Differentially 4-Uniform Bijections by Permuting the Inverse Function

Deng Tang[1,2] Claude Carlet[2] Xiaohu Tang[1]

Abstract

Block ciphers use Substitution boxes (S-boxes) to create confusion into the cryptosystems. Functions used as S-boxes should have low differential uniformity, high nonlinearity and algebraic degree larger than 3 (preferably strictly larger). They should be fastly computable; from this viewpoint, it is better when they are in even number of variables. In addition, the functions should be bijections in a Substitution-Permutation Network. Almost perfect nonlinear (APN) functions have the lowest differential uniformity 2 and the existence of APN bijections over $\mathbb{F}_{2^n}$ for even $n \geq 8$ is a big open problem. In the present paper, we focus on constructing differentially 4-uniform bijections suitable for designing S-boxes for block ciphers. Based on the idea of permuting the inverse function, we design a construction providing a large number of differentially 4-uniform bijections with maximum algebraic degree and high nonlinearity. For every even $n \geq 12$, we mathematically prove that the functions in a subclass of the constructed class are CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions. This is the first mathematical proof that an infinite class of differentially 4-uniform bijections is CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions. We also get a general lower bound on the nonlinearity of our functions, which can be very high in some cases, and obtain three improved lower bounds on the nonlinearity for three special subcases of functions which are extremely large.

Keywords: block cipher, substitution box, differentially 4-uniform bijection, CCZ-equivalence, nonlinearity.

[1]Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, 610031, China.

[2]LAGA, Universities of Paris 8 and Paris 13; CNRS, UMR 7539. Address: University of Paris 8, Department of Mathematics, 2 rue de la liberté, 93526 Saint-Denis cedex 02, France.

Email: dtang@foxmail.com (D. Tang), claude.carlet@univ-paris8.fr (C. Carlet), xhutang@ieee.org (X. Tang)

1 Introduction

The generally accepted design principles for block ciphers and stream ciphers are confusion and diffusion; they were introduced by Shannon in [12]. Confusion means making the relation between the ciphertext and the plaintext as complex as possible for the attacker and diffusion is the spreading out of the influence of one or several arbitrary bits of the plaintext or/and of the key over the output bits. In block ciphers, the confusion property is provided by Substitution boxes (S-boxes) with good cryptographic properties and the diffusion is created by (generally) linear transformations with large branch number (related to codes of large minimum distance). In addition, S-boxes must be bijective in Substitution-Permutation Networks (like the Advanced Encryption Standard, AES). In the present paper, we concentrate on the design of bijective S-boxes.

An S-box with n input bits and m output bits is a multiple-output Boolean function which is often called an (n, m)-function or (if the values n and m are omitted) a vectorial Boolean function. The S-boxes used in cryptosystems should satisfy all relevant design criteria simultaneously in order to be resistant against the known attacks and, hopefully, against some attacks which may exist but are not yet efficient and might be improved in the future. Linear cryptanalysis is a known-plaintext attack based on the existence of linear relations satisfied with a probability significantly different from 1/2, relating the plaintext bits, the ciphertext bits and the key bits. To contribute to resisting linear cryptanalysis [10], S-boxes used in cryptosystems should have high nonlinearity. The differential attack, developed by Biham and Shamir [1], is a chosen-plaintext attack that exploits the correlation between the input and output differences of a pair of plaintext blocks through the network of transformations with same key. The differential attack has a substantial impact on the design of block encryption algorithms. After this attack was invented, Nyberg [11] proposed the concept of differential δ-uniformity (see Definition 1 below), for measuring the ability of a given function to contribute to resisting this attack. For a given (n, m)-function G, the value of δ should be as small as possible. It is well-known that the smallest possible value of δ is 2 when $n = m$; the functions achieving this value are called almost perfect nonlinear (APN). Furthermore, functions used as S-boxes should have algebraic degree as high as possible, or at least not low, to resist the higher order differential attack [8] introduced by Knudsen. The algebraic degree of 2 is very weak but a degree of 3 seems not enough and a degree at least 4 is safer. In addition, functions would better have high graph algebraic immunity to resist the algebraic attacks (this attack is not yet efficient but we must consider the possibility it becomes efficient in the future). Moreover, we need the S-boxes to be efficiently computable, which in software is easier if the number n of input bits is even; in fact, the best is to take n equal to a power of 2, since this allows decomposing optimally the computation of the output in $\mathbb{F}_{2^n}$ into computations in subfields. In hardware, n does not need to be a power of 2, but we like in general the cryptosystems to be efficiently

implementable in both hardware and software (which is also more convenient for the design of the whole cipher); for instance the number of input and output bits of the S-boxes of the AES is 8.

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 dimensions, we need to choose differentially 4-uniform bijections as S-boxes when n is even. 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. By now, only a few classes of differentially 4-uniform bijections in even dimensions have been found, some of them are listed in [5, 14]. We list all known APN bijections and differentially 4-uniform bijections in even dimensions below for the convenience of the reader. Clearly, 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, any bijection is CCZ-equivalent (see definition in Section 2) to its compositional inverse, so we also omit d^{-1} when d is co-prime with $2^n - 1$.

- There is only one example of APN bijection on 6 variables, given by J. Dillon [3] (the problem of finding an example of APN bijections in even number of variables had been open for ten years). But it is CCZ-equivalent to a quadratic function, which may be vulnerable by the higher order differential attack, and its expression is complex, which leads to inefficient implementation in both hardware and software.
- The inverse function x^{2^n-2} is bijective and is differentially 4-uniform when n is even [11]; it is used as the S-box of the AES with $n = 8$. This class of functions has best known nonlinearity $2^{n-1} - 2^{n/2}$ and has maximum algebraic degree $n-1$. But it is the worst possible with respect to algebraic attacks since if we denote $y = x^{-1}$ then we have the bilinear relation $x^2 y = x$. As mentioned above, though the algebraic attacks are not yet efficient, they represent a threat. A possible way to repair this weakness will be to compose the inverse function with a simple permutation, see below.
- The Gold functions x^{2^i+1} such that $\gcd(i, n) = 2$ are differentially 4-uniform. Sometimes, functions in this class are bijective since $\gcd(2^i + 1, 2^n - 1)$ divides $\gcd(2^{2i} - 1, 2^n - 1) = 2^{\gcd(2i,n)} - 1$; hence if $n \equiv 2 \pmod 4$, the function is bijective, but n is not a power of 2 and more problematically this class of functions is quadratic and can not be used as S-box.
- The Kasami functions $x^{2^{2i}-2^i+1}$ such that $n \equiv 2 \pmod 4$ and $\gcd(i, n) = 2$ are differentially 4-uniform. Sometimes, functions in this class are bijective as well. This class of functions never reaches the maximum algebraic degree $n - 1$ (but this may not be a problem). More problematically, it is related to quadratic functions when it is bijective, since $2^{2i} - 2^i + 1 = \frac{2^{3i}+1}{2^i+1}$, $2^i + 1$ is co-prime with $2^n - 1$ when $n \equiv 2 \pmod 4$ and $\gcd(i, n) = 2$; this implies that it has the form $F(x) = Q_1(x)Q_2^{-1}(x)$ where Q_1

and Q_2 are quadratic permutations. Maybe this could be used in an extended higher order differential attack. So this function, which is clearly the most interesting power function to be used as S-box, would represent some risk.

- 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. It is bijective if n is divisible by 4 but not by 8; in this case, n is not a power of 2; more problematically the function has algebraic degree 3 which is too low.
- Very recently, Qu *et. al* [14] proposed two classes of differentially 4-uniform bijections in even dimensions by adding some special Boolean functions to the inverse function. 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 a nonlinearity greater 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 $d = 3(2^t+1)$, $2 \leq t \leq n/2-1$. It has algebraic degree $n-1$ as well and a nonlinearity at least $2^{n-2} - 2^{n/2-1} - 1$. The authors did not 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 then interesting; they have high nonlinearity, maximum algebraic degree and no obvious weakness.

Except for the the inverse function (which has however a potential weakness), the Kasami functions (which may have some potential weaknesses) and the functions constructed in [14] (which have not been proven CCZ-inequivalent to the inverse function) there is no low differentially uniform bijection which can be used as S-box. Therefore, the research of more functions having all the desired features is useful and this is our motivation in the present paper.

Since the inverse function is a differentially 4-uniform bijection when n is even and has best known nonlinearity and maximum algebraic degree, we can try, as Qu *et. al*, to construct new differentially 4-uniform bijections by modifying the inverse function. A natural method for doing this is, contrary to Qu *et. al*, to compose the inverse function with a well-chosen permutation, simple enough to allow handling the behavior of the parameters above. In the present paper, we give a construction of differentially 4-uniform bijections in even dimensions by "permuting" this way the inverse function. More precisely, for any even $n \geq 6$, we show we can find a class of subsets, denoted by U, of $\mathbb{F}_{2^n}$, such that, taking as output $(x+1)^{2^n-2}$ if $x \in U$ and x^{2^n-2} otherwise gives a differentially 4-uniform permutation. For every even n, we can get at least $2^{2^{n-3}-2^{n/2-2}}$ different such sets U. For example, for $n = 6$ we can obtain 2^7 differentially 4-uniform bijections; for $n = 8$ we can obtain 2^{36} ones. We list the numbers of constructed differentially 4-uniform bijections in Table 2 for even n ranging from 6 to 20. Furthermore, for every even $n \geq 12$, we mathematically prove that if the size of U is such that $0 < |U| < (2^{n-1} - 2^{n/2})/3 - 2$ then our functions are CCZ-

inequivalent to known differentially 4-uniform power functions and to quadratic functions. This is the first time that can be mathematically proven that an infinite class of differentially 4-uniform bijections contains elements CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions. By computer investigation, we checked that when $n = 6$ all the obtained bijections are CCZ-inequivalent to known differentially 4-uniform bijections listed above. We also prove that, for any even $n \geq 6$, our functions have maximum algebraic degree $n - 1$. We also have a lower bound on the nonlinearity for all our functions, that is $2^{n-1} - 2^{n/2} - |U|$, which can be quite high in some cases since the size of U can take any even integer ranging from 2 to U_{max} (see the definition of U_{max} in Subsection 4.2). For special sets $U = U_{max}$, $U = U_{m_0}$ and $U = U_{m_1}$ (see Subsection 4.2 for their definitions) we obtain improved lower bounds on the nonlinearity and the actual nonlinearities are very high. We summarize in Table 1 the cryptographic properties of known differentially 4-uniform bijections on even variables. It is seen from Table 1 that all known differentially 4-uniform power bijections on even variables have exact or potential weakness, so we only compare our functions with known non-power differentially 4-uniform bijections proposed in [14]. We can see from Table 1 that compared with the bijections constructed in [14], our lower bound on nonlinearity with $0 < |U| < (2^{n-1} - 2^{n/2})/3 - 2$ is better than that of the functions in [14] when we restrict the size of U to at most $2^{n/2}$. We also can see from Table 1 that the lower bounds on the nonlinearity of our functions with $U = U_{max}$, $U = U_{m_0}$ and $U = U_{m_1}$ are a little less than that of the first class of functions in [14] but much better than that of the second one in [14] . Actually, for small numbers of variables n, the exact nonlinearities of these three classes of functions are very close to that of the first class in [14] (see Table 4 in Section 5) and, the most important point, our functions with $U = U_{m_0}$ and $U = U_{m_1}$ are CCZ-inequivalent to known differentially 4-uniform power functions.

Table 1: Known differentially 4-uniform bijections on even variables n

Known differentially 4-uniform bijections	Lower bound on nonlinearity	CCZ-inequivalent to known power functions for large n	Algebraic degree	Cryptographic properties
The inverse function	$2^{n-1} - 2^{n/2}$	–	$n-1$	potentially weak
The Gold functions	$2^{n-1} - 2^{n/2}$	–	2	very weak
The Kasami functions	$2^{n-1} - 2^{n/2}$	–	$< n-1$	potentially weak
Functions in [2]	$2^{n-1} - 2^{n/2}$	–	3	very weak
The first class in [14]	$2^{n-1} - 2^{n/2+1} - 2$	unknown	$n-1$	strong
The second class in [14]	$2^{n-2} - 2^{n/2-1} - 1$	unknown	$n-1$	weak
Ours with $U = U_{max}$	$2^{n-1} - 3 \cdot 2^{n/2} - 2$	unknown	$n-1$	strong
Ours with $0 < \|U\| < (2^{n-1} - 2^{n/2})/3 - 2$	$2^{n-1} - 2^{n/2} - \|U\|$	Yes	$n-1$	strong
Ours with $U = U_{m_0}$	$2^{n-1} - 2^{n/2+2} - 2$	Yes	$n-1$	very strong
Ours with $U = U_{m_1}$	$2^{n-1} - 2^{n/2+2} - 2$	Yes	$n-1$	very strong

The remainder of this paper is organized as follows. In Section 2, the notation and the necessary preliminaries required for the subsequent sections are reviewed. We propose in

Section 3 a new construction of differentially 4-uniform bijections over $\mathbb{F}_{2^n}$ (n even). In Section 4, the algebraic degree is determined and several lower bounds on the nonlinearity of the constructed functions are presented. The CCZ-inequivalence between constructed functions and known differentially 4-uniform power bijections are proved as well. In Section 5, we compare the nonlinearity of our functions to the nonlinearity of all known differentially 4-uniform bijections. Finally, Section 6 concludes the paper.

2 Preliminaries

Let n and m be two integers; mappings G from the finite field $\mathbb{F}_{2^n}$ to the finite field $\mathbb{F}_{2^m}$ are often called (n,m)-*functions* or (if the values n and m are omitted) *vectorial Boolean* functions. G is called a *Boolean function* (in n variables) when $m = 1$. We denote by $\mathcal{B}_n$ the set of Boolean functions in n variables. The basic representation of a Boolean function $f(x_1, \cdots, x_n)$ is by its *truth table*, i.e.,

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

We say that a Boolean function f is *balanced* if its truth table contains an equal number of ones and zeros, that is, if its Hamming weight equals 2^{n-1}. The *Hamming weight* of f, denoted by $\mathrm{wt}(f)$, is the size of the *support* of f, where the support of f is defined as $\mathrm{Supp}(f) = \{x \in \mathbb{F}_2^n \,|\, f(x) = 1\}$. Given two Boolean functions f and g in n variables, the *Hamming distance* between f and g is defined as $d_H(f,g) = |\{x \in \mathbb{F}_2^n \,|\, f(x) \neq g(x)\}|$. Let G be an (n,m)-function, the Boolean functions $g_1(x), \cdots, g_m(x)$ such that $G(x) = (g_1(x), \cdots, g_m(x))$, are called the coordinate functions of G. The linear combinations, with non all-zero coefficients, of the coordinate functions of G are called the *component functions* of G. The component functions of G can be expressed as $tr_1^n(aG)$, where $a \in \mathbb{F}_{2^n}^*$ and $tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Design criteria on S-boxes can be expressed as properties of the component functions or of the vectorial function itself.

For measuring the quality of a given function to resist the differential attack [1], Nyberg [11] introduced the concept of *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.*

The smaller δ is, the better is the contribution of G to resist the differential attack. The values of δ are always even since if x is a solution of equation $G(x)+G(x+a) = b$ then $x+a$ is also a solution. When $m = n$, the smallest possible value of δ is 2 and the functions achieving this value are called *almost perfect nonlinear* (APN) functions. For every $a \in \mathbb{F}_{2^n}^*$ and every $b \in \mathbb{F}_{2^m}$, we denote by $\delta_G(a,b)$ the size of the set $\{x \in \mathbb{F}_{2^n} \,|\, G(x) + G(x+a) = b\}$ and

therefore 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.

S-boxes used in cryptosystems should have high nonlinearity in order to prevent linear cryptanalysis [10]. The *nonlinearity* $NL(G)$ of an (n,m)-function G is the minimum Hamming distance between all the component functions $tr_1^n(aG)$ of G, where $a \in \mathbb{F}_{2^n}^*$, and all affine functions on n variables. We have:

$$NL(G) = 2^{n-1} - \frac{1}{2} \max_{(a,b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^n}} |W_G(a,b)|,$$

where $W_G(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(aG(x)+bx)}$ is the value of the *Walsh transform* of G at (a,b); the multi-set of these values is called the *Walsh spectrum* of G. We call *extended Walsh spectrum* of G the multi-set of their absolute values. It is well known that the nonlinearity $NL(G)$ is upper-bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$ for $n = m$ and the best known value of $NL(G)$ is $2^{n-1} - 2^{\frac{n}{2}}$ for even $n = m$.

The algebraic degree is also an important parameter of the S-boxes used in cryptosystems. Every (n,m)-function G can be uniquely represented by an univariate polynomial:

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

The *algebraic degree*, denoted by $\deg(G)$, is defined as the maximal 2-weight of the exponents 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. S-boxes used in cryptosystems should have high algebraic degree, or at least not a low one, to resist the higher order differential attack; it is known that the algebraic degree of bijective functions on n variables is upper-bounded by $n-1$.

Two functions are considered as equivalent if one can be obtained from the other by some simple transformation (and a function equivalent to a weak function under some transformation preserving the attack on this function will be weak as well). There are mainly three such equivalence notions, called affine equivalence, extended affine equivalence (in brief, EA equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence), respectively. Given two (n,n)-functions G and H, we say that they are *affine equivalent* if $G(x) = A_1(H(A_2(x)))$, where A_1 and A_2 are affine permutations on $\mathbb{F}_{2^n}$; we say that they are *EA-equivalent* if $G(x) = A_1(H(A_2(x))) + A_3(x)$, where A_1 and A_2 are affine permutations on $\mathbb{F}_{2^n}$ and A_3 is an affine function on F_{2^n}; we say that they are *CCZ-equivalent* [6, 4] 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 $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, where L_1 and L_2 are two affine functions from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, such that $y = G(x) \Leftrightarrow L_2(x,y) = H(L_1(x,y))$. It is well-known that EA equivalence implies CCZ-equivalence, but the converse is false. The differential spectrum and extended Walsh spectrum are invariant under EA and CCZ-equivalence; the algebraic degree is not invariant

under CCZ-equivalence but it is invariant under EA equivalence, for functions of degrees at least 2.

3 New differentially 4-uniform bijections

Let n be an even integer. In this section, we obtain a class of differentially 4-uniform bijections of the form $x \in \mathbb{F}_{2^n} \to (T(x))^{-1} \in \mathbb{F}_{2^n}$ (we shall call such composition with T "permuting the inverse function"), where T is a bijective mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ and $x \to x^{-1}$ is the inverse function, with the convention $0^{-1} = 0$ (we shall always use this kind of convention in the sequel). It is well-known that the inverse function is a differentially 4-uniform bijection.

Construction 1. *Let $n \geq 6$ be an even number and U be a subset of $\mathbb{F}_{2^n}$ satisfying:*
a) for any $x \in U$, $x + 1 \in U$ and
b) for any $x \in U$, $tr_1^n(x^{-1}) = 1$.
We define an (n, n)-function F on $\mathbb{F}_{2^n}$ as follows:

$$F(x) = \begin{cases} (x+1)^{-1}, & x \in U \\ x^{-1}, & x \in \mathbb{F}_{2^n} \setminus U \end{cases}.$$

In fact, the function F can be rewritten as

$$F(x) = (x + \delta_U(x))^{-1} \tag{1}$$

where δ_U is the indicator function of U, i.e. $\delta_U(x) = 1$ if $x \in U$ and $\delta_U(x) = 0$ otherwise. Since U is stable under the addition by 1, i.e.,

$$\delta_U(x) + \delta_U(x+1) = 0, \text{ for all } x \in \mathbb{F}_{2^n},$$

we can easily see that $x \to x + \delta_U(x)$ is its own inverse, and therefore is a bijection on $\mathbb{F}_{2^n}$. Hence, function F is bijective on $\mathbb{F}_{2^n}$.

3.1 Differential 4-uniformity

In what follows, we shall prove that any function F, defined above, is differentially 4-uniform. For doing this, we first need several preliminary results.

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 $\mu(x) = 0$ has 2 solutions if and only if $tr_1^n(b^{-2}ac) = 0$.*

Lemma 2. *Let n be a positive integer. For any $b \in \mathbb{F}_{2^n}^*$, let us define the polynomial $\mu(x) = bx^2 + (1 + b)x + b^{-1} \in \mathbb{F}_{2^n}[x]$. If $\mu(x) = 0$ has 2 solutions λ, ν then we have $tr_1^n(\lambda^{-1}) = tr_1^n(\nu^{-1}) = 0$ if n is even and $tr_1^n(\lambda^{-1}) = tr_1^n(\nu^{-1}) = 1$ if n is odd.*

Proof. The two roots λ and ν of the equation $bx^2 + (1+b)x + b^{-1} = 0$ are nonzero since $b \neq 0$. It is sufficient to show that $tr_1^n(\lambda^{-1}+1) = tr_1^n(\nu^{-1}+1) = 0$. Note that λ^{-1} and ν^{-1} are the roots of the reciprocal equation $b + (1+b)x + b^{-1}x^2 = 0$. Multiplying by b, we have $x^2 + (b+b^2)x + b^2 = 0$. Given an equation $x^2 + Sx + P = 0$, adding 1 to each root corresponds to keeping the same sum S and to replacing the product P by $P + S + 1$. We obtain here the equation $x^2 + (b+b^2)x + b + 1 = 0$ having roots $\lambda^{-1}+1$ and $\nu^{-1}+1$. What we need is to prove that the roots of this equation have null trace, that is, have the form $u+u^2$. Given an equation $x^2+sx+p=0$ whose roots are u and v, the equation whose roots are $u+u^2$ and $v+v^2$ is $x^2+Sx+P=0$ with $S = s+s^2$ and $P = p(1+s+p)$. Applying this observation to the equation $x^2 + (b+b^2)x + b + 1 = 0$ with $s = b$ and $S = b+b^2$, the roots have null trace only if there exists p in $\mathbb{F}_{2^n}$ such that $p^2 + (b+1)p = b+1$. The existence of p is guaranteed by Lemma 1, due to the fact that $tr_1^n((b+1)^{-1}) = tr_1^n((b+1)^{-2}) = 0$, where the latter follows from applying Lemma 1 to the original equation $bx^2 + (1+b)x + b^{-1} = 0$ with two solutions. □

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

Lemma 3. *Let U be the set defined in Construction 1. For any $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, let us consider the four following equations on $\mathbb{F}_{2^n}$:*

$$x^{-1} + (x+a)^{-1} = b, \qquad x, x+a \in \mathbb{F}_{2^n} \setminus U \tag{2}$$

$$(x+1)^{-1} + (x+1+a)^{-1} = b, \qquad x, x+a \in U \tag{3}$$

$$(x+1)^{-1} + (x+a)^{-1} = b, \quad x \in U, x+a \in \mathbb{F}_{2^n} \setminus U \tag{4}$$

$$x^{-1} + (x+1+a)^{-1} = b, \quad x \in \mathbb{F}_{2^n} \setminus U, x+a \in U. \tag{5}$$

If $(a,b) \in \mathbb{F}_{2^n} \setminus \{0,1\} \times \mathbb{F}_{2^n}^*$, then the following statements hold:

1) The sum of the numbers of solutions of (2) and (3) is at most 4. Moreover:

1.1) If $ab \neq 1$, then the sum of the numbers of solutions of (2) and (3) is at most 2.

1.2) If $a \in U$ and $b(a+1) = 1$, then equations (2) and (3) have no solution.

2) The sum of the numbers of solutions of (4) and (5) is at most 4. Moreover:

2.1) If $b(a+1) \neq 1$ or $a \notin U$, then the sum of the numbers of solutions of (4) and (5) is at most 2.

2.2) If $ab = 1$, then equations (4) and (5) have no solution.

Lemma 3 will be proved in Appendix. Now we are ready to prove our main result.

Theorem 1. *The bijection F defined in Construction 1 is differentially 4-uniform.*

Proof. Let us check that

$$F(x) + F(x+a) = b \tag{6}$$

has at most 4 solutions for every fixed $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$. By the definition of F, (6) is equivalent to equations (2)-(5). Recall that F is a bijection. Then (6) has no solution for $(a, b) \in \mathbb{F}_{2^n}^* \times \{0\}$. So we only need to consider $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$.

Firstly, we can see that (6) has at most 4 solutions if $(a, b) \in \{1\} \times \mathbb{F}_{2^n}^*$. In this case, (2) and (3) become the same equation $x^{-1} + (x+a)^{-1} = b$ with $x, x+a$ in U and $\mathbb{F}_{2^n} \setminus U$ respectively. Since the function $x \to x^{-1}$ is 4 uniform, we can see that the sum of the numbers of solutions of (2) and (3) is at most 4; and (4), (5) have no solution for $a = 1$ since we assume $b \neq 0$.

Secondly, we prove that (6) has at most 4 solutions for every $(a, b) \in \mathbb{F}_{2^n} \setminus \{0, 1\} \times \mathbb{F}_{2^n}^*$.
Case A. $ab = 1$.
It follows from 1) in Lemma 3 that the sum of the numbers of solutions of (2) and (3) is at most 4 and from 2.2) of Lemma 3 that equations (4) and (5) have no solution. Therefore, (6) has at most 4 solutions.
Case B. $ab \neq 1$
• **Case B-1** $b(a+1) = 1$ and $a \in U$
According to 1.2) in Lemma 3, equations (2) and (3) have no solution in this case, and according to 2) in Lemma 3, the sum of the numbers of solutions of (4) and (5) is at most 4. This implies that (6) has at most 4 solutions in this case.
• **Case B-2** $b(a+1) \neq 1$ or $a \notin U$
According to 1.1) (2.1) resp.) in Lemma 3 respectively, the sum of the numbers of solutions of (2) and (3) ((4) and (5) resp.) is at most 2. So (6) has at most 4 solutions.

Hence, function F is differentially 4-uniform. □

4 Other cryptographic properties of F

In this section, we focus on the cryptographic properties of F. We first prove that F has maximum algebraic degree $n-1$. In addition, we obtain several lower bounds on the nonlinearity for F. Finally, we show that our functions, in some cases, are CCZ-inequivalent to known differentially 4-uniform power functions, including the inverse function, and to quadratic functions.

4.1 Algebraic degree

Theorem 2. *For every even $n \geq 6$, F has algebraic degree $n-1$.*

Proof. Recall 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 $n-1$. Recall the following two facts:

1. F has algebraic degree at most k if and only if, for every $a \in \mathbb{F}_{2^n}^*$, the Boolean function $tr_1^n(aF)$ defined on $\mathbb{F}_{2^n}$ has algebraic degree at most k;

2. An n-variable Boolean function f has algebraic degree n if and only if $\mathrm{wt}(f) \equiv 1 \pmod 2$.

If F has algebraic degree at most k, we have that, for every n-variable Boolean function h with $\deg(h) \leq n-k-1$, the expression $tr_1^n(\sum_{x\in\mathbb{F}_{2^n}} aF(x)h(x)) = \sum_{x\in\mathbb{F}_{2^n}} tr_1^n(aF(x))h(x)$ is null for all $a \in \mathbb{F}_{2^n}^*$ and hence $\sum_{x\in\mathbb{F}_{2^n}} F(x)h(x) = 0$.

Therefore, for proving that F has algebraic degree at least $n-1$, it is sufficient to show that there exists a Boolean function h with algebraic degree at most 1 such that $\sum_{x\in\mathbb{F}_{2^n}} F(x)h(x) \neq 0$. Taking $h(x) = tr_1^n(x)$ which has algebraic degree 1, we have

$$\begin{aligned}
& \sum_{x\in\mathbb{F}_{2^n}} F(x)h(x) \\
= & \sum_{x\in\mathbb{F}_{2^n}} tr_1^n(x)(x+\delta_U(x))^{-1} \\
= & \sum_{x\in\mathbb{F}_{2^n}} tr_1^n(x+\delta_U(x))x^{-1} \\
= & \sum_{x\in U} tr_1^n(x+1)x^{-1} + \sum_{x\in\mathbb{F}_{2^n}\setminus U} tr_1^n(x)x^{-1} \\
= & \sum_{x\in\mathbb{F}_{2^n}} tr_1^n(x)x^{-1} \\
= & \sum_{x\in\mathbb{F}_{2^n}^*} \sum_{i=0}^{n-1} x^{2^i-1} \\
= & \ 1
\end{aligned}$$

where we use that $x \to x+\delta_U(x)$ is its own inverse in the second identity, that $tr_1^n(1) = 0$ for even n in the fourth identity, and that $\sum_{x\in\mathbb{F}_{2^n}^*} x^{2^i-1} = \sum_{x\in\mathbb{F}_{2^n}^*} 1 = 1 (\mathrm{mod}\, 2)$ for $i = 0$ and $\sum_{x\in\mathbb{F}_{2^n}^*} x^{2^i-1} = 0$ for $0 < i < n$ in the last identity. □

4.2 Nonlinearity

In this subsection, we will give several lower bounds on the nonlinearity of F. Let us first give a lower bound on the nonlinearity of F, which only relies on the nonlinearity of the inverse function and on the size of U.

Let us denote by I the inverse function. We recall what we know on the Walsh spectrum of the component functions of I.

Lemma 4 ([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 $[-2^{n/2+1}+1, 2^{n/2+1}+1]$.*

By Lemma 4, the following naive bound on the nonlinearity of F is straightforward.

Theorem 3. *For every even $n \geq 6$, we have $NL(F) \geq 2^{n-1} - 2^{n/2} - |U|$.*

Proof. For any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, we have

$$\begin{aligned} & |W_F(a,b)| \\ = & |\sum_{x \in \mathbb{F}_{2^n} \setminus U} (-1)^{tr_1^n(ax^{-1}+bx)} + \sum_{x \in U} (-1)^{tr_1^n(a(x+1)^{-1}+bx)}| \\ = & |\sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(ax^{-1}+bx)} + \sum_{x \in U} (-1)^{tr_1^n(a(x+1)^{-1}+bx)} - \sum_{x \in U} (-1)^{tr_1^n(ax^{-1}+bx)}| \\ \leq & |W_I(a,b)| + 2|U|. \end{aligned}$$

By Lemma 4 we have $|W_F(a,b)| \leq 2^{n/2+1} + 2|U|$ and therefore $NL(F) \geq 2^{n-1} - 2^{n/2} - |U|$. □

This bound indicates that if the size of U is very small, then the nonlinearity of F is close to that of I, which is very high. However, if the size of U is too small, then F is very close to the inverse function. Then if there exists an attack on the inverse function, this attack can represent a threat for function F too. Thus, the size of U should not be too small.

For even $n \geq 6$, we can see that the union of all the sets U satisfying the conditions of Construction 1, that is the set $\{x \in \mathbb{F}_{2^n} \,|\, tr_1^n(x^{-1}) = tr_1^n((x+1)^{-1}) = 1\}$, that we shall denote by $U_{\max}$ from now on, is the largest one. Let us define $U_{m_0} = \{x \in U_{\max} \,|\, tr_1^n(x) = 0\}$ and $U_{m_1} = \{x \in U_{\max} \,|\, tr_1^n(x) = 1\}$ from now on. We can see that $U_{\max} = U_{m_0} \cup U_{m_1}$, and both U_{m_0} and U_{m_1} satisfy the two conditions for U in Construction 1. It is easily checked that

$$\delta_{U_{\max}}(x) = tr_1^n(x^{-1}) tr_1^n((x+1)^{-1}) \quad (7)$$

$$\delta_{U_{m_0}}(x) = (1 + tr_1^n(x)) tr_1^n(x^{-1}) tr_1^n((x+1)^{-1}) \quad (8)$$

and

$$\delta_{U_{m_1}}(x) = tr_1^n(x) tr_1^n(x^{-1}) tr_1^n((x+1)^{-1}) \quad (9)$$

In what follows, we will give three lower bounds on the nonlinearity of F with $U = U_{\max}, U_{m_0}, U_{m_1}$ respectively.

We need some lemmas and corollaries, which will be useful for establishing our lower bounds.

Lemma 5. *Let n be a positive integer and h be a Boolean function defined on $\mathbb{F}_{2^n}$. Then for any $b \in \mathbb{F}_{2^n}$, the following statements hold:*

1) $\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=0} (-1)^{h(x)+tr_1^n(bx)} = \frac{1}{2}\big(W_h(b) + W_h(b+1)\big)$;

2) $\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=1} (-1)^{h(x)+tr_1^n(bx)} = \frac{1}{2}\big(W_h(b) - W_h(b+1)\big)$;

3) $|\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=c} (-1)^{h(x)+tr_1^n(bx)}| \le \max_{a\in\mathbb{F}_{2^n}} |W_h(a)|$, *where* $c \in \mathbb{F}_2$.

We omit the proof of Lemma 5, which follows easily from the fact that $\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x)} = 0$.

Lemma 6 ([14])**.** *Let n be a positive integer, then $|\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax+bx^{-1}+x^2(x+1)^{-1})}| \le 2\lfloor 2^{n/2+1}\rfloor + 4$ 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 6 is equivalent to:

Corollary 1. *For any positive integer n, 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 $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.*

Lemma 7. *For any even integer n, we have*

$$\max_{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*} |\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=c} (-1)^{tr_1^n(ax^{-1}+bx)+tr_1^n(x^{-1})tr_1^n((x+1)^{-1})}| \le 6\cdot 2^{n/2} + 4,$$

where $c \in \mathbb{F}_2$.

Proof. For any $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax^{-1}+bx)+tr_1^n(x^{-1})tr_1^n((x+1)^{-1})} \\
=\ &\sum_{x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2} (-1)^{tr_1^n(ax+bx^{-1})+tr_1^n(x)tr_1^n(x(x+1)^{-1})} + \sum_{x\in\mathbb{F}_2} (-1)^{tr_1^n(ax+bx^{-1})+tr_1^n(x)tr_1^n((x+1)^{-1})} \\
&\text{(by changing } x \text{ into } x^{-1} \text{ and checking for } x = 0, 1) \\
=\ &\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax+bx^{-1})+tr_1^n(x)tr_1^n((x+1)^{-1})} \text{ (since } tr_1^n(1) = 0 \text{ for even } n) \\
=\ &\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=0} (-1)^{tr_1^n(ax+bx^{-1})} + \sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=1} (-1)^{tr_1^n(ax+bx^{-1}+(x+1)^{-1})}
\end{aligned}$$

It follows from Lemmas 4 and 5 that

$$|\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=c} (-1)^{tr_1^n(ax+bx^{-1})}| \le 2^{n/2+1}.$$

By Corollary 1 and Lemma 5, we get

$$|\sum_{x\in\mathbb{F}_{2^n},tr_1^n(x)=c}(-1)^{tr_1^n(ax+bx^{-1}+(x+1)^{-1})}| \leq 2^{n/2+2}+4$$

Therefore, we have $\max_{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*}|\sum_{x\in\mathbb{F}_{2^n},tr_1^n(x)=c}(-1)^{tr_1^n(ax^{-1}+bx)+tr_1^n(x^{-1})tr_1^n((x+1)^{-1})}| \leq 6\cdot 2^{n/2}+4$. □

Lemma 8. *Let n be an integer and f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(x)+f(x+1)=0$. Then for any $(a,b)\in F_{2^n}^*\times\mathbb{F}_{2^n}$, we have $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(a(x+f(x))^{-1}+bx)} = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax^{-1}+b(x+f(x)))}$.*

Proof. Indeed, $x\to x+f(x)$ is a bijection on $\mathbb{F}_{2^n}$. The equality is then obtained by the change of variable $x:=x+f(x)$. □

We are now ready to give the lower bounds on the nonlinearity of F with $U=U_{\max}, U_{m_0}$ and U_{m_1} respectively

Theorem 4. *For every even $n\geq 6$, taking $U=U_{\max}$, we have $NL(F)\geq 2^{n-1}-3\cdot 2^{n/2}-2$.*

Proof. If $b=0$, then we have $W_F(a,b)=0$ for all $a\in\mathbb{F}_{2^n}^*$ since F is bijective. We assume now that $b\neq 0$. Then, by Lemma 8 and Equation (7), we have

$$\begin{aligned} W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(a(x+\delta_{U_{\max}}(x))^{-1}+bx)} \\ &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax^{-1}+b(x+\delta_{U_{\max}}(x)))} \\ &= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax^{-1}+bx)+\delta_{U_{\max}}(x)tr_1^n(b)}. \end{aligned}$$

If $tr_1^n(b)=0$, then $W_F(a,b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax^{-1}+bx)}$ and hence $|W_F(a,b)|\leq 2^{n/2+1}$ according to Lemma 4. If $tr_1^n(b)=1$, we have

$$\begin{aligned} & |W_F(a,b)| \\ = & |\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax^{-1}+bx)+\delta_{U_{\max}}(x)}| \\ = & |\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax^{-1}+bx)+tr_1^n(x^{-1})tr_1^n((x+1)^{-1})}|, \end{aligned}$$

which is less or equal to $6\cdot 2^{n/2}+4$ by Lemma 7.

We deduce that $|W_F(a,b)|\leq 6\cdot 2^{\frac{n}{2}+1}+4$ for all $(a,b)\in F_{2^n}^*\times\mathbb{F}_{2^n}^*$. Recall that $W_F(a,b)=0$ if $b=0$. Then we can see that $NL(F)\geq 2^{n-1}-3\cdot 2^{n/2}-2$. □

Theorem 5. *For every even $n \geq 6$, taking $U = U_{m_0}$, we have $NL(F) \geq 2^{n-1} - 2^{n/2+2} - 2$.*

Proof. Since F is bijective, we have $W_F(a,b) = 0$ for all $a \in \mathbb{F}_{2^n}^*, b = 0$. We assume now that $b \neq 0$. Applying Lemma 8 to Equation (8), we have

$$\begin{aligned} W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(a(x+\delta_{U_{m_0}}(x))^{-1}+bx)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax^{-1}+b(x+\delta_{U_{m_0}}(x)))} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax^{-1}+bx)+\delta_{U_{m_0}}(x)tr_1^n(b)}. \end{aligned}$$

If $tr_1^n(b) = 0$, then $W_F(a,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax^{-1}+bx)}$ and therefore $|W_F(a,b)| \leq 2^{n/2+1}$, by Lemma 4.

Consider the case $tr_1^n(b) = 1$, we get

$$\begin{aligned} W_F(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax^{-1}+bx)+\delta_{U_{m_0}}(x)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(ax^{-1}+bx)+(1+tr_1^n(x))tr_1^n(x^{-1})tr_1^n((x+1)^{-1})} \\ &= \sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=1} (-1)^{tr_1^n(ax^{-1}+bx)} + \\ &\quad \sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=0} (-1)^{tr_1^n(ax^{-1}+bx)+tr_1^n(x^{-1})tr_1^n((x+1)^{-1})} \end{aligned}$$

By Lemmas 4 and 5, we have

$$\left| \sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=1} (-1)^{tr_1^n(ax^{-1}+bx)} \right| \leq 2^{n/2+1}.$$

According to Lemma 7, we have

$$\left| \sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=0} (-1)^{tr_1^n(ax^{-1}+bx)+tr_1^n(x^{-1})tr_1^n((x+1)^{-1})} \right| \leq 6 \cdot 2^{n/2} + 4.$$

Hence, $|W_F(a,b)| \leq 8 \cdot 2^{n/2} + 4$ for $tr_1^n(b) = 1$.

Combining above cases, we can see that $|W_F(a,b)| \leq 8 \cdot 2^{n/2} + 4$ for all $(a,b) \in F_{2^n}^* \times \mathbb{F}_{2^n}^*$. Recall that $W_F(a,b) = 0$ if $b = 0$. Therefore, we have $NL(F) \geq 2^{n-1} - 2^{n/2+2} - 2$. □

Similar to the case $U = U_{m_0}$, we can easily get a lower bound on the nonlinearity of F with $U = U_{m_1}$.

Theorem 6. *For every even $n \geq 6$, taking $U = U_{m_1}$, we have $NL(F) \geq 2^{n-1} - 2^{n/2+2} - 2$.*

4.3 CCZ-inequivalence

Since our functions are derived from the inverse function, we need to investigate whether they are CCZ-inequivalent to the inverse function. We will prove that, for any even $n \geq 6$, our functions are CCZ-inequivalent to the inverse function when the size of U is such that $0 < |U| < (2^{n-1} - 2^{n/2})/3 - 2$. Besides, we also prove that our functions are CCZ-inequivalent to the Gold functions, the Kasami functions, the functions discussed in [2] and quadratic functions. Thus, our functions are CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions for any even $n \geq 6$ when the size of U is such that $0 < |U| < (2^{n-1} - 2^{n/2})/3 - 2$.

Proving the CCZ-inequivalence between two functions by directly using the definition of CCZ-equivalence is very difficult, but some CCZ-invariant parameters can be proved to be different for the two functions. Our results on the CCZ-inequivalence rely on the following lemma.

Lemma 9 ([6, 4])**.** *The differential and extended Walsh spectra are CCZ-invariant parameters.*

As we know, for even n, the number of pairs $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ such that $\delta_I(a, b) = 4$ is $2^n - 1$. According to Lemma 9, for proving that F is CCZ-inequivalent to the inverse function, we only need to prove that the number of pairs (a, b) such that $\delta_F(a, b) = 4$ is not $2^n - 1$; similarly, for proving that F is not CCZ-equivalent to the Gold functions, the Kasami functions, the functions discussed in [2] and quadratic functions, we only need to show that F has extended Walsh spectrum distinct from those of these functions.

We first need the following corollaries which can be deduced from Lemma 4.

Corollary 2. *For even $n \geq 6$, we have $2^{n-2} - 2^{n/2-1} \leq |U_{\max}| \leq 2^{n-2} + 2^{n/2-1}$*

Proof. Let $R = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{-1}+(1+x)^{-1})}$. On one hand, since the Hamming weights of the functions $tr_1^n(x^{-1})$ and $tr_1^n((1+x)^{-1})$ equal 2^{n-1}, then $R = 2^n - 2\mathrm{wt}(tr_1^n(x^{-1}) + tr_1^n((1+x)^{-1})) = 2^n - 2\mathrm{wt}(tr_1^n(x^{-1})) - 2\mathrm{wt}(tr_1^n((1+x)^{-1})) + 4|U_{\max}| = -2^n + 4|U_{\max}|$ and $|U_{\max}| = 2^{n-2} + R/4$. On the other hand, $R = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{-1}+(1+x)^{-1})} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x+(1+x^{-1})^{-1})} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x+1+(x+1)^{-1})} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x+x^{-1})}$, which can be checked separately for $x \notin \mathbb{F}_2$ and $x \in \mathbb{F}_2$ by using that $tr_1^n(1) = 0$. Then by Lemma 4 we have $|R| \leq 2^{n/2+1}$ and hence $2^{n-2} - 2^{n/2-1} \leq |U_{\max}| \leq 2^{n-2} + 2^{n/2-1}$. □

Remark 1. *Obviously, the size of U can be any even integer ranging from 2 to $U_{\max}$. By Corollary 2, we can see that there are at least $2^{2^{n-3}-2^{n/2-2}}$ different sets U. We list in Table 2 the exact numbers of sets U for even n ranging from 6 to 20.*

Corollary 3. *Let $n \geq 3$ be an integer and $h \in \mathcal{B}_n$ be defined as $h(x) = tr_1^n(x^{-1})$. Define $C_{h_{\mu,\nu}}(\tau) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(\mu x^{-1}) + tr_1^n(\nu(x+\tau)^{-1})}$, where $\mu, \nu, \tau \in \mathbb{F}_{2^n}^*$. Then the value of $C_{h_{\mu,\nu}}(\tau)$ belongs to $[-2^{n/2+1} - 3, 2^{n/2+1} + 1]$ and is divisible by 4.*

Table 2: The exact numbers of the sets U

n	6	8	10	12	14	16	18	20
numbers of U	2^7	2^{36}	2^{121}	2^{518}	2^{2059}	2^{8136}	2^{32893}	2^{130922}

Proof. For any $\mu, \nu, \tau \in \mathbb{F}_{2^n}^*$, we have (still using the convention $\frac{1}{0} = 0$)

$$\begin{aligned}
& C_{h_{\mu,\nu}} \\
= & \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(\frac{\mu}{x}+\frac{\nu}{x+\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\tau\}} (-1)^{tr_1^n(\frac{\mu}{x}+\frac{\nu}{x+\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\tau^{-1}\}} (-1)^{tr_1^n(\mu x+\frac{\nu x}{1+\tau x})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\tau^{-1}\}} (-1)^{tr_1^n(\mu x+\frac{1}{1+\tau x}\cdot\frac{\nu}{\tau}+\frac{\nu}{\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1\}} (-1)^{tr_1^n(\frac{\mu x}{\tau}+\frac{\nu}{\tau x}+\frac{\mu}{\tau}+\frac{\nu}{\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,\frac{\tau}{\nu}\}} (-1)^{tr_1^n(\frac{1}{x}+\frac{\mu\nu}{\tau^2}x)+tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})} \\
= & \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(\frac{1}{x}+\frac{\mu\nu}{\tau^2}x)+tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} - (-1)^{tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} - (-1)^{tr_1^n(0)} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})}
\end{aligned}$$

where the third, fifth, and sixth identities hold by changing x to $\frac{1}{x}$, $\frac{x+1}{\tau}$, and $\frac{\nu x}{\tau}$ respectively. Note that $-(-1)^{tr_1^n(\frac{\mu}{\tau}+\frac{\nu}{\tau})} - (-1)^{tr_1^n(0)} + (-1)^{tr_1^n(\frac{\mu}{\tau})} + (-1)^{tr_1^n(\frac{\nu}{\tau})}$ equals 0 or -4. According to Lemma 4, we can see that $C_{h_{\mu,\nu}}(\tau)$ belongs to $[-2^{n/2+1}-3, 2^{n/2+1}+1]$ and is divisible by 4. This finishes the proof. □

In addition, we need the following lemmas.

Lemma 10. *Let n be an even number and U be a set defined in Construction 1. Then for any $\beta \in U$, there is no $a \in \mathbb{F}_{2^n}$ such that*

$$a(\beta+1)^{-1} + a(\beta+a)^{-1} + 1 = 0, \tag{10}$$

Proof. In (10), note that $a \neq \beta$ and $\beta \neq 1$ because of $1 \notin U$. Multiplied by $(\beta+1)(\beta+a)$, it gives $a^2 + \beta a + (\beta^2+\beta) = 0$. Further, $\beta \neq 0$ because of $0 \notin U$. We then have $tr_1^n((\beta^2+\beta)\beta^{-2}) = tr_1^n(1+\beta^{-1}) = tr_1^n(1) + tr_1^n(\beta^{-1}) = 0+1 = 1$ for n even and $\beta \in U$. Hence, it follows from Lemma 1 that $a^2 + \beta a + (\beta^2+\beta) = 0$ has no solution in $\mathbb{F}_{2^n}$. That is to say, there is no element $a \in \mathbb{F}_{2^n}$ satisfying Equation (10). □

Lemma 11. *Let n be an even number and U be the set defined in Construction 1. Then for any $\beta \in U$ and $\xi \in \mathbb{F}_{2^n}$, there are at most two elements $a \in \mathbb{F}_{2^n} \setminus \{0, \beta\}$ such that $\big((\beta+1)^{-1} + (\beta+a)^{-1}\big)\xi^2 + \big(a(\beta+1)^{-1} + a(\beta+a)^{-1}\big)\xi + a = 0$.*

Proof. If $\xi = 0$, then there is no such element $a \in \mathbb{F}_{2^n} \setminus \{0, \beta\}$. So we assume that $\xi \neq 0$. Since $a(\beta+a)^{-1} = 1 + \beta(\beta+a)^{-1}$, the equality

$$\Big((\beta+1)^{-1} + (\beta+a)^{-1}\Big)\xi^2 + \Big(a(\beta+1)^{-1} + a(\beta+a)^{-1}\Big)\xi + a = 0$$

is equivalent to

$$(\xi^2 + \beta\xi)(\beta+a)^{-1} + (\xi(\beta+1)^{-1} + 1)a + (\xi + \xi^2(\beta+1)^{-1}) = 0. \tag{11}$$

Since $\beta \neq a$, multiplied by $\beta + a$, (11) becomes

$$(\xi^2 + \beta\xi) + (\xi(\beta+1)^{-1} + 1)(\beta a + a^2) + (\xi + \xi^2(\beta+1)^{-1})(\beta + a) = 0,$$

or equivalently

$$\big(\xi(\beta+1)^{-1} + 1\big)a^2 + (\xi(\beta+1)^{-1} + 1)(\beta + \xi)a + \xi^2(\beta+1)^{-1} = 0, \tag{12}$$

which is a quadratic equation in a. Note that $\xi \neq 0$. Then we have $\xi^2(\beta+1)^{-1} \neq 0$ and hence the coefficients of Equation (12) do not vanish simultaneously, implying that for any $\beta \in U$ and $\xi \in \mathbb{F}_{2^n}^*$, there are at most two elements $a \in \mathbb{F}_{2^n} \setminus \{0, \beta\}$ satisfying Equation (11). □

We now show the CCZ-inequivalence of our functions.

Theorem 7. *For every even $n \geq 6$, the functions generated by Construction 1 are CCZ-inequivalent to the inverse function when the set U is such that $0 < |U| < \frac{2^{n-1}-2^{n/2}}{3} - 2$.*

Proof. As mentioned before, it suffices to show that the number of pairs $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ such that $\delta_F(a, b) = 4$ is strictly greater than $2^n - 1$ when $0 < |U| \leq \lceil \frac{2^{n-1}-2^{n/2}}{3} \rceil - 3$. Recall that (6) is equivalent to Equations (2)-(5). For obtaining such a lower bound, we consider the following two cases:

• **Case 1.** $ab = 1$

For every $a \notin U$, we can see that $x = 0, x = a$ are two solutions of Equation (2). Let us bound from below the number of cases that Equation (2) has two more solutions. It follows from $ab = 1$ that $tr_1^n((ab)^{-1}) = tr_1^n(1) = 0$ and hence the equation $bx^2 + abx + a = 0$ has two solutions, that is, $\big(\frac{x}{a}\big)^2 + \frac{x}{a} = \frac{1}{ab}$ has two solutions. More precisely, it is easy to see that, denoting by d the integer $(2^n - 1)/3$ and by α a primitive element of $\mathbb{F}_{2^n}$, the two solutions are $a\alpha^d$ and $a\alpha^d + a$ since $\alpha^{2d} + \alpha^d = 1$. Hence, if $a\alpha^d \notin U$ and $a\alpha^d + a \notin U$ then we can check that $a\alpha^d$ and $a\alpha^d + a$ are two more solutions of Equation (2). Note that $a\alpha^d$

and $a\alpha^d + a$ range over $\mathbb{F}_{2^n}^*$ when a ranges over $\mathbb{F}_{2^n}^*$. So there are at most $2|U|$ elements $a \in \mathbb{F}_{2^n}^*$ such that $a\alpha^d \in U$ or $a\alpha^d + a \in U$. Further by excluding the case where $a \in U$, there are at least $2^n - 1 - 3|U|$ pairs (a, a^{-1}) with $\delta_F(a, a^{-1}) = 4$.

• **Case 2.** $ab \neq 1$, $b \neq 0$

Note that we need to exclude $b = 0$ because, F being bijective, we have $\delta_F(1, 0) = 0$. For simplicity, we restrict our discussion to the case that there exists $\beta \in U$ such that $b = (\beta + 1)^{-1} + (\beta + a)^{-1}$, which satisfies $ab \neq 1$ by Lemma 10. In this case, β and $\beta + a$ are respectively the solutions of Equations (4) and (5) only if $\beta \in U$ and $\beta + a \in \mathbb{F}_{2^n} \setminus U$. Additionally, we require $tr_1^n((ab)^{-1}) = 0$ so that $bx^2 + abx + a = 0$ has two solutions and then (2) may have two solutions. We shall bound from below the number of such pairs (a, b).

Firstly we bound the cardinality of $T_\beta = \{a \in \mathbb{F}_{2^n} \setminus \{0, 1, \beta\} \,|\, tr_1^n((ab)^{-1}) = 0, b = (\beta + 1)^{-1} + (\beta + a)^{-1}\}$ for given $\beta \in U$, where we exclude $a = 1$ for avoiding $b = 0$ and $a = \beta$ for simplifying our proof. Since

$$\begin{aligned}
(ab)^{-1} &= (a(\beta + 1)^{-1} + a(\beta + a)^{-1})^{-1} \\
&= (\beta^2 + \beta + a\beta + a)(a + a^2)^{-1} \\
&= (\beta^2 + \beta + a\beta + a)(a^{-1} + (a + 1)^{-1}) \\
&= (\beta^2 + \beta)a^{-1} + \beta + 1 + (\beta^2 + \beta + a\beta + a)(a + 1)^{-1} \\
&= (\beta^2 + \beta)a^{-1} + (\beta^2 + 1)(a + 1)^{-1},
\end{aligned}$$

applying Corollary 3 in place of $x = a$, $\mu = \beta^2 + \beta$, $\nu = \beta^2 + 1$ and $\tau = 1$, we deduce that $C_{h_{\mu,\nu}}(\tau) = 2N - 2^n \geq -2^{n/2+1} - 3$ where N is the number of $a \in \mathbb{F}_{2^n}$ with $tr_1^n((ab)^{-1}) = 0$. That is, $2N - 2^n \geq -2^{n/2+1}$ because $C_{h_{\mu,\nu}}(\tau)$ is divisible by 4 and n is even. Therefore, $|T_\beta| \geq 2^{n-1} - 2^{n/2} - 3$.

For any $a \in T_\beta$, assume that the two distinct solutions of equation $bx^2 + abx + a = 0$, or equivalently

$$\Big((\beta + 1)^{-1} + (\beta + a)^{-1}\Big)x^2 + \Big(a(\beta + 1)^{-1} + a(\beta + a)^{-1}\Big)x + a = 0 \tag{13}$$

are x'_a and x''_a. There are 3 cases: 1) $x'_a, x''_a \in U$, 2) $x'_a, x''_a \notin U$ and 3) $x'_a \in U, x''_a \notin U$ or $x''_a \in U, x'_a \notin U$. Suppose that cases 1), 2) and 3) occur t_1, t_2 and t_3 times respectively with a ranging through T_β. Straightforwardly, $t_1 + t_2 + t_3 = |T_\beta|$. It further follows from Lemma 11 that, if we let $x = x'_a$ or $x = x''_a$ in (13), there are at most two $a \in T_\beta$ such that Equation (13) holds. This means that every element of U as the solutions of (13) appears at most two times when a runs through T_β. So we have $2t_1 + t_3 \leq 2|U|$ and hence $t_2 = |T_\beta| - (t_1 + t_3) \geq |T_\beta| - (2t_1 + t_3) \geq |T_\beta| - 2|U|$.

Denote by S_β the subset of T_β such that Equation (2) has two distinct solutions. We then have $|S_\beta| = t_2 \geq 2^{n-1} - 2^{n/2} - 2|U| - 3$. Define $S'_\beta = \{a \in S_\beta \,|\, \beta + a \notin U\}$ whose size is at least $2^{n-1} - 2^{n/2} - 3|U| - 3$. By the definition of S'_β and $\beta \in U$, β and $\beta + a$ are

respectively solutions of (4) and (5) for any $a \in S'_\beta$. Note that $\beta \neq \beta + a$ for every $a \in T_\beta$ due to $a \neq 1$. Note also that neither β nor $\beta + a$ are solutions of (2) due to $\beta \in U$. In other words, for any $a \in S'_\beta$, the four elements β, $\beta + a$, x'_a and x''_a are distinct. Therefore, given an element $\beta \in U$, for all $a \in S'_\beta$ and $b = (\beta+1)^{-1} + (\beta+a)^{-1} \neq 0$ we have $\delta_F(a,b) = 4$ in this case.

Next we bound from below the total number of pairs $(a,b) = (a, (\beta+1)^{-1} + (\beta+a)^{-1})$ such that $\delta_F(a,b) = 4$ when β runs through U. For any two distinct elements $\beta_1, \beta_2 \in U$, we define $B_i = \{(a,b) \,|\, a \in S'_{\beta_i}, b = (\beta_i+1)^{-1} + (\beta_i+a)^{-1}\}$ for $i = 1, 2$. We now prove that the intersection of B_1 and B_2 is empty. Assume that B_1 and B_2 have a common element (a,b). According to the definitions of S'_{β_1} and S'_{β_2}, β_1, β_2 (resp. $\beta_1 + a, \beta_2 + a$) are two distinct solutions of (4) and (5), $\beta_1 \neq \beta_2 + a$ and $\beta_2 \neq \beta_1 + a$ because of $\beta_1, \beta_2 \in U$. Moreover, $\beta_1 \neq \beta_1 + a$ and $\beta_2 \neq \beta_2 + a$ because of $a \neq 0$. Hence, $\beta_1, \beta_2, \beta_1 + a + 1$ and $\beta_2 + a + 1$ are four distinct solutions of Equation (6). Since $\beta_1, \beta_2 \in U$ and $\beta_1 + a, \beta_2 + a \notin U$, none of them is a solutions of (2). By the definitions of S'_{β_1} and S'_{β_2}, Equation (2) has two distinct solutions x'_a and x''_a. That is to say, the six elements $\beta_1, \beta_2, \beta_1 + a, \beta_2 + a, x'_a, x''_a$ are distinct, a contradiction to the fact that F is differentially 4-uniform. Then, for any two distinct elements $\beta_1, \beta_2 \in U$, sets B_1 and B_2 have no common element. Thus, there are at least $\sum_{\beta \in U} |S'_\beta| \geq (2^{n-1} - 2^{n/2} - 3|U| - 3)|U|$ pairs (a,b) with $ab \neq 1$ such that $\delta_F(a,b) = 4$ when β runs through U in this case.

From above discussion, there are at least $\big(2^n - 1 - 3|U|\big)$ pairs (a,b) with $ab = 1$ such that $\delta_F(a,b) = 4$ by Case 1 and there are at least $(2^{n-1} - 2^{n/2} - 3|U| - 3)|U|$ pairs (a,b) with $ab \neq 1$ such that $\delta_F(a,b) = 4$ by Cases 2. We then have $\big(2^n - 1 - 3|U|\big) + \big(2^{n-1} - 2^{n/2} - 3|U| - 3\big)|U| > 2^n - 1$, i.e., $\big(2^{n-1} - 2^{n/2} - 3|U| - 6\big)|U| > 0$ if and only if $0 < |U| < \frac{2^{n-1} - 2^{n/2}}{3} - 2$. This completes the proof. □

Theorem 8. *For every even $n \geq 6$, the functions F are CCZ-inequivalent to the Gold functions, the Kasami functions, the functions discussed in [2] and quadratic functions.*

Proof. By Lemma 9, 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 that F is CCZ-inequivalent to those functions, it is sufficient to prove that F has different extended Walsh spectrum compared to theirs. Note that, for any $(a,b) \in F_{2^n}^* \times \mathbb{F}_{2^n}$,

we get

$$\begin{aligned} & W_F(a,b) \\ = & \sum_{x\in\mathbb{F}_{2^n}\setminus U}(-1)^{tr_1^n(ax^{-1}+bx)}+\sum_{x\in U}(-1)^{tr_1^n(a(x+1)^{-1}+bx)} \\ = & \sum_{x\in\mathbb{F}_{2^n}\setminus U}(-1)^{tr_1^n(ax^{-1}+bx)}+\sum_{x\in U}(-1)^{tr_1^n(ax^{-1}+b(x+1))} \end{aligned}$$

where in the last identity we make use of the fact that U is stable with respect to the addition by 1. Then, $W_F(a,b)=W_I(a,b)$ when $tr_1^n(b)=0$. Let b_0 be a nonzero element of $\mathbb{F}_{2^n}^*$ with $tr_1^n(b_0)=0$. Thus, we have $W_F(a,b_0)=W_I(a,b_0)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(ax^{-1}+b_0x)}=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(x^{-1}+ab_0x)}=W_I(1,ab_0)$ for any $a\in\mathbb{F}_{2^n}^*$. Note that ab_0 can runs through $\mathbb{F}_{2^n}^*$ when a runs through $\mathbb{F}_{2^n}^*$ and $W_I(1,0)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n(x^{-1})}=0$. Therefore, it follows from Lemma 4 that the extended Walsh spectrum of F includes any value divisible by 4 in the range $[-2^{n/2+1}+1,2^{n/2+1}+1]$. That is, the extended Walsh spectrum of F is different from that of the Gold functions, the Kasami functions, the functions discussed in [2] and quadratic functions, and then functions F are CCZ-inequivalent to them. This completes the proof. □

By Theorems 7 and 8, we directly get the following corollary.

Corollary 4. *For every even $n\geq 6$, F is CCZ-inequivalent to all known differentially 4-uniform power functions and to quadratic functions when the set U is such that $0<|U|<\frac{2^{n-1}-2^{n/2}}{3}-2$.*

Remark 2. *This is the first time mathematically prove that an infinite class of differentially 4-uniform functions is CCZ-inequivalent to all known differentially 4-uniform power functions and to quadratic functions.*

For $n=6$, by a Magma program, we checked that there are 14 elements of $\mathbb{F}_{2^6}$ such that $tr_1^n(x^{-1})=tr_1^n((x+1)^{-1})=1$. So there are $2^7=128$ different sets U. With the help of computer, we can obtain all differentially 4-uniform bijections generated by Construction 1. There exist at least 22 classes of differentially 4-uniform bijections according to nonlinearity and differential spectrum are CCZ-invariant parameters. We list them in Table 3, in which $D_t=|\{(a,b)\,|\,\delta_F(a,b)=t\}|$, and α is the default primitive element of $\mathbb{F}_{2^6}$ in Magma version 2.12-16. We also checked that these 22 classes of differentially 4-uniform bijections are CCZ-inequivalent to the two classes of functions $x^{-1}+tr_1^n(x^2(x+1)^{-1})$ and $x^{-1}+tr\big(x^{-d}+(x^{-1}+1)^d\big)$ where $d=3(2^t+1)$ and $2\leq t\leq n/2-1$ presented in [14].

We shall now prove that F with $U=U_{m_0}$ and $U=U_{m_1}$ are CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions. For doing this, we first need two upper bounds on the sizes of U_{m_0} and U_{m_1} respectively.

Table 3: The classes of differentially 4-uniform bijections for $n = 6$

U	nl	(D_0,D_2,D_4)
$\{\alpha^i \mid i \in \{21, 42\}\}$	22	(2127,1794,111)
$\{\alpha^i \mid i \in \{5, 30\}\}$	22	(2139,1770,123)
$\{\alpha^i \mid i \in \{20, 40, 57, 51\}\}$	22	(2181, 1686, 165)
$\{\alpha^i \mid i \in \{21, 40, 42, 51\}\}$	20	(2181, 1686, 165)
$\{\alpha^i \mid i \in \{5, 17, 30, 39\}\}$	20	(2187, 1674, 171)
$\{\alpha^i \mid i \in \{5, 10, 15, 30, 60, 34\}\}$	20	(2211, 1626, 195)
$\{\alpha^i \mid i \in \{5, 10, 21, 30, 60, 42\}\}$	20	(2217, 1614, 201)
$\{\alpha^i \mid i \in \{5, 21, 40, 30, 42, 51\}\}$	18	(2217, 1614, 201)
$\{\alpha^i \mid i \in \{5, 10, 17, 30, 60, 39\}\}$	20	(2223, 1602, 207)
$\{\alpha^i \mid i \in \{5, 10, 15, 17, 30, 60, 34, 39\}\}$	20	(2235, 1578, 219)
$\{\alpha^i \mid i \in \{10, 15, 20, 40, 60, 34, 57, 51\}\}$	20	(2241, 1566, 225)
$\{\alpha^i \mid i \in \{5, 10, 15, 21, 30, 60, 34, 42\}\}$	18	(2241, 1566, 225)
$\{\alpha^i \mid i \in \{5, 10, 17, 40, 30, 60, 39, 51\}\}$	20	(2247, 1554, 231,)
$\{\alpha^i \mid i \in \{5, 17, 20, 21, 30, 39, 57, 42\}\}$	20	(2253, 1542, 237)
$\{\alpha^i \mid i \in \{5, 20, 21, 40, 30, 57, 42, 51\}\}$	18	(2253, 1542, 237)
$\{\alpha^i \mid i \in \{5, 10, 15, 17, 20, 30, 60, 34, 39, 57\}\}$	20	(2259, 1530, 243)
$\{\alpha^i \mid i \in \{5, 10, 15, 17, 21, 30, 60, 34, 39, 42\}\}$	18	(2259, 1530, 243)
$\{\alpha^i \mid i \in \{5, 10, 15, 21, 40, 30, 60, 34, 42, 51\}\}$	18	(2265, 1518, 249)
$\{\alpha^i \mid i \in \{5, 10, 17, 21, 40, 30, 60, 39, 42, 51\}\}$	18	(2271, 1506, 255)
$\{\alpha^i \mid i \in \{5, 10, 15, 17, 20, 40, 30, 60, 34, 39, 57, 51\}\}$	22	(2277, 1494, 261)
$\{\alpha^i \mid i \in \{5, 10, 15, 17, 21, 40, 30, 60, 34, 39, 42, 51\}\}$	18	(2277, 1494, 261)
$\{\alpha^i \mid i \in \{5, 10, 15, 17, 20, 21, 40, 30, 60, 34, 39, 57, 42, 51\}\}$	20	(2289, 1470, 273)

Lemma 12. *For every even $n \geq 6$, we have $2^{n-3} - 7 \cdot 2^{n/2-2} \leq |U_{m_0}| \leq 2^{n-3} + 7 \cdot 2^{n/2-2}$ and $2^{n-3} - 5 \cdot 2^{n/2-2} \leq |U_{m_1}| \leq 2^{n-3} + 5 \cdot 2^{n/2-2}$.*

This lemma will be proved in Appendix.

We can easily deduce that $2^{n-3} + 7 \cdot 2^{n/2-2} < (2^{n-1} - 2^{n/2})/3 - 2$ when $n \geq 12$. Hence, By Lemma 12 and Theorem 7, we directly obtain the following theorem.

Theorem 9. *For even $n \geq 12$. F with $U = U_{m_0}$ and $U = U_{m_1}$ are CCZ-inequivalent to known differential 4-uniformity power functions and to quadratic functions.*

5 Comparison of the nonlinearity with that of all known differentially 4-uniform bijections

In this section, we compare our lower bounds and the actual values on the nonlinearity of F to that of all known differentially 4-uniform bijections.

We first compare our lower bounds and the actual values on the nonlinearity of F to that of known differentially 4-uniform non-power bijections. In [14], two infinite classes of differentially 4-uniform bijections were proposed. They are of the form $x^{-1}+tr_1^n(x^2(x+1)^{-1})$ and $x^{-1} + tr\big(x^{-d} + (x^{-1}+1)^d\big)$ where $d = 3(2^t+1)$ and $2 \leq t \leq n/2-1$. To the best of our

knowledge, this was the first time an infinite family of non-power differentially 4-uniform bijections was found in even dimension. For convenience, we denote these two classes of functions by Q_1 and Q_2 respectively. For a given infinite class of functions, let us denote by $\mathcal{NL}$ the best known lower bound on their nonlinearity and by NL the actual value of their nonlinearity. We list in Table 4 below, for even numbers of variables ranging from 6 to 12, the concrete values of $\mathcal{NL}$ and NL of our functions and of the functions Q_1 and Q_2 (we list the values of NL corresponding to the parameter t from 2 to $n/2-1$ in one cell). We can see from Tables 1 and 4 that although the lower bounds on the nonlinearity of F with $U = U_{\max}$, $U = U_{m_0}$ and $U = U_{m_1}$ are a little less than that of the function Q_1, the actual value of the nonlinearity is very close to that of function Q_1, and that our three lower bounds are much better than those for function Q_2. Particularly, the lower bound on the nonlinearity of F given in Theorem 3 is better than the actual nonlinearities of Q_1 and Q_2 when we take $|U| < 10$ for $n = 8$, $|U| < 26$ for $n = 10$ and $|U| < 56$ for $n = 12$.

We now compare our lower bounds and the actual values on the nonlinearity of F to those of known differentially 4-uniform bijections. Recall that all known differentially 4-uniform power bijections have exact nonlinearity $2^{n-1} - 2^{n/2}$ which is equal to the best known nonlinearity. We can see from Table 1 that all our lower bounds on nonlinearity of F are strictly less than that those for the differentially 4-uniform power bijections. But by Theorem 3, the nonlinearity of our functions can be very close to $2^{n-1} - 2^{n/2}$ when we restrict the size of U to a very small value (e.g. $|U| = 2$). More interestingly, we can see from Table 1 that the lower bounds on the nonlinearity of F with $U = U_{\max}$, $U = U_{m_0}$ and $U = U_{m_1}$ are not much less than $2^{n-1} - 2^{n/2}$ and we can see from Table 4 that the actual values on the nonlinearity of F with those sets are better than their lower bounds.

Obviously, the lower bound given in Theorem 3 is not tight, we give some examples for $n = 8$ below to show that Construction 1 can generate bijections with actual nonlinearity larger than those of Q_1 and Q_2 and very close to $2^{n-1} - 2^{n/2} = 112$ when the size of U is greater than 10.

Example 1. *For $n = 8$, let α be the default primitive element of $\mathbb{F}_{2^8}$ in Magma version 2.12-16.*

- *If $U = \{\alpha^i \mid i \in \{11, 22, 44, 88, 95, 97, 125, 133, 175, 176, 190, 194, 215, 235, 245, 250, 138, 42, 162, 168\}\}$, we have the size of U is 20 and $NL(F) = 106$.*
- *If $U = \{\alpha^i \mid i \in \{5, 10, 11, 20, 21, 22, 40, 42, 44, 65, 69, 80, 81, 84, 88, 95, 97, 111, 123, 125, 130, 133, 138, 160, 162, 168, 175, 176, 183, 189, 190, 194, 215, 219, 222, 235, 237, 245, 246, 250, 186, 174, 167, 158, 122, 211, 233, 244\}\}$, we have the size of U is 48 and $NL(F) = 104$.*

Table 4: Comparison of the lower bound and actual values on nonlinearity

n	Our functions F						Functions in [14]				Known maximal NL on n-dimensional bijections
	$U = U_{\max}$		$U = U_{m_0}$		$U = U_{m_1}$		Q_1		Q_2		
	$\mathcal{NL}$	NL	$\mathcal{NL}$	NL	$\mathcal{NL}$	NL	$\mathcal{NL}$	NL	$\mathcal{NL}$	NL	
6	6	20	-2	22	-2	22	14	20	12	22	24
8	78	100	62	102	62	102	94	102	56	98,100	112
10	414	442	382	450	382	444	446	454	240	446,448,440	480
12	1854	1902	1790	1924	1790	1892	1918	1928	992	1884,1890,1898,1900	1984

6 Conclusion

For any even $n \geq 6$, a construction of differentially 4-uniform bijections on $\mathbb{F}_{2^n}$ are proposed in this paper. We deduced a lower bound on the nonlinearity for our functions which is very high in some cases and three improved lower bounds on the nonlinearity for three special subcases. Compared to all known differentially 4-uniform functions, the lower bounds on the nonlinearity of our functions are sometimes very close to the best known ones. The constructed functions have maximum algebraic degree and are CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions in some cases. This is the first time that is mathematically proved that an infinite class of differentially 4-uniform bijections contains functions CCZ-inequivalent to known differentially 4-uniform power functions and to quadratic functions.

Appendix:

***Proof of Lemma 3*:** For every $a \in \mathbb{F}_{2^n}$, if $x \neq 0$ and $x \neq a$, Equation (2) is equivalent to the equation:

$$bx^2 + abx + a = 0, \quad x, x + a \in \mathbb{F}_{2^n} \setminus U, \tag{14}$$

if $x \neq 1$ and $x \neq a + 1$, Equation (3) is equivalent to the equation:

$$bx^2 + abx + ab + a + b = 0, \quad x, x + a \in U, \tag{15}$$

if $x \neq 1$ and $x \neq a$, Equation (4) is equivalent to the equation:

$$bx^2 + b(a + 1)x + ab + a + 1 = 0, \quad x \in U, x + a \in \mathbb{F}_{2^n} \setminus U, \tag{16}$$

and if $x \neq 0$ and $x \neq a + 1$, Equation (5) is equivalent to the equation:

$$bx^2 + b(a + 1)x + a + 1 = 0, \quad x \in \mathbb{F}_{2^n} \setminus U, x + a \in U. \tag{17}$$

Note that the root λ of the equation $bx^2+abx+a = 0$, if exist, is one-to-one corresponding to the root $\lambda + 1$ of the equation $bx^2 + abx + ab + a + b = 0$ plus 1. Since U is stable under

the addition by 1, equations (14) and (15) cannot have solutions simultaneously. Therefore, the sum of the numbers of solutions of (14) and (15) is at most 2.

Similarly, the sums of the roots in the equations $bx^2 + b(a+1)x + ab + a + 1 = 0$ and $bx^2 + b(a+1)x + a + 1 = 0$ both equal $a+1$. If γ is a solution of (16), then $\gamma + a + 1$ is not a solution of (16) because of $\gamma + a \in \mathbb{F}_{2^n} \setminus U$; and so does for the solution γ of (17). That is, each equation has at most one solution. Then, the sum of the numbers of solutions of (16) and (17) is at most 2.

1) Note that $0, 1 \notin U$ since $tr_1^n(1) = 0$. Clearly, $x = 1, a+1$ do not satisfy $x, x+a \in U$, which indicate that Equation (3) has the same solutions as Equation (15). Recall that the sum of the numbers of solutions of (14) and (15) is at most 2. Then, the sum of the numbers of solutions of (2) and (3) is at most 4 since in contrast to Equation (14), Equation (2) may have two more solutions $x = 0, a$.

   1.1) If $ab \neq 1$, obviously $0, a$ are not solutions of (2). Thus, the sum of the numbers of solutions of (2) and (3) is at most 2.

   1.2) If $a \in U$ and $b(a+1) = 1$, we have again $ab \neq 1$ since $b \neq 0$. Thus, equations (2) and (3) are equivalent to (14) and (15), respectively. By dividing ab in $b(a+1) = 1$, we have $1 + a^{-1} = (ab)^{-1}$ and hence $tr_1^n((ab)^{-1}) = tr_1^n(1 + a^{-1}) = tr_1^n(a^{-1}) = 1$, which implies that (14) has no solution by Lemma 1. Moreover, by $b(a+1) = 1$, the equality (15) becomes $bx^2 + abx + a + 1 = 0$, which has no solution by Lemma 1 due to $tr_1^n(b(a+1)(ab)^{-2}) = tr_1^n((ab)^{-2}) = 1$. Therefore, (2) and (3) have no solution.

2) Since $1 \notin U$, we have that 1 and $a+1$ are not solutions of (4) and (5) respectively. Hence, the sum of the numbers of solutions of (4) and (5) is at most 4, which is at most 2 more than that of (16) and (17).

   2.1) If $b(a+1) \neq 1$ or $a \notin U$, clearly $1, a$ are not solutions of (4) and $0, a+1$ are not solutions of (5). Then equations (4) and (5) have the same solutions as equations (16) and (17). Hence, the sum of the numbers of solutions of (4) and (5) is at most 2, according to the observation above.

   2.2) If $ab = 1$, then we have $b(a+1) \neq 1$ since $b \neq 0$. It follows from above that equations (4) and (5) have the same solutions as equations (16) and (17). Assume that λ is a solution of (16), then $\lambda \in U$ and hence $tr_1^n(\lambda^{-1}) = 1$. Therefore, (16) has no solution, according to Lemma 2. Assume that γ is a solution of (17), then we have that $\gamma \notin U$ and $\gamma + a \in U$. It is easy to verify that $\gamma + a$ is a solution of (16), a contradiction. That is, (17) has no solution. Therefore, we deduce that both (16) and (17) have no solution.

Proof of Lemma 12: Define $A_0 = \{x \in \mathbb{F}_{2^n} \,|\, (tr_1^n(x), tr_1^n(x^{-1}), tr_1^n((1+x)^{-1})) = (1,0,0)\}$, $A_1 = \{x \in \mathbb{F}_{2^n} \,|\, (tr_1^n(x), tr_1^n(x^{-1}), tr_1^n((1+x)^{-1})) = (1,0,1)\}$, $A_2 = \{x \in$

$\mathbb{F}_{2^n} \,|\, (tr_1^n(x), tr_1^n(x^{-1}), tr_1^n((1+x)^{-1})) = (1,1,0)\}$ and $A_3 = \{x \in \mathbb{F}_{2^n} \,|\, (tr_1^n(x), tr_1^n(x^{-1}), tr_1^n((1+x)^{-1})) = (1,1,1)\}$. Obviously, $|U_{m_1}| = |A_3|$ according to (9), and $\sum_{i=0}^{4} |A_i| = 2^{n-1}$ due to $\mathrm{wt}(tr_1^n(x)) = 2^{n-1}$.

Note that $\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x+x^{-1}+(x+1)^{-1})} = 2^n - 2\mathrm{wt}(tr_1^n(x + x^{-1} + (x+1)^{-1})) = 2^n - 2\big(\mathrm{wt}(tr_1^n(x)) + \mathrm{wt}(tr_1^n(x^{-1} + (x+1)^{-1})) - 2|\{x \in \mathbb{F}_{2^n} \,|\, tr_1^n(x) = tr_1^n(x^{-1} + (x+1)^{-1}) = 1\}|\big) = -2\mathrm{wt}(tr_1^n(x^{-1} + (x+1)^{-1})) + 4(|A_1| + |A_2|)$. Then, $4(|A_1| + |A_2|) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x+x^{-1}+(x+1)^{-1})} + 2\mathrm{wt}(tr_1^n(x^{-1} + (x+1)^{-1}))$. Recall that in the proof of Corollary 2, we have already proven $|\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{-1}+(1+x)^{-1})}| \le 2^{n/2+1}$. Hence, we have then $2^n - 2^{n/2+1} \le 2\mathrm{wt}(tr_1^n(x^{-1} + (x+1)^{-1})) \le 2^n + 2^{n/2+1}$. Besides, by Corollary 1, $-2^{n/2+2} - 4 \le \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x+x^{-1}+(x+1)^{-1})} \le 2^{n/2+2} + 4$. Therefore,

$$2^{n-2} - 3\cdot 2^{n/2-1} - 1 \le |A_1| + |A_2| \le 2^{n-2} + 3\cdot 2^{n/2-1} + 1$$

by $\sum_{i=0}^{4} |A_i| = 2^{n-1}$ which gives

$$2^{n-2} - 3\cdot 2^{n/2-1} - 1 \le |A_0| + |A_3| \le 2^{n-2} + 3\cdot 2^{n/2-1} + 1 \tag{18}$$

Note that $\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=1} (-1)^{tr_1^n(x^{-1})} = \frac{1}{2}\big(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{-1})} - \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{-1}+x)}\big) = -\frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{-1}+x)}$ and $\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=1} (-1)^{tr_1^n(x^{-1})} = |A_0| + |A_1| - |A_2| - |A_3|$. Then, by Lemma 4, we have

$$-2^{n/2} \le |A_0| + |A_1| - |A_2| - |A_3| \le 2^{n/2} \tag{19}$$

Similarly, we have $\sum_{x\in\mathbb{F}_{2^n}, tr_1^n(x)=1} (-1)^{tr_1^n((x+1)^{-1})} = -\frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n((x+1)^{-1}+x)}$ and then

$$-2^{n/2} \le |A_0| + |A_2| - |A_1| - |A_3| \le 2^{n/2}. \tag{20}$$

Combining (18)-(20), we get $2^{n-3} - 5\cdot 2^{n/2-2} \le |A_3| \le 2^{n-3} + 5\cdot 2^{n/2-2}$, which implies $2^{n-3} - 5\cdot 2^{n/2-2} \le |U_{m_1}| \le 2^{n-3} + 5\cdot 2^{n/2-2}$. By $U_{\max} = U_{m_0} \cup U_{m_1}$ and $2^{n-2} - 2^{n/2-1} \le |U_{\max}| \le 2^{n-2} + 2^{n/2-1}$, we have $2^{n-3} - 7\cdot 2^{n/2-2} \le |U_{m_0}| \le 2^{n-3} + 7\cdot 2^{n/2-2}$, which completes the proof.

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] Budaghyan L., Carlet C., Pott A.: New Classes of Almost Bent and Almost Perfect Nonlinear Functions. IEEE Trans. Inf. Theory **52**(3), 1141-1152 (2006).

[5] Carlet C.: On Known and New Differentially Uniform Functions. In: Proc. Australasian Conf. Inf. Security Privacy. Lecture Notes in Computer Science, vol. 6812, pp. 1-15. Springer, Berlin (2011),

[6] Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.* **15**(2), 125-156 (1998).

[7] Edel Y., Pott A.: A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, **3**(1) 59-81 (2009).

[8] Knudsen L.: Truncated and Higher Order Differentials. In: Proc. 2nd Int. Workshop Fast Softw. Encrypt. Lecture Notes in Computer Science, vol. 1008, pp. 196-211. Springer, Berlin (1995).

[9] MacWilliams F.J., Sloane N.J.: The theory of error-correcting codes, Amsterdam, North Holland. 1977.

[10] Matsui M.: Linear Cryptanalysis Method for DES Cipher. In: Advances in Cryptology-EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765, pp. 386-397. Springer, Berlin (1994).

[11] Nyberg K.: Differentially uniform mappings for cryptography. In Advances in Cryptology-EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765, pp. 55-64. Springer, Berlin (1994).

[12] Shannon C.E.: Communication theory of secrecy systems. Bell system technical journal **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).