On permutation polynomials EA-equivalent to the inverse function over GF(2^n)

Yongqiang Li[1,2] and Mingsheng Wang[1]

1. The State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
2. Graduate School of Chinese Academy of Sciences, Beijing 100190, China
liyongqiang@is.iscas.ac.cn
mingsheng_wang@yahoo.com.cn

Abstract. It is proved that there does not exist a linearized polynomial $L(x) \in \mathbb{F}_{2^n}[x]$ such that $x^{-1} + L(x)$ is a permutation on $\mathbb{F}_{2^n}$ when $n \geq 5$, which is proposed as a conjecture in [15]. As a consequence, a permutation is EA-equivalent to the inverse function over $\mathbb{F}_{2^n}$ if and only if it is affine equivalent to it when $n \geq 5$.

Key words: Inverse function, EA-equivalence, Permutation polynomial, S-box, Kloosterman sums

1 Introduction

Permutation polynomials over finite fields play an important role in cryptography, especially in block ciphers they are often used as substitution boxes (S-boxes) of block ciphers. A function $F(x)$ from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$ is called differentially δ-uniform if for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, $F(x) + F(x + a) = b$ has at most δ solutions [18]. The functions with differentially 2-uniform are said to be almost perfect nonlinear (APN). APN functions provide the best resistance to differential attack [3]. Much work has been done on APN functions, see [1,4,5,6,11].

For efficiency of software and hardware implementations, an S-box is often designed as a permutation over $\mathbb{F}_{2^{2n}}$ in practice. However the existence of APN permutations on $\mathbb{F}_{2^{2n}}$ is a major open problem in the study of vectorial boolean functions. The main results concerning this problem are that there are no APN permutations over $\mathbb{F}_{2^4}$ and there are no APN permutations over $\mathbb{F}_{2^{2n}}$ with coefficients in $\mathbb{F}_{2^n}$ [13]. A breakthrough of this problem is that Dillon found a first APN permutation on $\mathbb{F}_{2^6}$, which is CCZ-equivalent to the Kim map [9]. The existence of APN permutations on $\mathbb{F}_{2^{2n}}, n \geq 4$ remains open.

Therefore, it is optimal to choose differentially 4-uniform permutations as S-boxes of block ciphers in real applications. The most famous differentially 4-uniform permutation is the inverse function over $\mathbb{F}_{2^{2n}}$ [2,18], which also has the highest known nonlinearity on $\mathbb{F}_{2^{2n}}$ [14]. Based on these reasons, it is appropriate to choose the permutation polynomials affine or extend affine (EA) equivalent to the inverse function on $\mathbb{F}_{2^{2n}}$ as the S-boxes of block ciphers. For example, the S-box of AES is affine equivalent to the inverse function over $\mathbb{F}_{2^8}$.

Recall that two functions $F_1(x)$ and $F_2(x)$ over $\mathbb{F}_{2^n}$ are called EA-equivalent if there exist affine permutations $A_1(x), A_2(x) \in \mathbb{F}_{2^n}[x]$ and an affine polynomial $A(x) \in \mathbb{F}_{2^n}[x]$ such that $F_1(x) = A_1(F_2(A_2(x))) + A(x)$ [5,18]. When $A(x) = 0$, $F_1(x)$ and $F_2(x)$ are said to be affine equivalent. Let $S_A(F)$ and $S_E(F)$ be the sets of functions over $\mathbb{F}_{2^n}$ which are affine and EA-equivalent to $F(x)$ respectively. Then it is easy to see that $S_A(F) \subsetneq S_E(F)$. Since in most cases an S-box is a permutation on $\mathbb{F}_{2^n}$, it is interesting to know whether or not $SP_A(F) \subsetneq SP_E(F)$, where $SP_A(F)$ and $SP_E(F)$ are the sets of permutation polynomials on $\mathbb{F}_{2^n}$ which are affine and EA-equivalent to $F(x)$ respectively.

Investigating this problem means that we have to characterize the existence of permutation polynomials EA-equivalent and affine inequivalent to $F(x)$. Notice that if a permutation on $\mathbb{F}_{2^n}$ is EA-equivalent and affine inequivalent to $F(x)$, then there exists a nontrivial linearized polynomial $L(x) \in \mathbb{F}_{2^n}[x]$ such that $F(x) + L(x)$ is a permutation on $\mathbb{F}_{2^n}$. For $F(x) = x^d$ with $\gcd(d, 2^n - 1) > 1$, some work have been done concerning the existence of permutation polynomials of the type $x^d + L(x)$, see [15,19,20]. For the inverse mapping over $\mathbb{F}_{2^n}$, let us recall the following conjecture raised in [15].

Conjecture 1. There does not exist a linearized polynomial $L(x) \in \mathbb{F}_{2^n}[x]$ such that $x^{-1} + L(x)$ is a permutation on $\mathbb{F}_{2^n}$ when $n \geq 5$.

In [15], some elementary simulation results are given to support Conjecture 1. The present paper attempts to give further study on this conjecture because of the importance of x^{-1} in cryptography. Making use of results from Kloosterman sums over a finite field, one can characterize the existence of permutation polynomials of the form $x^{-1} + L(x)$, which leads to a complete solution of conjecture 1.

The paper is organized as follows. In Sect. 2, some preliminary results are introduced that will be used throughout the paper. The proof of the conjecture 1 is provided in Sect. 3. The conclusion is given in Sect. 4.

2 Preliminaries

Let n be a positive integer and $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. Tr denotes the absolute trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

In this section, let us recall some known results that will be used in this paper. First, we introduce the definition of Kloosterman sums. For any $a \in \mathbb{F}_{2^n}$, the classical Kloosterman sum $K(a)$ over $\mathbb{F}_{2^n}$ is defined as $K(a) = \sum\limits_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)}$. The complete Kloosterman sum $\mathcal{K}(a)$ is defined as $\mathcal{K}(a) = K(a) + 1$, or equivalently

$$\mathcal{K}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(x^{-1}+ax)}.$$

The set of values of $\mathcal{K}(a)$ is $\{k \in \mathbb{Z} \mid k \equiv 0 \bmod 4, k \in [-2^{\frac{n}{2}+1} + 1, 2^{\frac{n}{2}+1} + 1]\}$[14]. Some properties of boolean functions are related to the complete Kloosterman sums, such as for $\lambda \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}(\lambda x^{2^m-1})$ is a bent function on $\mathbb{F}_{2^{2m}}$

if and only if the complete Kloosterman sum of λ over $\mathbb{F}_{2^m}$ equals zero, i.e. $\sum\limits_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}(x^{-1}+\lambda x)}=0$ [10,8]. Characterizing the set of those $\lambda\in\mathbb{F}_{2^n}$ with $\mathcal{K}(\lambda)=0$ is raised as an open problem in [8]. The complete kloosterman sums are also powerful for us to characterize the permutation polynomials of the type $x^{-1}+L(x)$ over $\mathbb{F}_{2^n}$, especially we need the following results.

Lemma 1. *[12,7,17] Let $n\geq 3$. For any $a\in\mathbb{F}_{2^n}$, $\mathcal{K}(a)\equiv 0 \mod 8$ if $\mathrm{Tr}(a)=0$ and $\mathcal{K}(a)\equiv 4 \mod 8$ if $\mathrm{Tr}(a)=1$.*

Lemma 2. *[17] Let $n\geq 4$. For any $a\in\mathbb{F}_{2^n}$, $\mathcal{K}(a)$ is divisible by 16 if and only if $\mathrm{Tr}(a)=0$ and $\mathrm{Tr}(y)=0$, where $y^2+ay+a^3=0$.*

The following results are from [15].

Theorem 1. *Let $n\geq 3$, and $L(x)=\sum\limits_{i=0}^{n-1}c_ix^{2^i}\in\mathbb{F}_{2^n}[x]$ be a linearized polynomial. If for some $1\leq k\leq n-1$, $c_{n-k}+c_k^{2^{n-k}}\neq 0$, then $x^{-1}+L(x)$ is not a permutation polynomial on $\mathbb{F}_{2^n}$.*

Example 1. $x^{-1}+\alpha x^{2^i}$ is not a permutation on $\mathbb{F}_{2^n}$ for $\alpha\in\mathbb{F}_{2^n}^*$ and i with $0\leq i\leq n-1$.

At last, let us recall Hermite's criterion, which is often used for determining whether a polynomial is a permutation over finite fields.

Lemma 3 (Hermite's Criterion). *[16] Let $\mathbb{F}_q$ be of characteristic p. Then $f\in\mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

1. *f has exactly one root on $\mathbb{F}_q$;*
2. *for each integer t with $1\leq t\leq q-2$ and $t\not\equiv 0 \mod p$, the reduction of*

$$f(x)^t \mod (x^q-x)$$

has degree $\leq q-2$.

3 Permutation polynomials of the type $x^{-1}+L(x)$

Throughout this section, for an integer $i\in\mathbb{Z}$, c_i means $c_{i'}$, where $i'\in\{0,1,\ldots,n-1\}$ with $i'\equiv i \bmod n$. In particular, $c_n=c_0$. Moreover, $L(x)\in\mathbb{F}_{2^n}[x]$ always denotes a nontrivial linearized polynomial, and for $t\in\mathbb{N}$, $\omega_2(t)$ denotes the number of nonzero terms in the binary expansion of t. We shall first prove the following lemma that will be used in the subsequent discussions of this paper.

Lemma 4. *Let $n\geq 4$, and $L(x)=\sum\limits_{i=0}^{n-1}c_ix^{2^i}\in\mathbb{F}_{2^n}[x]$ be a linearized polynomial. If $x^{-1}+L(x)$ is a permutation on $\mathbb{F}_{2^n}$, then for any $1\leq i<j\leq n-1$, we have $c_{i+1}c_{j+1}+c_{j-i+1}^{2^i}c_{i-1}^2+c_{j-i-1}^{2^{i+1}}c_{j-1}^2=0$.*

Proof. Suppose $x^{-1}+L(x)$ is a permutation on $\mathbb{F}_{2^n}$. For $1\le i<j\le n-1$, we have $1\le 2^i+2^j+1\le 2^n-2$ because of $n\ge 4$, and

$$\begin{aligned}&(x^{-1}+L(x))^{2^i+2^j+1}\\&=x^{-(2^i+2^j+1)}+x^{-2^i}L(x)^{2^j+1}+x^{-2^j}L(x)^{2^i+1}+x^{-1}L(x)^{2^i+2^j}\\&+x^{-(2^i+2^j)}L(x)+x^{-(2^i+1)}L(x)^{2^j}+x^{-(2^j+1)}L(x)^{2^i}+L(x)^{2^i+2^j+1}.\end{aligned}$$

It is easy to check that for $0\le k_1\ne k_2\le n-1$,

$$\begin{aligned}L(x)^{2^{k_1}+2^{k_2}}&=(\sum_{l=0}^{n-1}c_l^{2^{k_1}}x^{2^{l+k_1}})(\sum_{l=0}^{n-1}c_l^{2^{k_2}}x^{2^{l+k_2}})\\&=\sum_{l_1=0}^{n-1}\sum_{l_2=0}^{n-1}c_{l_1}^{2^{k_1}}c_{l_2}^{2^{k_2}}x^{2^{l_1+k_1}+2^{l_2+k_2}}.\end{aligned}$$

Now x^{2^n-1} is one of the terms of $x^{-2^k}L(x)^{2^{k_1}+2^{k_2}} \bmod (x^{2^n}+x)$ if and only if $2^k\equiv(2^{l_1+k_1}+2^{l_2+k_2}) \bmod (2^n-1)$ for some $0\le l_1,l_2\le n-1$, which is equivalent to

$$\begin{cases}l_1+k_1\equiv k-1 \bmod n\\ l_2+k_2\equiv k-1 \bmod n.\end{cases}$$

Thus $l_1\equiv k-k_1-1 \bmod n, l_2\equiv k-k_2-1 \bmod n$. Hence using the convention of notation in the beginning of this section, the coefficient of x^{2^n-1} in

$$x^{-2^k}L(x)^{2^{k_1}+2^{k_2}} \bmod (x^{2^n}+x)$$

is $c_{k-k_1-1}^{2^{k_1}}c_{k-k_2-1}^{2^{k_2}}$.

On the other hand, $x^{2^n-1}$is one of the terms of $x^{-(2^{k_1}+2^{k_2})}L(x)^{2^k} \bmod (x^{2^n}+x)$ if and only if for some $0\le i\le n-1$, $2^i\equiv 2^{k_1}+2^{k_2} \bmod (2^n-1)$. When $0\le k_1\ne k_2\le n-1$, there are no $0\le i\le n-1$ satisfied the above formula since $\omega_2(2^{k_1}+2^{k_2} \bmod (2^n-1))=2$. Then x^{2^n-1} is not a term of $x^{-(2^{k_1}+2^{k_2})}L(x)^{2^k} \bmod (x^{2^n}+x)$.

Also, the algebraic degree of the terms of $L(x)^{2^{k_1}+2^{k_2}+1}$ is at most 3 and $\omega_2(2^n-1)=n\ge 4$, hence x^{2^n-1} is not one of the terms of $L(x)^{2^{k_1}+2^{k_2}+1} \bmod (x^{2^n}+x)$.

Thus the coefficient of x^{2^n-1} in $(x^{-1}+L(x))^{2^i+2^j+1} \bmod (x^{2^n}+x)$ is

$$c_{i-j-1}^{2^j}c_{i-1}+c_{j-i-1}^{2^i}c_{j-1}+c_{-i-1}^{2^i}c_{-j-1}^{2^j},$$

which equal to zero by Hermite's criterion. By Theorem 1, $c_{n-k}=c_k^{2^{n-k}}$ for $1\le k\le n-1$. Remember $c_0=c_n$, then for any $0\le k\le n$, $c_{n-k}=c_k^{2^{n-k}}$. Hence we have

$$\begin{aligned}0&=c_{i-j-1}^{2^j}c_{i-1}+c_{j-i-1}^{2^i}c_{j-1}+c_{-i-1}^{2^i}c_{-j-1}^{2^j}\\&=c_{j-i+1}^{2^{i-1}}c_{i-1}+c_{j-i-1}^{2^i}c_{j-1}+c_{i+1}^{2^{n-1}}c_{j+1}^{2^{n-1}}.\end{aligned}$$

The proof is finished by squaring the above formula. □

By Lemma 4, it is possible to get more relations among coefficients of $L(x)$ when $L(x)$ is a linearized polynomial and $x^{-1}+L(x)$ is a permutation on $\mathbb{F}_{2^n}$. Some useful relations are given as follows.

Corollary 1. *Let $n \geq 4$ and $L(x)=\sum\limits_{i=0}^{n-1} c_i x^{2^i} \in \mathbb{F}_{2^n}[x]$ be a linearized polynomial. Assume that $x^{-1}+L(x)$ is a permutation on $\mathbb{F}_{2^n}$. Then the following statements hold.*

(1) For any $2 \leq k \leq n-2$, $c_k c_{k+2} + c_3^{2^{k-1}} c_{k-2}^2 + c_1^{2^k} c_k^2 = 0$.
(2) For any $2 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$, $c_{k+2} c_{2k+1} + c_k^{2^{k+1}+2} + c_{k-2}^{2^{k+2}} c_{2k-1}^2 = 0$.

Proof. By Lemma 4, setting $i=k-1, j=k+1$, we get (1); Similarly, by setting $i=k+1, j=2k$, (2) is obtained. The corresponding boundary of k is deduced from the inequality $1 \leq i < j \leq n-1$. □

By means of Lemma 4, we can obtain many relations about the coefficients of $L(x)$. But it is not enough to give complete solution to Conjecture 1. However, results on the Kloosterman sums can be used to prove that certain coefficients of $L(x)$ are zero when $x^{-1}+L(x)$ is permutation on $\mathbb{F}_{2^n}$. The following is such a result.

Lemma 5. *Let $n \geq 3$, and $L(x)=\sum\limits_{i=0}^{n-1} c_i x^{2^i} \in \mathbb{F}_{2^n}[x]$ be a linearized polynomial. If $x^{-1}+L(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$, then the following statements are true:*

(1) $\forall \alpha \in \mathbb{F}_{2^n}^*, \mathcal{K}(\alpha L(\alpha))=0$;
(2) $\forall x \in \mathbb{F}_{2^n}$, $\mathrm{Tr}(xL(x))=0$;
(3) $c_0=0$.

Proof. (1) Suppose $x^{-1}+L(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$. Then for any $\alpha \in \mathbb{F}_{2^n}^*$, $\mathrm{Tr}(\alpha(x^{-1}+L(x)))$ is a balanced boolean function, which implies that

$$\begin{aligned} 0 &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\alpha(x^{-1}+L(x)))} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(x^{-1}+\alpha L(\alpha x)))}. \end{aligned}$$

Since $x^{-1}+L(x)$ is a permutation, we have $c_{n-i}=c_i^{2^{n-i}}$ for all $0 \leq i \leq n-1$ (remember $c_n=c_0$). Thus $\forall x \in \mathbb{F}_{2^n}$, and $\forall \alpha \in \mathbb{F}_{2^n}^*$,

$$\begin{aligned} \mathrm{Tr}(\alpha L(\alpha x)) &= \mathrm{Tr}(\alpha \sum_{i=0}^{n-1} c_i (\alpha x)^{2^i}) \\ &= \sum_{i=0}^{n-1} \mathrm{Tr}(\alpha c_i (\alpha x)^{2^i}) \end{aligned}$$

$$\begin{aligned}
&= \sum_{i=0}^{n-1} \mathrm{Tr}((\alpha c_i(\alpha x)^{2^i})^{2^{n-i}}) \\
&= \sum_{i=0}^{n-1} \mathrm{Tr}(\alpha (c_i\alpha)^{2^{n-i}} x) \\
&= \mathrm{Tr}((\sum_{i=0}^{n-1} \alpha c_{n-i}\alpha^{2^{n-i}})x) \\
&= \mathrm{Tr}(\alpha L(\alpha) x).
\end{aligned}$$

Therefore, $\forall \alpha \in \mathbb{F}_{2^n}^*$, the complete Kloosterman sums $\mathcal{K}(\alpha L(\alpha)) = 0$, thus (1) is proved.

(2) Since $\mathcal{K}(\alpha L(\alpha)) = 0, \forall \alpha \in \mathbb{F}_{2^n}^*$, by Lemma 1, we have $\forall \alpha \in \mathbb{F}_{2^n}^*$,

$$\mathrm{Tr}(\alpha L(\alpha)) = 0.$$

Notice that 0 satisfies also the above formula, then $\mathrm{Tr}(xL(x)) = 0, \forall x \in \mathbb{F}_{2^n}$.

(3) When n is even, $\forall x \in \mathbb{F}_{2^n}$, we have:

$$\begin{aligned}
xL(x) &= c_0x^2 + \sum_{i=1}^{n-1} c_i x^{2^i+1} \\
&= c_0x^2 + \sum_{i=1}^{\frac{n}{2}-1} (c_i x^{2^i+1} + c_i^{2^{n-i}} x^{2^{n-i}+1}) + c_{2^{\frac{n}{2}}} x^{2^{\frac{n}{2}}+1} \\
&= c_0x^2 + \sum_{i=1}^{\frac{n}{2}-1} (c_i^{2^{n-i}} x^{2^{n-i}+1} + (c_i^{2^{n-i}} x^{2^{n-i}+1})^{2^i}) + c_{2^{\frac{n}{2}}} x^{2^{\frac{n}{2}}+1}.
\end{aligned}$$

Since $x^{-1} + L(x)$ is a permutation, then $c_{\frac{n}{2}} \in \mathbb{F}_{2^{\frac{n}{2}}}$ by Theorem 1. Also $\forall x \in \mathbb{F}_{2^n}$, $x^{2^{\frac{n}{2}}+1} \in \mathbb{F}_{2^{\frac{n}{2}}}$. So $\forall x \in \mathbb{F}_{2^n}$, $\mathrm{Tr}(c_{\frac{n}{2}} x^{2^{\frac{n}{2}}+1}) = 0$. Hence $0 = \mathrm{Tr}(xL(x)) = \mathrm{Tr}(c_0x^2), \forall x \in \mathbb{F}_{2^n}$, which implies $c_0 = 0$ when n is even.

Similarly, when n is odd, we still have $\mathrm{Tr}(xL(x)) = \mathrm{Tr}(c_0x^2)$, hence $c_0 = 0$. Then we complete the proof. □

The following proposition is needed in the proof of Lemma 7. In this proposition, $a + b$ always means $(a + b) \bmod (2^n - 1)$.

Proposition 1. *Let $n \geq 5$ and $S_k = \{(2^k + 1)2^i \ mod\ (2^n - 1) \mid 0 \leq i \leq n - 1\}$. Then the following statements hold.*

(1) For any $a, b \in \bigcup_{i=2}^{\lfloor \frac{n}{2} \rfloor} S_i$, $a + b \notin S_1$.

(2) Let $a = (2^k + 2^{k+1})\ mod\ (2^n - 1)$ for some $0 \leq k \leq n - 1$, $b \in \bigcup_{i=2}^{\lfloor \frac{n}{2} \rfloor} S_i$. Then $a + b \in S_1$ if and only if $b = (2^k + 2^{k+3})\ mod\ (2^n - 1)$.

Proof. First, notice that $\omega_2(a) = 2$ for all $a \in \bigcup_{i=1}^{\lfloor \frac{n}{2} \rfloor} S_i$, and $S_i \cap S_j = \varnothing$ for $1 \le i < j \le \lfloor \frac{n}{2} \rfloor$.

(1) Suppose $a = (2^{k_1}+1)2^{i_1} \bmod (2^n-1)$, $b = (2^{k_2}+1)2^{i_2} \bmod (2^n-1)$ for some $2 \le k_1, k_2 \le \lfloor \frac{n}{2} \rfloor$, $0 \le i_1, i_2 \le n-1$. Then

$$a + b = (2^{k_1+i_1} + 2^{i_1} + 2^{k_2+i_2} + 2^{i_2}) \bmod (2^n-1).$$

Let $K_l = \{i_l, (k_l+i_l) \bmod n\}, l = 1, 2$, then there are three cases as follows:

Case 1: $K_1 \cap K_2 = \varnothing$. Then $a + b \notin S_1$, since $\omega_2(a+b) = 4$.

Case 2: $|K_1 \cap K_2| = 1$. Then it is easy to see that $\omega_2(a+b) = 3$ since $2 \le k_1, k_2 \le \lfloor \frac{n}{2} \rfloor$. For example, if $k_1 + i_1 = (k_2+i_2) \bmod n$ and $i_1 \ne i_2$, then

$$\begin{aligned} a + b &= (2^{k_1+i_1+1} + 2^{i_1} + 2^{i_2}) \bmod (2^n-1) \\ &= (2^{k_2+i_2+1} + 2^{i_1} + 2^{i_2}) \bmod (2^n-1). \end{aligned}$$

Meanwhile, $i_1 \ne (k_1+i_1+1) \bmod n$ and $i_2 \ne (k_2+i_2+1) \bmod n$ since $2 \le k_1, k_2 \le \lfloor \frac{n}{2} \rfloor$. Then we have $\omega_2(a+b) = 3$. The other cases can be deduced similarly and hence $a + b \notin S_1$.

Case 3: $K_1 = K_2$. Then $a + b = 2a \in S_{k_1}$, which means $a + b \notin S_1$ since $S_1 \cap S_{k_1} = \varnothing$ for $2 \le k_1 \le \lfloor \frac{n}{2} \rfloor$.

Therefore, the proposition holds.

(2) The sufficiency is obvious, we only need to prove the necessity. Suppose $a = (2^k+2^{k+1}) \bmod (2^n-1)$ for some $0 \le k \le n-1$, $b = (2^{k_3}+1)2^{i_3} \bmod (2^n-1)$ for some $2 \le k_3 \le \lfloor \frac{n}{2} \rfloor$, $0 \le i_3 \le n-1$, then

$$a + b = (2^k + 2^{k+1} + 2^{k_3+i_3} + 2^{i_3}) \bmod (2^n-1).$$

Notice that $b \in \bigcup_{i=2}^{\lfloor \frac{n}{2} \rfloor} S_i$ and $a \in S_1$, then $|\{k, (k+1) \bmod n\} \cap K_b| \le 1$, where $K_b = \{i_3, (k_3+i_3) \bmod n\}$. Since $\omega_2(a+b) = 2$, then it must have $k \in K_b$. Otherwise, $\omega_2(a+b) = 4$ when $\{k, (k+1) \bmod n\} \cap K_b = \varnothing$; and $\omega_2(a+b) = 3$ when $((k+1) \bmod n) \in K_b$ and $k \notin K_b$, which can be easily proved as in the case 2 in (1).

Let $\{k^{'}\} = K_b \setminus \{k\}$, then we have

$$\begin{aligned} (a+b) &= 2^k + 2^{k+1} + 2^k + 2^{k^{'}} \bmod (2^n-1) \\ &= (2^{k+2} + 2^{k^{'}}) \bmod (2^n-1). \end{aligned}$$

Since $a + b \in S_1$, then $k^{'} = (k+1) \bmod n$ or $k^{'} = (k+3) \bmod n$. If $k^{'} = (k+1) \bmod n$, then $b = a \in S_1$, which contradicts with $b \in \bigcup_{i=2}^{\lfloor \frac{n}{2} \rfloor} S_i$. Therefore, $k^{'} = (k+3) \bmod n$ and $b = (2^k + 2^{k+3}) \bmod (2^n-1)$. □

We also recall the following lemma [15]:

Lemma 6. *Let $F(x) \in \mathbb{F}_{2^n}[x]$, S be a subset of $\mathbb{F}_{2^n}$, $H(x) = \prod_{\alpha \in S}(x+\alpha)$. Then the following statements hold.*

1. *$Tr(F(x)) = 0$ for all $x \in S$ if and only if there exists $G(x) \in \mathbb{F}_{2^n}[x]$ such that $F(x) \equiv (G(x) + G(x)^2)$ mod $H(x)$.*
2. *$\mathrm{Tr}(F(x)) = 1$ for all $x \in S$ if and only if there exist $G(x) \in \mathbb{F}_{2^n}[x], \gamma \in \mathbb{F}_{2^n}, \mathrm{Tr}(\gamma) = 1$ such that $F(x) \equiv (G(x) + G(x)^2 + \gamma)$ mod $H(x)$.*

Lemma 7. *Let $n \geq 7$ and $L(x) = \sum_{i=0}^{n-1} c_i x^{2^i} \in \mathbb{F}_{2^n}[x]$ be a linearized polynomial. Assume that $x^{-1} + L(x)$ is a permutation. Then $c_1 = 0$ and $c_3 = 0$.*

Proof. Assume that $x^{-1} + L(x)$ is a permutation on $\mathbb{F}_{2^n}$. By Lemma 5, $c_0 = 0$, and $\forall x \in \mathbb{F}_{2^n}$, $\mathrm{Tr}(xL(x)) = 0$. Let

$$F(x) = \begin{cases} \sum_{i=1}^{\frac{n-1}{2}} \sum_{j=0}^{i-1} (c_i^{2^{n-i}} x^{2^{n-i}+1})^{2^j}, & \text{for odd } n, \\ \sum_{i=1}^{\frac{n-2}{2}} \sum_{j=0}^{i-1} (c_i^{2^{n-i}} x^{2^{n-i}+1})^{2^j} + \sum_{j=0}^{\frac{n}{2}-1} (\gamma^{2^{\frac{n}{2}}} x^{2^{\frac{n}{2}}+1})^{2^j}, & \text{for even } n, \end{cases}$$

where $\gamma \in \mathbb{F}_{2^n}$ with $\gamma + \gamma^{\frac{n}{2}} = c_{\frac{n}{2}}$ when n is even, which is true since by Theorem 1, $c_{\frac{n}{2}} \in \mathbb{F}_{2^{\frac{n}{2}}}$. Thus it easy to check that

$$xL(x) = (F(x) + F(x)^2) \text{ mod } (x^{2^n} + x).$$

Therefore, for any $\alpha \in \mathbb{F}_{2^n}$ with $L(\alpha) \neq 0$, the roots of equation

$$y^2 + \alpha L(\alpha) y + (\alpha L(\alpha))^3 = 0$$

are $\alpha L(\alpha) F(\alpha)$ and $\alpha L(\alpha) F(\alpha) + \alpha L(\alpha)$. It has shown that $\mathcal{K}(\alpha L(\alpha)) = 0$ by Lemma 5. Then according to Lemma 2, we have

$$\begin{aligned} 0 &= \mathrm{Tr}(\alpha L(\alpha) F(\alpha)) \\ &= \mathrm{Tr}(F(\alpha)^2 + F(\alpha)^3) \\ &= \mathrm{Tr}(F(\alpha) + F(\alpha)^3) \end{aligned}$$

for all $\alpha \in \mathbb{F}_{2^n} \setminus \ker(L)$. Notice that for $\alpha \in \ker(L)$, the above formula also holds. Then we have

$$\forall \alpha, \mathrm{Tr}(F(\alpha) + F(\alpha)^3) = 0.$$

According to Lemma 6, there exists $G(x) \in \mathbb{F}_{2^n}[x]$ such that

$$\begin{aligned} F(x) + F(x)^3 &= (G(x) + G(x)^2) \text{ mod } (x^{2^n} + x) \\ &= \sum_{i=0}^{2^n-1} (g_i + g_{\frac{i}{2}}^2) x^i, \end{aligned} \tag{1}$$

where $\frac{i}{2}$ is interpreted as an element in $\mathbb{Z}_{2^n-1}$, and $\frac{1}{2}$ is the unique inverse of 2 in $\mathbb{Z}_{2^n-1}$.

Writing $F(x)$ as $F(x) = c_1^{2^{n-1}} x^{2^{n-1}+1} + K(x)$, then

$$\begin{aligned}
F(x)^3 &= (c_1^{2^{n-1}} x^{2^{n-1}+1} + K(x))^3 \bmod (x^{2^n} + x) \\
&= (c_1^{2^{n-1}+1} x^{2^{n-1}+4} + c_1^{2^{n-1}} x^{2^{n-1}+1} K(x)^2 + c_1 x^3 K(x) + K(x)^3 \bmod (x^{2^n} + x)) \\
&= (\ c_1^{2^{n-1}+1} x^{2^{n-1}+4} + K_1(x) + K_2(x) + K_3(x)) \bmod (x^{2^n} + x)
\end{aligned}$$

where $K_1(x) = c_1^{2^{n-1}} x^{2^{n-1}+1} K(x)^2, K_2(x) = c_1 x^3 K(x), K_3(x) = K(x)^3$.

Let S_k be the same sets as in Proposition 1, $1 \le k \le \lfloor \frac{n}{2} \rfloor$, and $x^{S_1} = \{x^d \mid d \in S_1\}$. It is easy to see $S_{n-k} = S_k$ for $1 \le k \le \lfloor \frac{n}{2} \rfloor$. Considering the following cases:

(i) The terms of $K_3(x)$ are of the form $x^{a+b} \bmod (x^{2^n} + x)$ for $a, b \in \bigcup_{i=2}^{\lfloor \frac{n}{2} \rfloor} S_i$, which can never be in x^{S_1} according to (1) of Proposition 1.

(ii) The terms of $K_2(x)$ are of the form $x^{2^{n-i+j}+2^j+3} \bmod (x^{2^n} + x)$ for $2 \le i \le \lfloor \frac{n}{2} \rfloor, 0 \le j \le i-1$. By (2) of Proposition 1, it is in S_1 if and only if $(2^{n-i+j} + 2^j) \bmod (2^n - 1) = 9$. Therefore, $j = 0, i = n-3$ or $i = j = 3$, which are impossible since $n \ge 7$ and $2 \le i \le \lfloor \frac{n}{2} \rfloor, 0 \le j \le i-1$.

(iii) The terms of $K_1(x)$ are of the the form $x^{2^{n-i+j+1}+2^{j+1}+2^{n-1}+1} \bmod (x^{2^n} + x)$ for $2 \le i \le \lfloor \frac{n}{2} \rfloor, 0 \le j \le i-1$. By (2) of Proposition 1, it is in x^{S_1} if and only if

$$\begin{cases} n - i + j + 1 = n - 1 \bmod n \\ j + 1 = 2 \bmod n, \end{cases}$$

which is equivalent to $j = 1, i = 3$.

Hence, the only term of $K_1(x)$ in x^{S_1} is $c_1^{2^{n-1}} c_3^{2^{n-1}} x^6$. Thus the terms of $(F(x) + F(x)^3) \bmod (x^{2^n} + x)$ in x^{S_1} with nonzero coefficients are $c_1^{2^{n-1}} x^{2^{n-1}+1}$ and $c_1^{2^{n-1}} c_3^{2^{n-1}} x^6$.

Equating the coefficient of x^{S_1} in equation (1), we have

$$\begin{cases} c_1^{2^{n-1}} & = g_{2^{n-1}+1} + g_{2^{n-2}+2^{n-1}}^2, \\ c_1^{2^{n-1}} c_3^{2^{n-1}} & = g_6 + g_3^2, \\ 0 & = g_i + g_{\frac{i}{2}}^2, \quad \text{for } i \in S_1 \setminus \{6, 2^{n-1}+1\}. \end{cases}$$

Therefore,

$$\begin{aligned}
c_1^{2^{n-1}} &= g_{2^{n-1}+1} + g_{2^{n-2}+2^{n-1}}^2 \\
&= g_{2^{n-1}+1} + g_{2^{n-3}+2^{n-2}}^{2^2} \\
&= \dots \\
&= g_{2^{n-1}+1} + g_{2^1+2^2}^{2^{n-2}} \\
&= g_{2^{n-1}+1} + g_6^{2^{n-2}},
\end{aligned}$$

and

$$\begin{aligned} c_1^{2^{n-1}} c_3^{2^{n-1}} &= g_6 + g_3^2 \\ &= g_6 + g_{2^{n-1}+1}^4. \end{aligned}$$

Then we have

$$c_1^{2^{n-1}} c_3^{2^{n-1}} = (c_1^{2^{n-1}})^4,$$

which is equivalent to $c_1 c_3 = c_1^4$.

Let $k = 3$ in (1) of Corollary 1, then we have

$$\begin{aligned} c_3 c_5 &= c_3^{2^2} c_1^2 + c_1^{2^3} c_3^2 \\ &= c_3^{2^2} c_1^2 + (c_1 c_3)^2 c_3^2 \\ &= 0. \end{aligned}$$

If $c_3 \neq 0$, then $c_5 = 0$. Let $k = 5$ in (1) of Corollary 1, then we have

$$c_3^{2^4} c_3^2 = c_5 c_7 + c_1^{2^5} c_5^2 = 0.$$

This shows $c_3 = 0$, which is a contradiction. Hence $c_3 = 0$. Furthermore $c_1 = 0$ from the equality $c_1^4 = c_1 c_3$ and $c_3 = 0$. □

With the above Preparations, we are ready to prove the main result of this paper.

Theorem 2. *Let $n \geq 7$ and $L(x) = \sum_{i=0}^{n-1} c_i x^{2^i} \in \mathbb{F}_{2^n}[x]$ be a linearized polynomial. Then $x^{-1} + L(x)$ is not a permutation on $\mathbb{F}_{2^n}$.*

Proof. Assume that $x^{-1} + L(x)$ is a permutation on $\mathbb{F}_{2^n}$. By Lemma 5, and Lemma 7, we have $c_0 = 0$, $c_1 = 0$ and $c_3 = 0$. According to (1) of Corollary 1, we have

$$\begin{aligned} 0 &= c_k c_{k+2} + c_3^{2^{k-1}} c_{k-2}^2 + c_1^{2^k} c_k^2 \\ &= c_k c_{k+2} \end{aligned} \tag{2}$$

for $2 \leq k \leq n-2$. In particular, let $k = 2$, we get $c_2 c_4 = 0$. Using (2) of Corollary 1 by setting $k = 2$, we have $c_2^{10} = c_4 c_5$ since $c_3 = 0$. Then

$$c_2^{11} = c_2 c_2^{10} = c_2 c_4 c_5 = 0.$$

Hence $c_2 = 0$.

Notice that equation (2) means that for $2 \leq k \leq n-2$, if $c_k \neq 0$, then $c_{k+2} = 0$. We claim that $c_k = 0$ for all $2 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. This can be proved by induction on k. First, we already have $c_2 = c_3 = 0$. Assume $c_j = 0$ for all j with $2 \leq j \leq k-1$. We need to show $c_k = 0$. Without loss of generality, we assume $k \geq 4$. Assume $c_k \neq 0$, then $c_{k+2} = 0$. According to (2) of Corollary 1, we have

$$0 = c_{k+2} c_{2k+1} + c_k^{2^{k+1}+2} + c_{k-2}^{2^{k+2}} c_{2k-1}^2$$

for all $2 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. Therefore from $c_{k+2} = 0$ and $c_{k-2} = 0$ (by induction), we know $c_k = 0$. This contradiction shows $c_k = 0$, and hence the claim holds. Then when n is odd, $L(x) = 0$, a contradiction. As for n is even, $L(x) = c_{\frac{n}{2}} x^{\frac{n}{2}}$. According to Example 1, $x^{-1} + L(x)$ is not a permutation on $\mathbb{F}_{2^n}$.

Thus we have proved that $x^{-1} + L(x)$ is not a permutation on $\mathbb{F}_{2^n}$ when $n \geq 7$. □

Summarize Theorem 2 and the simulation results in [15], the following result is obtained immediately.

Theorem 3. *Suppose $L(x) \in \mathbb{F}_{2^n}[x]$ is a linearized polynomial, then*

(1) When $n = 3$, $x^{-1} + L(x)$ is a permutation polynomial over $\mathbb{F}_{2^3}$ if and only if $L(x) = \alpha x^2 + \alpha^4 x^4$, where $\alpha \in \mathbb{F}_{2^3}^*$.
(2) When $n = 4$, $x^{-1} + L(x)$ is a permutation polynomial over $\mathbb{F}_{2^4}$ if and only if $L(x) = \alpha x^2 + (\alpha x)^8$, where $\alpha \in \mathbb{F}_{2^4}^*$ and $\alpha^5 = 1$.
(3) When $n \geq 5$, there are no permutation polynomials of the type $x^{-1} + L(x)$ over $\mathbb{F}_{2^n}$.

4 Conclusion

By means of Hermite's criterion and some results of the complete Kloosterman sums, we have proved the nonexistence of permutation polynomials of the form $x^{-1}+L(x)$ on $\mathbb{F}_{2^n}$ when $n \geq 5$. Hence a permutation polynomial is EA equivalent to the inverse function on $\mathbb{F}_{2^n}$ if and only if it is affine equivalent to it when $n \geq 5$.

References

1. Berger T.P., Canteaut A., Charpin P., Laigle-Chapuy Y.: On almost perfect nonlinear functions over $\mathbb{F}_{2^n}$. IEEE Trans. Inform. Theory 52(9), 4160-4170 (2006).
2. Beth T., Ding C.: On almost perfect nonlinear permutations. In: Advances in Cryptology -EUROCRYPT'93. LNCS, Vol. 765, pp. 65-76. Springer-Verlag, New York (1994).
3. Biham E., Shamir A.: Defferential cryptanalysis of DES-like cryptosystems. J. Cryptol. 4(1), 3-72 (1991).
4. Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. on Inform. Theory 52(3), 1141-1152 (2006).
5. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations sutiable for DES-like cryptosystems. Des. Codes Cryptogr. 15(2), 125-156 (1998).
6. Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. In: Advances in Cryptology -EUROCRYPT'94. LNCS, vol. 950, pp. 356-365. Springer-Verlag, New York (1995).
7. Charpin P., Helleseth T., Zinoviev V.: Propagation Characteristics of $x^{-1} \to x$ and Kloosterman Sums. Finite Fields Appl. 13, 366-381 (2007).
8. Charpin P, Gong G.: Hyperbent Functions, Kloosterman Sums, and Dickson Polynomials. IEEE Trans. Inform. Theory 54(9), 4230-4238 (2008).

9. Dillon J.F.: APN polynomials: An Update. In: proceedings of: The 9th Conference on Finite Fields and Applications FQ9 (to be published), Dublin, Ireland (2009).
10. Dillon J.F.: Elementary Hadamard Difference sets. Ph.D. dissertation, University of Maryland, 1974.
11. Edel Y., Kyureghyan G., PottA.: A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory 52(2), 744-747 (2006).
12. Helleseth T., Zinoviev V.: On Z_4-Linear Goethals Codes and Kloosterman Sums. Designs, Codes and Cryptography, 17, 269-288 (1999).
13. Hou X.D.: Affinity of permutations of $\mathbb{F}_2^n$. Discrete Appl. Math. 154(2), 313-325 (2006).
14. Lachaud G., Wolfmann J.: The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. IEEE Trans. Inform. Theory 36(3), 686-692 (1990).
15. Li Y., Wang M.: On EA-equivalence of certain permutations to power mappings. Des. Codes Cryptogr. (publised on line, 25 May) (2010).
16. Lidl R., Niederreiter H.: Finite Fields, Encyclopedia of Mathematics and its Applications 20, vol. 20. Addison-Wesley, Massachusetts (1983).
17. Lisoněk P.: On the Connection between Kloosterman Sums and Elliptic Curves. SETA 2008, LNCS 5203, pp. 182-187 (2008).
18. Nyberg K.: Differentially uniform mappings for cryptography. In: Advances in Cryptography-EUROCRYPT'93. LNCS, vol. 765, pp. 55-64. Springer-Verlag, New York (1994).
19. Pasalic E.: On Cryptographically Significant Mappings over $GF(2^n)$. In: WAIFI 2008, vol. 5130, pp. 189-204 (2008).
20. Pasalic E., Charpin P.: Some results concerning cryptographically significant mappings over GF(2^n). Des. Codes Cryptogr. 57(3), 257-269 (2010).