}{x+\beta_3} + \gamma x. \tag{12}$$

Then we can deduce that the genus g of K is equal to

$$g = \begin{cases} 1, & \text{if } \beta_1 = \beta_2 = \beta_3 \\ 2, & \text{if } \beta_1 = \beta_2 \neq \beta_3 \text{ or } \beta_1 \neq \beta_2 = \beta_3 \text{ or } \beta_1 = \beta_3 \neq \beta_2 \\ 3, & \text{if } \beta_1 \neq \beta_2 \neq \beta_3 \neq \beta_1 \end{cases}. \tag{13}$$

Denote by N the number of the places with degree one of K/F_{2^n}. Then by Serre bound, we have

$$|N-(2^n+1)| \leq g\lfloor 2^{n/2+1}\rfloor. \tag{14}$$

In what follows, we compute the points at infinity of (12). We first consider the case that $\alpha_1, \alpha_2, \alpha_3$ are pairwise distinct. The homogeneous equation of Equation (12) is equal to

$$(\frac{Y}{Z})^2+\frac{Y}{Z}=\frac{\alpha_1 Z}{X+\beta_1 Z}+\frac{\alpha_2 Z}{X+\beta_2 Z}+\frac{\alpha_3 Z}{X+\beta_3 Z}+\gamma\frac{X}{Z}. \tag{15}$$

If we multiply both sides of Eq. (15) by Z^2, we get

$$Y^2+YZ=[\frac{\alpha_1 Z}{X+\beta_1 Z}+\frac{\alpha_2 Z}{X+\beta_2 Z}+\frac{\alpha_3 Z}{X+\beta_3 Z}]Z^2+\gamma XZ. \tag{16}$$

Multiply both sides of Eq. (16) by $(X+\beta_1 Z)(X+\beta_2 Z)(X+\beta_3 Z)$ and then let $Z=0$, we have $X^3Y^2=0$. Hence, there are two points at infinity satisfying the Eq. (15), which are $(0:1:0)$ and $(1:0:0)$. We now compute the multiplicity of roots of $(0:1:0)$ and $(1:0:0)$, respectively. Let us first consider $(0:1:0)$, i.e., $Y=1$. We can use

$$(\frac{1}{z})^2+\frac{1}{z}=\frac{\alpha_1 z}{x+\beta_1 z}+\frac{\alpha_2 z}{x+\beta_2 z}+\frac{\alpha_3 z}{x+\beta_3 z}+\gamma\frac{x}{z} \tag{17}$$

to calculate the multiplicity of root. It should be note that $(0:1:0)$ is corresponding to $(0,0)$. Multiply Eq. (17) by z^2, we get

$$1+[\frac{\alpha_1}{x+\beta_1 z}+\frac{\alpha_2}{x+\beta_2 z}+\frac{\alpha_3}{x+\beta_3 z}]z^3=z+\gamma xz.$$

Multiply this new equation by $(x+\beta_1 z)(x+\beta_2 z)(x+\beta_3 z)$, we have

$$(x+\beta_1 z)(x+\beta_2 z)(x+\beta_3 z)+R(x,z)=0,$$

where $R(x,z)$ is a polynomial such that its every monomial has algebraic degree at least 3. This gives $(0:1:0)$ is a root of multiplicity 3. For the point $(1:0:0)$, i.e. $X=1$, we can use

$$(\frac{y}{z})^2+\frac{y}{z}=\frac{\alpha_1 z}{1+\beta_1 z}+\frac{\alpha_2 z}{1+\beta_2 z}+\frac{\alpha_3 z}{1+\beta_3 z}+\gamma\frac{1}{z} \tag{18}$$

to calculate the multiplicity of root. Similar with Eq. (17), Eq. (18) can be deduced as

$$\gamma z+(Y^2+yz)+[\frac{\alpha_1}{1+\beta_1 z}+\frac{\alpha_2}{1+\beta_2 z}+\frac{\alpha_3}{1+\beta_3 z}]z^3=0.$$

Multiply this new equation by $(1+\beta_1 z)(1+\beta_2 z)(1+\beta_3 z)$. Two cases can then occur, according to the values of γ.

- For$\gamma \neq 0$, we have $\gamma z + R_1(y,z) = 0$, where $R_1(y,z)$ is such that its every monomial has algebraic degree at least 1. This implies that $(1:0:0)$ is a root of multiplicity 1.
- For $\gamma = 0$, we can deduce that $(y^2 + yz) + R_2(y,z) = 0$ where $R_2(y,z)$ is such that its every monomial has algebraic degree at least 2, which implies $(1:0:0)$ is a root of multiplicity 2.

Therefore, Eq. (12) has at most five points at infinity in the case that $\alpha_1, \alpha_2, \alpha_3$ are pairwise distinct. Then

$$N \geq S - 5. \tag{19}$$

Similarly, we can deduce that Eq. (12) has at most four points at infinity if $\alpha_1, \alpha_2, \alpha_3$ are not pairwise distinct. So we have

$$N \geq S - 4. \tag{20}$$

Equations (11), (14), (19) and (20) combined give our statement. □

We are ready now to state and prove the main result of this subsection.

Theorem 8. *For any even $n \geq 8$, F_1 is CCZ-inequivalent to all known differentially 4-uniform power functions and to quadratic functions.*

Proof. By Theorem 5, we can see that F_1 is CCZ-inequivalent to the Gold functions, the Kasami functions, the functions discussed in [2] and to quadratic functions. So, for proving our statement, we only need to prove that F_1 is CCZ-inequivalent to the inverse function. It is well-known that the number of pairs $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^n$ such that $I(x) + I(x+a) = b$ has 4 solutions is $2^n - 1$. Recall that the differential spectrum is a CCZ-invariant parameter. So we only need to prove that the number of pairs $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^n$ such that $F_1(x) + F_1(x+a) = b$ has 4 solutions is at least 2^n.

We identify a with (a', a_n) and b with (b', b_n). Let us first give a sufficient condition for the sum of the numbers of distinct solutions (9) and (10) to equal 4. For every $a' \in \mathbb{F}_{2^{n-1}}^*$ and for every fixed $x_0 \in \mathbb{F}_{2^{n-1}} \setminus \{0, a', a'/(c+1)\}$, if we assume that x_0 is a solution of $1/x' + c/(x'+a') = b'$ which is equivalent to

$$b'{x'}^2 + (a'b' + c + 1)x' + a' = 0 \tag{21}$$

thanks to $x_0 \neq 0, a$, then we have $b'{x_0}^2 + (a'b' + c + 1)x_0 + a' = 0$ and hence $b' = (a' + (c+1)x_0)/({x_0}^2 + a'x_0)$ which is nonzero since $x_0 \neq a'/(c+1), 0, a'$. Further, we can deduce that the other solution of (21) is $x_1 = x_0 + a' + (c+1)/b' = c{a'}^2/\big((c+1)(cx_0 + x_0 + a')\big) + a'/(c+1)$. For ensuring $x_0 \neq x_1$, $a' + (c+1)/b'$ should not be equal to 0, which is equivalent to saying that x_0 should not be a solution of equation $(a' + (c+1)x')/({x'}^2 + a'x') = (c+1)/a'$. This implies that $x_0 \neq a'(c+1)^{2^{n-2}}$. Hence, for every $a' \in \mathbb{F}_{2^{n-1}}^*$, then for every fixed $x_0 \in \mathbb{F}_{2^{n-1}} \setminus \{0, a', a'(c+1)^{2^{n-2}}, a'/(c+1)\}$, equation $1/x' + c/(x'+a') = b'$ with $b' = (a' + (c+1)x_0)/({x_0}^2 + a'x_0)$ has two distinct solutions x_0, x_1. Further, by (3) of Lemma 2, x_0+a', x_1+a' are two distinct solutions of $c/x'+1/(x'+a')=b'$. We can see that $x_1+a' \neq x_0$ since $(c+1)/b' \neq 0$. This gives that x_0, x_1, x_0+a', x_1+a' are four distinct elements. Therefore, for every $a' \in \mathbb{F}_{2^{n-1}}^*$ and for every fixed $x_0 \in \mathbb{F}_{2^{n-1}} \setminus \{0, a', a'(c+1)^{2^{n-2}}, a'/(c+1)\}$, (9) and (10) have four pairwise distinct solutions if $f(x') + f((x'+a')/c) = f(x'/c) + f((x'+a'))$, in which $b' = (a'+(c+1)x_0)/(x_0{}^2+a'x_0)$ and $b_n = f(x')+f((x'+a')/c)$, and therefore (6) has four distinct solutions. For every $a' \in \mathbb{F}_{2^{n-1}}^*$, let us define $T_{a'} = \{x \in \mathbb{F}_{2^{n-1}} \setminus \{0, a', a'(c+1)^{2^{n-2}}, a'/(c+1)\} | f(x')+f((x'+a')/c)+f(x'/c)+f((x'+a'))=0\}$. Note that (21) has at most two solutions when a', b' are fixed. Thus, for every $a' \in \mathbb{F}_{2^{n-1}}^*$, there are at least $T_{a'}/2$ distinct pairs $(a,b) = \big((a',1),(b',b_n)\big)$ such that (6) has four distinct solutions.

We now show that the number of pairs $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^n$ such that $F_1(x) + F_1(x+a) = b$ has 4 solutions is not less than 2^n. We replace $f(x')$ in $T_{a'}$ by $tr_1^{n-1}(1/(x'+1))$, then $T_{a'}$ becomes $T_{a'} = \{x_0 \in \mathbb{F}_{2^{n-1}} \setminus \{0, a', a'(c+1)^{2^{n-2}}, a'/(c+1)\} | tr_1^n\big(1/(x_0+1)+1/((x_0+a')/c+1)+1/(x_1+1)+1/((x_1+a')/c+1)\big)=0\}$. Recall that $x_1 = x_0+a'+(c+1)/b' = ca'^2/\big((c+1)(cx_0+x_0+a')\big)+a'/(c+1)$. Then for every $a' \in \mathbb{F}_{2^n} \setminus \{0, 1+c, (c+1)^{2^{n-2}}\}$, we have

$$T_{a'} = \Big\{x_0 \in \mathbb{F}_{2n-1} \setminus \{0, a', a'(c+1)^{2^{n-2}}, a'/(c+1)\} | tr_1^{n-1}\Big(\frac{\frac{c}{(a'+c+1)^2}}{x_0+\frac{1}{a'+c+1}} + \frac{\frac{ca'^2}{(a'^2+c+1)^2}}{x_0+\frac{a'+c+1}{a'^2+c+1}} + \frac{\frac{a'^2}{(c+1)^2}}{x_0+\frac{a'+c+1}{c+1}} + x_0 + \frac{c}{a'+c+1} + \frac{ca'^2}{(a'+c+1)(a'^2+c+1)} + \frac{a'^2}{(a'+c+1)(c+1)}\Big) = 0\Big\}.$$

Therefore, the number of pairs $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^n$ such that $F_1(x)+F_1(x+a)=b$ has 4 solutions is greater than $(2^{n-1}-3)T_{a'}/2$, which is not less than 2^n-1 since $T_{a'} \geq 2^{n-2} - \frac{3}{2}\lfloor 2^{\frac{n-1}{2}+1} \rfloor - 7$ for every $a' \in \mathbb{F}_{2^n} \setminus \{0, 1+c, (c+1)^{2^{n-2}}\}$ according to Lemma 5. This completes the proof. □

Remark 4. By computer investigation, we checked that the extended Walsh spectrum of F_1 for even numbers of variables ranging from 6 to 12 are different from those of all the known differentially 4-uniform bijections listed in Sect. 2. This implies that functions F_1 are CCZ-inequivalent to all known differentially 4-uniform bijections in the dimensions ranging over even integers from 6 to 12.

5 Conclusion

In this paper, we first presented a construction of differentially 4-uniform bijections on $\mathbb{F}_{2^n}$, where $n \geq 6$ is even. For any even $n \geq 6$, this construction can generate at least $\big(2^{n-3} - \lfloor 2^{(n-1)/2-1} \rfloor - 1\big) \cdot 2^{2^{n-1}}$ bijections having algebraic degree $n-1$. In addition, we exhibited a subclass of these bijections which have high nonlinearity and are CCZ-inequivalent to all known differentially 4-uniform power bijections and to quadratic functions. The research of finding more subclasses with high nonlinearity from our construction is very interesting and is worthy of a further investigation.

Acknowledgement. The authors wish to thank Sihem Mesnager for helpful information. The work of D. Tang was supported by the program of China Scholarships Council (No. 201207000049). The work of X.H. Tang was supported by the Youngth Innovative Research Team of Sichuan Province under Grant 2011JTD0007. The work of Q.Y. Liao was supported by the National Science Foundation of China (No. A10990011), the Ph.D. Programs Foundation of Ministry of Education of China(No. 20095134120001) and Sichuan Provincial Advance Research Program for Excellent Youth Leaders of Disciplines in Science of China (No. 2011JQ0037).

References

1. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
2. Bracken, C., Leander, G.: A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields Appl. **16**(4), 231–242 (2010)
3. Browning, K.A., Dillon, J.F., McQuistan, M.T., Wolfe, A.J.: An APN permutation in dimension six. In: Postproceedings of the 9th International Conference on Finite Fields and their Applications Fq'9. Contemporary Mathematics Journal of American Mathematical Society, vol. 518, pp. 33–42 (2010)
4. Carlet, C.: On known and new differentially uniform functions. In: Parampalli, U., Hawkes, P. (eds.) ACISP 2011. LNCS, vol. 6812, pp. 1–15. Springer, Heidelberg (2011)
5. Carlet, C.: Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des. Codes Cryptogr. **59**(1–3), 89–109 (2011)
6. Carlet, C.: More constructions of APN and differentially 4-uniform functions by concatenation. Sci. China Math. **56**(7), 1373–1384 (2013)
7. Knudsen, L.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995)
8. Li, Y., Wang, M.: Constructing differentially 4-uniform permutations over $GF(2^{2m+1})$ from quadratic APN permutations over $GF(2^{2m})$. To appear in Des. Codes Cryptogr. (2012). doi:10.1007/s10623-012-9760-9
9. MacWilliams, F.J., Sloane, N.J.: The Theory of Error-Correcting Codes. North Holland, Amsterdam (1977)
10. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
11. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994)
12. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
13. Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inf. Theory **36**(3), 686–692 (1990)
14. Qu, L., Tan, Y., Tan, C., Li, C.: Constructing Differentially 4-Uniform Permutations over $\mathbb{F}_2^{2k}$ via the Switching Method. IEEE Trans. Inf. Theory **59**(7), 4675–4686 (2013)

Springer

http://www.springer.com/978-3-319-12086-7

Information Security and Cryptology
9th International Conference, Inscrypt 2013, Guangzhou,
China, November 27-30, 2013, Revised Selected Papers
Lin, D.; Xu, S.; Yung, M. (Eds.)
2014, XIII, 408 p. 51 illus., Softcover
ISBN: 978-3-319-12086-7