Two Applications of an Incomplete Additive Character Sum to Estimating Nonlinearity of Boolean Functions*

Yusong Du[1,2] and Fangguo Zhang[1,3]

[1] School of Information Science and Technology
Sun Yat-sen University, Guangzhou 510006, P.R. China
[2] Key Lab of Network Security and Cryptology
Fujian Normal University, Fuzhou 350007, P.R.China
[3] State Key Laboratory of Information Security, Institute of Software
Chinese Academy of Sciences, Beijing, P.R. China
yusongdu@hotmail.com, isszhfg@mail.sysu.edu.cn

Abstract. In recent years, several classes of Boolean functions with good cryptographic properties have been constructed by using univariate (or bivariate) polynomial representation of Boolean functions over finite fields. The estimation of an incomplete additive character sum plays an important role in analyzing the nonlinearity of these functions. In this paper, we consider replacing this character sum with another incomplete additive character sum, whose estimation was firstly given by A.Winterhof in 1999. Based on Winterhof's estimation, we try to modify two of these functions and obtain better nonlinearity bound of them.

Keywords: Boolean function, incomplete additive character sum, nonlinearity, algebraic degree, algebraic immunity.

1 Introduction

In order to resist all kinds of cryptographic attacks, Boolean functions used in stream ciphers should have good cryptographic properties including balancedness, high algebraic degree, high nonlinearity, high resiliency and large algebraic immunity. Construction of Boolean functions with good cryptographic properties has been an important problem for many years.

In 2008, Carlet and Feng exploited the univariate polynomial representation of Boolean functions in finite fields and constructed successfully a class of balanced Boolean functions with optimal algebraic degree, optimal algebraic immunity and good nonlinearity [1]. Before this result, none of constructed Boolean functions with optimal algebraic immunity could be proven to have good nonlinearity. This class of functions was then called the Carlet-Feng function. From

* This work is supported by Funds of Key Lab of Fujian Province University Network Security and Cryptology (2011008) and National Natural Science Foundations of China (Grant No. 61070168, Grant No. 10971246).

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 190–201, 2011.

then on, Boolean functions with optimal algebraic immunity constructed by using univariate (or bivariate) polynomial representation received more attention [2,3,4,5,6,7,8].

P.Rizomiliotis discussed the resistance of Boolean functions against (fast) algebraic attacks and provided a sufficient and necessary condition of Boolean function having optimal algebraic immunity under univariate polynomial representation [7]. Before long, X.Zeng *et al.* exploited the sufficient and necessary condition and provided more constructions of Boolean functions with optimal algebraic immunity under univariate polynomial representation [8].

Tu and Deng firstly studied the algebraic immunity of a subclass of the so-called *Partial Spread* functions introduced by Dillon [9]. They obtained a class of bent functions with optimal algebraic immunity based on an unproven combinatoric conjecture and constructed a class of Boolean functions in even variables with optimal algebraic degree, better nonlinearity (than that of the Carlet-Feng function) and optimal algebraic immunity based on the conjecture [3]. This class of functions was then called the Tu-Deng function. They also proposed a class of 1-resilient functions in even variables with optimal algebraic degree, good nonlinearity and suboptimal algebraic immunity based on the conjecture [5].

Before long, X.Tang *et al.* generalized Tu-Deng's results. Based on Tu-Deng's conjecture, they further improved the nonlinearity of balanced Boolean functions with optimal algebraic immunity and also gave a class of 1-resilient functions in even variables with optimal algebraic degree, good nonlinearity and suboptimal algebraic immunity [6].

It is easy to see that the estimation of the incomplete additive character sum over $\mathbb{F}_{2^n}$,

$$\left| \sum_{i=2^{n-1}-1}^{2^n-2} (-1)^{tr(\lambda\alpha^i)} \right| \leq 2^{\frac{n}{2}} n \cdot \ln 2 + 1, \quad (\lambda \in \mathbb{F}_{2^n}^*)$$

plays an important role in analyzing the nonlinearity of the Carlet-Feng function, the Tu-Deng function and Tu-Deng's 1-resilient function, where α is a primitive element of $\mathbb{F}_{2^n}$ and $tr(\cdot) = tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\cdot)$ is the absolute trace function.

In this paper, we would like to consider replacing this character sum with another incomplete additive character sum, whose estimation was firstly given by A.Winterhof in 1999 [10]. Based on the character sum considered by Winterhof, we try to modify the Tu-Deng function and Tu-Deng's 1-resilient function. Using Winterhof's estimation, we can obtain better nonlinearity bound of these two functions.

The nonlinearity bound of the modified functions will be better than that of the original functions, but unfortunately it is worse than that of the Boolean functions given by X.Tang *et al.* in [6]. Moreover, the algebraic degree of the modified Tu-Deng function will decrease compared with the original function. This means that the modified functions given by us may not be a good choice for stream ciphers. However, we believe that our work will help us understand the impact of incomplete additive character sums on the estimation of nonlinearity of Boolean functions.

The rest of the paper is organized as follows. Section 2 provides some preliminaries and recalls the character sum considered by Winterhof. Section 3 and Section 4 modify the Tu-Deng function and Tu-Deng's 1-resilient function respectively and discuss their cryptographic properties.

2 Preliminaries

Let n be a positive integer. We denote by $\mathbb{B}_n$ the set of all the n-variable Boolean functions. Any n-variable Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form*(ANF),

$$f(x_1, x_2, \cdots, x_n) = a_0 + \sum_{1 \le i \le n} a_i x_i + \sum_{1 \le i < j \le n} a_{ij} x_i x_j + \cdots + a_{12\cdots n} x_1 x_2 \cdots x_n,$$

where $a_0, a_i, a_{ij}, \ldots, a_{12\cdots n}$ belong to $\mathbb{F}_2$. The algebraic degree of Boolean function f, denoted by $\deg(f)$, is the degree of this polynomial, i.e., the number of variables in the highest order term with nonzero coefficient. A boolean function is *affine* if there exists no term of degree strictly greater than 1 in the ANF.

A Boolean function $g \in \mathbb{B}_n$ is called an *annihilator* of $f \in \mathbb{B}_n$ if $fg = 0$. The lowest algebraic degree of all the nonzero annihilators of f and $1 + f$ is called *algebraic immunity* of f, denoted by $\mathcal{AI}_n(f)$. It has been also proved that $\mathcal{AI}_n(f) \le \lceil \frac{n}{2} \rceil$ for a given $f \in \mathbb{B}_n$ [11,12]. A Boolean function $f \in \mathbb{B}_n$ has *optimal (suboptimal) algebraic immunity* if $\mathcal{AI}_n(f) = \lceil \frac{n}{2} \rceil$ $(= \lceil \frac{n}{2} \rceil - 1)$.

For $f \in \mathbb{B}_n$, the set of $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$ for which $f(x) = 1$ (resp. $f(x) = 0$) is called the on-set (resp. off-set) of f, denoted by $\mathrm{supp}(f)$ (resp. $\mathrm{supp}(1 + f)$). The Hamming weight of f is the cardinality of $\mathrm{supp}(f)$, denoted by $\mathrm{wt}(f)$. f is called balanced if $\mathrm{wt}(f) = 2^{n-1}$.

The Hamming distance of $f \in \mathbb{B}_n$ from $g \in \mathbb{B}_n$ is the Hamming weight of $f+g$. The nonlinearity of an n-variable Boolean function f is its minimum Hamming distance from all the n-variable affine functions. The nonlinearity of $f \in \mathbb{B}_n$ can be described through its Walsh transform:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|,$$

where $W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \omega \cdot x}$ and $\omega \cdot x \in \mathbb{F}_2$ is the usual inner product over $\mathbb{F}_2^n$. Moreover, $W_f(\omega) = -2 \sum_{\mathrm{supp}(f)} (-1)^{\omega \cdot x}$ for $\omega \neq 0$.

By identifying the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$, an n-variable Boolean function f can be written as a univariate polynomial over $\mathbb{F}_{2^n}$: $f(x) = \sum_{i=0}^{2^n-1} f_i x^i$, where f_0, $f_{2^n-1} \in \mathbb{F}_2$ and $f_{2i} = (f_i)^2 \in \mathbb{F}_{2^n}$, $1 \le i \le 2^n - 2$. The algebraic degree $\deg(f)$ (not the degree of the polynomial over $\mathbb{F}_{2^n}$) is given by the largest integer $s = \mathrm{wt}_2(i)$ such that $f_i \neq 0$, where $\mathrm{wt}_2(i)$ is the number of nonzero coefficients in the binary representation of i.

Let $n = 2k$ then $\mathbb{F}_{2^n} \cong \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and an n-variable Boolean function f can be written as a bivariate polynomial over $\mathbb{F}_{2^k}$: $f(x, y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j$,

where $h_{i,j} \in \mathbb{F}_{2^k}$. The algebraic degree of Boolean function f, $\deg(f)$ is given by the largest integer $s = \mathrm{wt}_2(i) + \mathrm{wt}_2(j)$ such that $h_{i,j} \neq 0$. Under bivariate polynomial representation over $\mathbb{F}_{2^k}$ the Walsh transform of Boolean function $f(x,y) \in \mathbb{B}_{2k}$ is given by $W_f(a,b) = \sum_{(x,y)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}} (-1)^{f(x,y)+tr(ax+by)}$ where $tr(\cdot)$ is the absolute trace function. Moreover, for $(a,b) \neq 0$, we have

$$W_f(a,b) = -2 \sum_{(x,y)\in \mathrm{supp}(f)} (-1)^{tr(ax+by)}.$$

Let ψ be the additive canonical character of $\mathbb{F}_{2^n}$, i.e.,

$$\psi(c) = (-1)^{tr(c)} \quad \text{for all} \quad c \in \mathbb{F}_{2^n},$$

and $g(x) \in \mathbb{F}_{2^n}[x]$ be a univariate polynomial over $\mathbb{F}_{2^n}$. Winterhof gave the following results.

Lemma 1. *[10] If the degree of $g(x)$ as a polynomial over $\mathbb{F}_{2^n}$, denoted by $\deg(g)$, is more than 2 and $\gcd(\deg(g), 2) = 1$, then*

$$\left| \sum_{x\in V} \psi(g(x)) \right| \leq (\deg(g) - 1) \cdot 2^{\frac{n}{2}}$$

holds for any additive subgroup V of $\mathbb{F}_{2^n}$.

3 The Modified Tu-Deng Functions with a Better Nonlinearity Bound

In this section we modify the Tu-Deng function according to Lemma 1, i.e., the incomplete additive character sum considered by Winterhof. Before this we recall the Tu-Deng function, which can be considered as a bivariate polynomial over $\mathbb{F}_{2^k}$.

Definition 1. *$2k$-variable Boolean function $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ is called the Tu-Deng function if*

$$F(x,y) = \begin{cases} f(\frac{x}{y}) & \text{if} \quad x \cdot y \neq 0 \\ 1 & \text{if} \quad x = 0, y \in \Delta \\ 0 & \text{otherwise} \end{cases},$$

where the k-variable Boolean function $f : \mathbb{F}_{2^k} \to \mathbb{F}_2$ is defined by

$$\mathrm{supp}(f) = \{1, \alpha^1, \cdots, \alpha^{2^{k-1}-1}\},$$

α is a primitive element of $\mathbb{F}_{2^k}$ and $\Delta = \{\alpha^i : i = 2^{k-1} - 1, 2^{k-1}, \cdots, 2^k - 2\}$.

In the following content in this paper, the k-variable Boolean function $f : \mathbb{F}_{2^k} \to \mathbb{F}_2$ is always defined by $\mathrm{supp}(f) = \{1, \alpha^1, \cdots, \alpha^{2^{k-1}-1}\}$ and α is a primitive element of $\mathbb{F}_{2^k}$.

It was proven that the Tu-Deng function has the optimal algebraic immunity if Tu-Deng's conjecture is true [3,4]. According to the fact that $2k$-variable Boolean function $H : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ defined by

$$H(x,y) = \begin{cases} f(\frac{x}{y}) & \text{if} \quad x \cdot y \neq 0 \\ 0 & \text{otherwise} \end{cases},$$

is a bent function and the estimation of the incomplete additive character sum over $\mathbb{F}_{2^k}$ given by Carlet and Feng,

$$\left| \sum_{i=2^{k-1}-1}^{2^k-2} (-1)^{tr(\lambda \alpha^i)} \right| \leq 2^{\frac{k}{2}} k \cdot \ln 2 + 1, \quad (\lambda \in \mathbb{F}_{2^k}^*)$$

it was shown also in [3,4] that the nonlinearity of the Tu-Deng function is greater and equal to

$$2^{2k-1} - 2^{k-1} - 2^{\frac{k}{2}} \cdot k \cdot \ln 2 - 1.$$

Now we give the modified Tu-Deng function. Let V be an additive subgroup (or considered as a vector subspace over $\mathbb{F}_2$) of dimension $k-1$ of $\mathbb{F}_{2^k}$, t be a positive integer and

$$V^t = \{\gamma^t \,|\, \gamma \in V\}.$$

It is not hard to see that $|V^t| \leq |V|$ and the equality holds if $\gcd(t, 2^k - 1) = 1$.

Definition 2. *$2k$-variable Boolean function $G_t : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ is defined by*

$$G_t(x,y) = \begin{cases} f(\frac{x}{y}) & \textit{if} \quad x \cdot y \neq 0 \\ 1 & \textit{if} \quad x = 0, y \in V^t \\ 0 & \textit{otherwise} \end{cases},$$

where V is an additive subgroup of dimension $k-1$ of $\mathbb{F}_{2^k}$ and t is a positive integer.

We discuss respectively the algebraic immunity, balanceness, nonlinearity and algebraic degree of $G_t(x,y) \in \mathbb{B}_{2k}$.

Recall the proof of the Tu-Deng function about optimal algebraic immunity in [3,4], we can see that replacing Δ in Definition 1 with V^t in Definition 2 does not essentially affect the procedures of the proof (Note that $h(x,0) =$ for $\forall x \in \mathbb{F}_{2^k}^*$ can imply that $h_{i,0} = 0$ for $1 \leq i \leq 2^k - 2$ but for $0 \leq i \leq 2^k - 1$). Therefore, $G_t(x,y) \in \mathbb{B}_{2k}$ still has optimal algebraic immunity if Tu-Deng's conjecture is true.

Theorem 1. *Boolean function $G_t(x,y) \in \mathbb{B}_{2k}$ defined as in Definition 2 has optimal algebraic immunity if Tu-Deng's conjecture is true.*

It is clear that $\mathrm{wt}(G_t(x,y)) = 2^{k-1}(2^k - 1) + |V^t|$. Since $|V^t| = |V| = 2^{k-1}$ if $\gcd(t, 2^k - 1) = 1$, about the balanceness of $G_t(x,y)$ we have the following result directly.

Theorem 2. *Boolean function $G_t(x, y) \in \mathbb{B}_{2k}$ defined as in Definition 2 is balanced if* $\gcd(t, 2^k - 1) = 1$.

Note that

$$2^k - 1 \equiv (-1)^k - 1 \equiv (-2) \bmod 3$$

if k is odd and

$$2^k - 1 \equiv (-1)^{\frac{k}{2}} - 1 \equiv (-2) \bmod 5$$

if $k \equiv 2 \bmod 4$. Then we have the following corollaries.

Corollary 1. *Boolean function $G_3(x, y) \in \mathbb{B}_{2k}$ defined as in Definition 2 is balanced if k is odd.*

Corollary 2. *Boolean function $G_5(x, y) \in \mathbb{B}_{2k}$ defined as in Definition 2 is balanced if $k \equiv 2 \bmod 4$.*

Theorem 3. *Let Boolean function $G_t(x, y) \in \mathbb{B}_{2k}$ be defined as in Definition 2. If $t > 2$ and $\gcd(t, 2^k - 1) = 1$ then its nonlinearity satisfies*

$$nl(G_t(x, y)) \geq 2^{2k-1} - 2^{k-1} - (t - 1) \cdot 2^{\frac{k}{2}}.$$

In particular,

$$nl(G_3(x, y)) \geq 2^{2k-1} - 2^{k-1} - 2^{\frac{k}{2}+1}$$

if k is odd, and

$$nl(G_5(x, y)) \geq 2^{2k-1} - 2^{k-1} - 2^{\frac{k}{2}+2}$$

if $k \equiv 2 \bmod 4$.

Proof. Since $\gcd(t, 2^k - 1) = 1$, G_t is balanced by Theorem 2 and $W_{G_t}(0, 0) = 0$. Let $0 \neq (a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, then

$$\begin{aligned} |W_{G_t}(a, b)| &= \left| -2 \sum_{(x,y) \in \mathrm{supp}(G_t)} (-1)^{tr(ax+by)} \right| \\ &= \left| W_H(a, b) - 2 \sum_{x=0, y \in V^t} (-1)^{tr(ax+by)} \right| \\ &\leq 2^k + 2 \left| \sum_{y \in V^t} (-1)^{tr(by)} \right|, \end{aligned}$$

where the $2k$-variable Boolean function H as mentioned before is a bent function.

From Lemma 1, if $t > 2$ and $\gcd(t, 2^k - 1) = 1$ then

$$\left| \sum_{y \in V^t} (-1)^{tr(by)} \right| = \left| \sum_{z \in V} (-1)^{tr(bz^t)} \right| \leq (t - 1) \cdot 2^{\frac{k}{2}},$$

which implies that

$$nl(G_t(x,y)) \geq 2^{2k-1} - 2^{k-1} - (t-1)\cdot 2^{\frac{k}{2}}.$$

It is trivial that the rest of the theorem holds. □

It is not hard to see that the nonlinearity bound of $G_3(x,y) \in \mathbb{B}_{2k}$ for odd k and $G_5(x,y) \in \mathbb{B}_{2k}$ for k with $k \equiv 2 \bmod 4$ are better than the nonlinearity bound of the original Tu-Deng function except for some small k. In other words, with Winterhof's estimation, in most of cases (at least three-fourth of all) the Tu-Deng function can be simply modified to have better nonlinearity bound.

However, the nonlinearity bound of $G_3(x,y)$ and $G_5(x,y)$ are still worse than the nonlinearity bound of the Boolean function given by X.Tang *et al.* in [6]. This is because H.Dobbertin's balanced Boolean function with very high nonlinearity [13] was involved cleverly in [6].

Before we determine the algebraic degree of $G_t(x,y) \in \mathbb{B}_{2k}$, we need two lemmas.

Lemma 2. *Let $0 \leq i \leq 2^k - 1$. If V is an additive subgroup of dimension $k-1$ of $\mathbb{F}_{2^k}$, then*

$$\sum_{\gamma \in V} \gamma^{-i} \neq 0$$

if and only if i is a power of 2.

Proof. Let $l(x) \in \mathbb{B}_k$ such that its on-set is V, i.e., $\mathrm{supp}(l(x)) = V$. Then $l(x)$ can be written as a univariate polynomial over $\mathbb{F}_{2^k}$:

$$l(x) = \sum_{\gamma \in V} (x+\gamma)^{2^k-1} = \sum_{i=0}^{2^k-1} \left(\sum_{\gamma \in V} \gamma^{2^k-1-i} \right) x^i = \sum_{i=0}^{2^k-1} \left(\sum_{\gamma \in V} \gamma^{-i} \right) x^i.$$

Then $\sum_{\gamma \in V} \gamma^{-i}$ is the coefficient of term x^i. Since V is an additive subgroup of dimension $k-1$ of $\mathbb{F}_{2^k}$, it is not hard to see that $l(x)$ is affine. Therefore,

$$l(x) = \sum_{j=0}^{k-1} \left(\sum_{\gamma \in V} \gamma^{2^k-1-2^j} \right) x^{2^j} = \sum_{j=0}^{k-1} \left(\sum_{\gamma \in V} \gamma^{-2^j} \right) x^{2^j}.$$

Comparing the coefficients of two equations above, we get desire result. □

Lemma 3. *Let k be a positive integer and j be a non-negative integer less than k. If k is odd then $\mathrm{wt}_2(\frac{2^k-1-2^j}{3}) = \frac{k-1}{2}$ where $j = 0, 2, 4, \cdots, k-1$. If $k \equiv 2 \bmod 4$ then $\mathrm{wt}_2(\frac{2^k-1-2^j}{5}) = \frac{k}{2}$ where $j = 3, 7, 11, \cdots, k-3$.*

Proof. If k is odd and $j = 0$, it is not hard to see that

$$2^k - 1 - 1 = 2(2^{k-1} - 1) = 2 \sum_{i=0}^{(k-3)/2} (2^{2i} + 2^{2i+1}) = 3 \sum_{i=0}^{(k-3)/2} 2^{2i+1}.$$

Thus, $\mathrm{wt}_2(\frac{2^k-2}{3}) = \frac{k-1}{2}$. Generally, for $j = 2, 4, 6, \cdots, k-1$, we have

$$2^k - 1 - 2^j = 2(2^{k-1} - 1) - (2^j - 1) = 3 \sum_{i=0}^{(k-3)/2} 2^{2i+1} - 3 \cdot 2^{j-2},$$

which implies that

$$\mathrm{wt}_2(\frac{2^k - 1 - 2^j}{3}) = \mathrm{wt}_2(\sum_{i=0}^{(k-3)/2} 2^{2i+1} - 2^{j-2}) = \frac{k-1}{2}.$$

Similarly, if $k \equiv 2 \bmod 4$ and $j = 3$ we have

$$2^k - 9 = 4(2^{k-2} - 1) - 5 = 5 \sum_{i=0}^{(k-6)/4} (2^{4i+2} + 2^{4i+3}) - 5$$

Therefore $\mathrm{wt}_2(\frac{2^k-9}{5}) = \frac{k-2}{2} + 1 = \frac{k}{2}$. Generally, for $j = 7, 11, \cdots, k-3$ we have

$$\begin{aligned}
&2^k - 1 - 2^j = 4(2^{k-2} - 1) - (2^j - 3) = 4(2^{k-2} - 1) - 3(2^{j-3} - 1) - 5 \cdot 2^{j-3} \\
&= 5 \sum_{i=0}^{(k-6)/4} (2^{4i+2} + 2^{4i+3}) - 5 \sum_{i=0}^{(j-7)/4} (2^{4i} + 2^{4i+3}) - 5 \cdot 2^{j-3} \\
&= 5 \sum_{i=(j+1)/4}^{(k-6)/4} (2^{4i+2} + 2^{4i+3}) + 5 \sum_{i=0}^{(j-7)/4} (2^{4i} + 2^{4i+1}) + 5(2^{j-1} + 2^j) - 5 \cdot 2^{j-3} \\
&= 5 \sum_{i=(j+1)/4}^{(k-6)/4} (2^{4i+2} + 2^{4i+3}) + 5 \sum_{i=0}^{(j-7)/4} (2^{4i} + 2^{4i+1}) + 5(2^{j-3} + 2^{j-2} + 2^j).
\end{aligned}$$

Therefore $\mathrm{wt}_2(\frac{2^k-1-2^j}{5}) = \frac{k-2}{2} - 2 + 3 = \frac{k}{2}$. □

Theorem 4. *Let $G_t(x, y) \in \mathbb{B}_{2k}$ be defined as in Definition 2. If k is odd then* $\deg(G_3(x, y)) = \frac{3k+1}{2}$. *If $k \equiv 2 \bmod 4$ then* $\deg(G_5(x, y)) = \frac{3k}{2}$.

Proof. Function $G_t(x, y)$ can be written as a bivariate polynomial over $\mathbb{F}_{2^k}$.

$$\begin{aligned}
G_t(x, y) &= H(x, y) + \sum_{a=0, b \in V^t} (1 + (x + a)^{2^k - 1})(1 + (y + b)^{2^k - 1}) \\
&= H(x, y) + \sum_{b \in V^t} (1 + x^{2^k - 1})(1 + (y + b)^{2^k - 1}),
\end{aligned}$$

where the $2k$-variable Boolean function H as mentioned before is a bent function.

Since $\deg(H) \leq k$, the algebraic degree of G_t is then determined by

$$\sum_{b \in V^t} (1 + x^{2^k - 1})(1 + (y + b)^{2^k - 1})$$

$$= (1+x^{2^k-1})(1+y^{2^k-1}) + \sum_{b\in(V^t)^*}(1+x^{2^k-1})(1+(y+b)^{2^k-1})$$

$$= x^{2^k-1} + y^{2^k-1} + \sum_{b\in(V^t)^*}\sum_{i=1}^{2^k-1} b^i y^{2^k-1-i}x^{2^k-1} + \sum_{b\in(V^t)^*}(y+b)^{2^k-1}$$

Thus, $\deg(G_t) = k + \mathrm{wt}_2(2^k-1-i)$ if and only if $\mathrm{wt}_2(2^k-1-i)$ is the largest integer such that

$$\sum_{b\in(V^t)^*} b^i \neq 0.$$

From Lemma 2, if k is odd, for $G_3(x,y)$,

$$\frac{2^k-1-2^j}{3}, \quad j = 0,2,4,\cdots,k-1$$

are all the integers such that

$$\sum_{b\in(V^3)^*} b^{\frac{2^k-1-2^j}{3}} = \sum_{b\in V^3} b^{\frac{2^k-1-2^j}{3}} = \sum_{b\in V} b^{2^k-1-2^j} = \sum_{b\in V} b^{-2^j} \neq 0.$$

By Lemma 3, $\mathrm{wt}_2(2^k-1-\frac{2^k-1-2^j}{3}) = k - \mathrm{wt}_2(\frac{2^k-1-2^j}{3}) = \frac{k+1}{2}$, i.e., $\deg(G_3) = k + \frac{k+1}{2} = \frac{3k+1}{2}$.

Similarly, from Lemma 2, if $k \equiv 2 \bmod 4$, for $G_5(x,y)$,

$$\frac{2^k-1-2^j}{5}, \quad j = 3,7,11,\cdots,k-3$$

are all the integers such that $\sum_{b\in(V^t)^*} b^{\frac{2^k-1-2^j}{5}} \neq 0$. By Lemma 3, $\mathrm{wt}_2(2^k-1-\frac{2^k-1-2^j}{5}) = k - \mathrm{wt}_2(\frac{2^k-1-2^j}{5}) = \frac{k}{2}$, i.e., $\deg(G_5) = k + \frac{k}{2} = \frac{3k}{2}$. The proof is completed. □

4 The Modified Tu-Deng's 1-Resilient Functions with a Better Nonlinearity Bound

Being similar to Section 3, in this section, we modify the 1-resilient Boolean function given by Tu and Deng according to Lemma 1, then discuss its cryptographic properties respectively.

Lemma 4. *[5] Let $F(x,y)$ be a $2k$-variable Boolean function, i.e., $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$. If its on-set $supp(F)$ is constituted by the following four disjoint parts:*

1. $\{(x,y) : y = \alpha^i x, x \in \mathbb{F}_{2^k}^*, i = 1,2,\cdots,2^{k-1}-1\}$
2. $\{(x,y) : y = x, x \in \mathcal{A}\}$
3. $\{(x,0) : x \in \mathbb{F}_{2^k} \setminus \mathcal{A}\}$
4. $\{(0,y) : y \in \mathbb{F}_{2^k} \setminus \mathcal{A}\}$

where $\mathcal{A} = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^{k-1}-1}\}$. *Then* F *is* 1*-resilient,* $deg(F) = 2k - 2$, $nl(F) \geq 2^{2k-1} - 2^{k-1} - 3 \cdot k \cdot 2^{\frac{k}{2}} \ln 2 - 7$ *and* $\mathcal{AI}_{2k}(F) \geq k - 1$ *if Tu-Deng's conjecture is true.*

The function $F(x, y)$ defined as in Lemma 4 is called Tu-Deng's 1-resilient function. Now we give the modified Tu-Deng's 1-resilient function.

Definition 3. *Let* V *be an additive subgroup of dimension* $k-1$ *of* $\mathbb{F}_{2^k}$ *and* $t \neq 2$ *be a positive integer such that* $\gcd(t, 2^k - 1) = 1$. *We define* $2k$*-variable Boolean function* $G_t(x, y) : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, *whose on-set* $\mathrm{supp}(G_t)$ *is constituted by the following four disjoint parts:*

1. $\{(x, y) : y = \alpha^i x, x \in \mathbb{F}_{2^k}^*, i = 1, 2, \cdots, 2^{k-1} - 1\}$
2. $\{(x, y) : y = x, x \in \mathcal{B}\}$
3. $\{(x, 0) : x \in \mathbb{F}_{2^k} \setminus \mathcal{B}\}$
4. $\{(0, y) : y \in \mathbb{F}_{2^k} \setminus \mathcal{B}\}$

where $\mathcal{B} = V^t \cup \{\beta\}$ *and* $\beta \in \mathbb{F}_{2^k} \setminus V^t$.

Recall the proofs of Tu-Deng's 1-resilient function about balanceness, 1-resiliency and optimal algebraic immunity respectively, we can see that replacing $\mathcal{A}$ in Lemma 4 with $\mathcal{B}$ in Definition 3 does not essentially affect the procedures of the proofs.

Theorem 5. *Let Boolean function* $G_t(x, y) \in \mathbb{B}_{2k}$ *be defined as in Definition 3. Then it is balanced and* 1*-resilient, and* $\mathcal{AI}_{2k}(G_t) \geq k - 1$ *if Tu-Deng's conjecture is true.*

Theorem 6. *Let Boolean function* $G_t(x, y) \in \mathbb{B}_{2k}$ *be defined as in Definition 3. Its nonlinearity satisfies*

$$nl(G_t(x, y)) \geq 2^{2k-1} - 2^{k-1} - 3(t-1) \cdot 2^{\frac{k}{2}} - 4.$$

In particular,

$$nl(G_3(x, y)) \geq 2^{2k-1} - 2^{k-1} - 3 \cdot 2^{\frac{k}{2}+1} - 4$$

if k *is odd, and*

$$nl(G_5(x, y)) \geq 2^{2k-1} - 2^{k-1} - 3 \cdot 2^{\frac{k}{2}+2} - 4$$

if $k \equiv 2 \bmod 4$.

Proof. Since G_t is balanced $W_{G_t}(0, 0) = 0$. Let $0 \neq (a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, then

$$\begin{aligned} W_{G_t}(a, b) &= -2 \sum_{(x,y) \in \mathrm{supp}(G_t)} (-1)^{tr(ax+by)} \\ &= -2 \sum_{i=1}^{2^{k-1}-1} \sum_{x \in \mathbb{F}_{2^k}^*} (-1)^{tr((a+b\alpha^i)x)} - 2 \sum_{x \in \mathcal{B}} (-1)^{tr((a+b)x)} \\ &\quad -2 \sum_{x \in \mathbb{F}_{2^k} \setminus \mathcal{B}} (-1)^{tr(ax)} - 2 \sum_{y \in \mathbb{F}_{2^k} \setminus \mathcal{B}} (-1)^{tr(by)} \end{aligned}$$

Since $t \neq 2$ and $\gcd(t, 2^k - 1) = 1$, from Lemma 1, we have

$$\left|\sum_{x\in\mathcal{B}}(-1)^{tr(ax)}\right| \leq \left|\sum_{x\in V^t}(-1)^{tr(ax)}\right| + 1 = \left|\sum_{z\in V}(-1)^{tr(az^t)}\right| + 1 \leq (t-1)\cdot 2^{\frac{k}{2}} + 1.$$

Similarly,

$$\left|\sum_{x\in\mathbb{F}_{2^k}\setminus\mathcal{B}}(-1)^{tr(ax)}\right| \leq (t-1)\cdot 2^{\frac{k}{2}} + 1.$$

Therefore, it can be verified that

$$\frac{1}{2}\left|\max_{(a,b)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}} W_{G_t}(a,b)\right| \leq 2^{k-1} + 1 + 3(t-1)\cdot 2^{\frac{k}{2}} + 3$$

which implies that

$$nl(G_t(x,y)) \geq 2^{2k-1} - 2^{k-1} - 3(t-1)\cdot 2^{\frac{k}{2}} - 4.$$

It is trivial that the rest of the theorem holds. □

Theorem 7. *Let Boolean function $G_t(x,y) \in \mathbb{B}_{2k}$ be defined as in Definition 3. If $k \neq 3$ then $\deg(G_3(x,y)) = \deg(G_5(x,y)) = 2k-2$.*

Proof. Let $F(x,y) \in \mathbb{B}_{2k}$ be defined as in Lemma 4. In [5] it was proved that $\deg(F) = 2k-2$ if

$$\sum_{\gamma\notin\mathcal{A}}\gamma^2 \neq 0.$$

It can be also see that replacing $\mathcal{A}$ in Lemma 4 with $\mathcal{B}$ in Definition 3 does not affect this result holding, i.e., for Boolean function $G_t(x,y) \in \mathbb{B}_{2k}$ defined as in Definition 3, $\deg(G_t) = 2k-2$ if

$$\sum_{\gamma\notin\mathcal{B}}\gamma^2 \neq 0.$$

Note that

$$\sum_{\gamma\notin\mathcal{B}}\gamma^2 + \sum_{\gamma\in\mathcal{B}}\gamma^2 = \sum_{\gamma\in\mathbb{F}_{2^k}}\gamma^2 = \left(\sum_{\gamma\in\mathbb{F}_{2^k}}\gamma\right)^2 = 0.$$

Then we have

$$\sum_{\gamma\notin\mathcal{B}}\gamma^2 = \sum_{\gamma\in\mathcal{B}}\gamma^2 = \sum_{\gamma\in V^t}\gamma^2 + \beta^2 = \left(\sum_{\gamma\in V^t}\gamma\right)^2 + \beta^2 = \left(\sum_{\gamma\in V}\gamma^t\right)^2 + \beta^2,$$

where $0 \neq \beta \in \mathbb{F}_{2^k} \setminus V^t$. According to Lemma 2, $\sum_{\gamma\in V}\gamma^3$ or $\sum_{\gamma\in V}\gamma^5$ can be nonzero only if $k = 3$. This means that

$$\sum_{\gamma\notin\mathcal{B}}\gamma^2 \neq 0$$

for $t = 3, 5$ when $k \neq 3$. Therefore $\deg(G_3(x,y)) = \deg(G_5(x,y)) = 2k-2$ when $k \neq 3$. □

5 Conclusion

In this paper, according to the incomplete additive character sum over finite filed $\mathbb{F}_{2^k}$ considered by Winterhof, we modify the Tu-Deng function and Tu-Deng's 1-resilient function respectively. Using Winterhof's estimation, we can obtain better nonlinearity bound of these two functions compared with the original functions. We also discuss other cryptographic properties of them.

References

1. Carlet, C., Feng, K.: An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 425–440. Springer, Heidelberg (2008)
2. Wang, Q., Peng, J., Kan, H., Xue, X.: Constructions of cryptographically significant Boolean functions using primitive polynomials. IEEE Trans. Inform. Theory 56(6), 3048–3053 (2010)
3. Tu, Z., Deng, Y.: A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Designs, Codes and Cryptography 60(1), 1–14 (2011)
4. Tu, Z., Deng, Y.: A Conjecture on Binary String and Its Applications on Constructing Boolean Functions of Optimal Algebraic Immunity. Cryptology ePrint Archive, `http://eprint.iacr.org/2009/272.pdf`
5. Tu, Z., Deng, Y.: Boolean functions with all main cryptographic properties. Cryptology ePrint Archive, `http://eprint.iacr.org/2010/518.pdf`
6. Tang, X., Tang, D., Zeng, X., Hu, L.: Balanced Boolean functions with (almost) optimal algebraic immunity and very high nonlinearity. Cryptology ePrint Archive, `http://eprint.iacr.org/2010/443`
7. Rizomiliotis, P.: On the Resistance of Boolean Functions Against Algebraic Attacks Using Univariate Polynomial Representation. IEEE Trans. Inform. Theory 56(8), 4014–4024 (2010)
8. Zeng, X., Carlet, C., Shan, J., Hu, L.: Balanced Boolean Functions with Optimum Algebraic Immunity and High Nonlinearity. Cryptology ePrint Archive, `http://eprint.iacr.org/2010/606`
9. Dillon, J.F.: Elementary Hadamard Difference Sets. PhD thesis, University of Maryland (1974)
10. Winterhof, A.: Incomplete Additive Character Sums and Applications. In: Jungnickel, D., Niederreiter, H. (eds.) The Fifth International Conference on Finite Fields and Applications Fq5 1999, pp. 462–474. Springer, Berlin (2001)
11. Courtois, N., Meier, W.: Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345–359. Springer, Heidelberg (2003)
12. Meier, W., Pasalic, E., Carlet, C.: Algebraic Attacks and Decomposition of Boolean Functions. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 474–491. Springer, Heidelberg (2004)
13. Dobbertin, H.: Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 61–74. Springer, Heidelberg (1995)