Applied Mathematics & Information Sciences **5**(1) (2011), 85-97
– An International Journal

Autocorrelation Coefficients of Two Classes of Semi-Bent Functions

Xuelian Li[1], Yupu Hu[2] and Juntao Gao[2]

[1]Department of Applied Mathematics of Xidian University, Xi'an, Shaanxi province,710071, China.

Email Address: xuelian202@163.com

[2]School of Telecommunications Engineering, Xidian University, Xi'an, Shannxi 710071, China.

Email Address: yphu@mail.xidian.edu.cn; jtgao@mail.xidian.edu.cn

Received October 12, 2010; Revised November 2, 2010

Low autocorrelation is an important prerequisite of Boolean functions when used as combiners in stream ciphers. In this paper, we investigate the autocorrelation of two classes of semi-bent functions constructed by Charpin et al.. We give all the autocorrelation coefficients of these semi-bent functions and prove that they have not correlation immune. Our results show that, although these semi-bent functions have good nonlinearity, they have high autocorrelations. The cipher constructed by these semi-bent functions can be prone to differential-like cryptanalysis, and they can not resist correlation attacks. These potential weakness have to be considered before we deploy them in applications.

Keywords: Boolean functions, Cryptography, Finite field, Semi-bent function, Walsh transforms, Additive autocorrelation.

1 Introduction

Boolean functions have wide applications in cryptography and coding theory. In general, a Boolean function should have good nonlinearity, resiliency and low autocorrelation. High nonlinearity ensures the cipher is not prone to linear approximation attack [1], while resiliency offers protection against correlation attack [2]. Usually, the resiliency of order 1 is enough for a Boolean function. Another criteria is low additive autocorrelation [3]. This ensures that the output of the Boolean function is complemented with a probability close to 1/2 when any number of input bits are complemented. As a result, the cipher does not suffer from differential-like cryptanalysis [4]. This is a more practical criteria for Boolean function than the propagation criteria of order k [5]. A function satisfying the propagation criterion of order k shows the perfect avalanche characteristic with respect to vectors of Hamming weight not larger than k. This property, however, does not rule out the

possibility that the function can have vectors of Hamming weight larger than k as its linear structures. Therefore the propagation criterion, though being an extension of the strict avalanche criterion (SAC), is merely another indicator for local properties. On the other hand, the criterion is too strict in the sense that it requires that $f(x) \oplus f(x+a)$ be 100 percent balanced. This leads to the situation where a function satisfying the propagation criterion of the largest possible order becomes bent. Although bent functions have nice nonlinearity, they are not balanced and hence can hardly be directly employed in practice. Global avalanche characteristics of cryptographic functions (GAC) [5] overcome the shortcomings of the SAC or its generalizations, and be able to forecast the overall avalanche characteristic of a cryptographic function. Additive autocorrelation is one of the two indicators of GAC. In addition, autocorrelation functions in another form also have applications in physics [6] [7].

Determining the autocorrelation coefficients $\Delta_f(a)$ for all $a \in F_{2^n}$, in other words, the addtive autocorrelation Δ_f, is of great interest in coding theory and cryptography [3] [8]. If all of the autocorrelation coefficients $\Delta_f(a)$ are low, then the Boolean function $f(x)$ can resist the differential-like cryptanalysis in all $a \in F_{2^n}$. Otherwise, the Boolean function $f(x)$ can suffer from differential-like cryptanalysis in some elements $a \in F_{2^n}$ which make $\Delta_f(a)$ be high. Although autocorrelation coefficient is an important indicator for a Boolean function, it is a difficult task to determine all the autocorrelation coefficients of the Boolean function. This is because computing the Hamming weights of these functions $f(x) \oplus f(x+a)$ for all $a \in GF(2^n)$ is not an easy thing.

In this paper, we investigate two classes of semi-bent functions constructed by Charpin et al. [9]. We point out the weakness of the construction techniques for these semi-bent functions in terms of autocorrelation coefficients and correlation immune. First, we prove that the two classes of semi-bent functions are not balanced, and give the conditions of their Hadamard transforms takeing zero or nonzero. We also correct an error statement for the conditions of Hadamard transforms of the semi-bent functions in [9] Theorem 12 i) takeing zero. Next, we deduce the dual functions of the two classes of semi-bent functions. By using the former conclusions, we get all the autocorrelation coefficients of the two classes of semi-bent functions, and obtain their absolute indicators Δ_f and sum of square indicators σ_f. In Section 2, we introduce some concepts and definitions which will be used throughout this paper. In Section 3, we deduce the dual functions of the two classes of semi-bent functions. Simultaneously, we give their all autocorrelation coefficients. Their orders of correlation immune are also given in Section 3. Concluding remarks and discussions will be given in Section 4.

2 Preliminaries

Let $GF(2^n)$ be the finite field of order 2^n and $GF(2^n)^*$ denote the set composed of all nonzero elements in $GF(2^n)$. The trace function $Tr : GF(2^n) \to GF(2)$ is defined as,

$$Tr(x) = x + x^2 + \cdots + x^{2^{n-1}}.$$

It is a linear function on $GF(2^n)$ and is basic to the representation of polynomial functions $f : GF(2^n) \to GF(2)$. The Hadamard transform of a polynomial function $f : GF(2^n) \to GF(2)$ at an element $\lambda \in GF(2^n)$ is define by,

$$\hat{f}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus Tr(\lambda x)}.$$

where $\oplus$ denotes the addition module 2. There is a natural correspondence between the polynomial functions $f : GF(2^n) \to GF(2)$ and the Boolean functions $g : GF(2)^n \to GF(2)$. Let $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ be a basis of $GF(2^n)$. This corresponding is given by

$$g(x_0, x_1, \cdots, x_{n-1}) = f(x_0\alpha_0 + x_1\alpha_1 + \cdots + x_{n-1}\alpha_{n-1})$$

The Hadamard transform or Walsh transform of a Boolean function $f : GF(2)^n \to GF(2)$ is

$$\hat{f}(\omega) = \sum_{x \in GF(2)^n} (-1)^{f(x) \oplus <\omega, x>}.$$

The scalar product $< \omega, x >: GF(2)^n \to GF(2)$, of vectors $x \in GF(2)^n$ and $\omega \in GF(2)^n$ is defined as $< \omega, x >= \sum_{i=0}^{n-1} \omega_i x_i$. We define the Walsh spectrum of $g(x)$ as the set $\{W_g(u) | u \in F_{2^n}\}$. The weight of a vector $\omega \in GF(2)^n$ is the number of ones in ω and is denoted by $wt(\omega)$. Correspondingly, The weight $wt(f)$ of a Boolean function f is the number of $x \in GF(2)^n$ such that $f(x) = 1$. A function f is said to be balanced if $wt(f) = wt(f \oplus 1)$, that is $\hat{f}(0) = 0$. A Boolean function $f : GF(2)^n \to GF(2)$ is kth order correlation immunity if $\hat{f}(\omega) = 0$ for all $1 \leq wt(\omega) \leq k$. Furthermore, if f is balanced and kth order correlation immunity, we say the Boolean function f is resilient of order k.

The nonlinearity of functions $f(x)$ is related to the Hadamard transform $\hat{f}(\omega)$. It is defined as follows,

$$N_f = 2^{n-1} - \frac{1}{2} max_{\omega \in GF(2)^n} |\hat{f}(\omega)|$$

The Boolean function $f(x)$ with a high nonlinearity can resist the linear approximation attack. Therefore, A high nonlinearity is necessary for a Boolean function. For even n, the bent functions are the functions of best nonlinearity. Semi-bent functions have almost optimal nonlinearity [15].

Definition 2.1 ([9]). Let n be an odd number. A Boolean function $f(x)$ with $f(0) = 0$ is said to be *semi-bent* if and only if its Walsh spectrum is

value	number it occurs
0	2^{n-1}
$2^{(n+1)/2}$	$2^{n-2}+2^{(n-3)/2}$
$-2^{(n+1)/2}$	$2^{n-2}-2^{(n-3)/2}$

Table 2.1: The Walsh spectrum of semi-bent function f (n is odd)

For even n, the semi-bent functions can be defined as follows.

Definition 2.2 ([9]). Let n be an even number. A Boolean function $f(x)$ with $f(0)=0$ is said to be *semi-bent* if and only if its Walsh spectrum is

value	number it occurs
0	$2^{n-1}+2^{n-2}$
$2^{(n+2)/2}$	$2^{n-3}+2^{(n-4)/2}$
$-2^{(n+2)/2}$	$2^{n-3}-2^{(n-4)/2}$

Table 2.2: The Walsh spectrum of semi-bent function f (n is even)

For an element $a \in GF(2)^{n^*}$, if $f(x) \oplus f(x+a) = constant$, then we call the a as a linear structure of $f(x)$. A nonzero linear structure is a bad character for a Boolean function because it makes the Boolean function be prone to differential-like cryptanalysis. If a Boolean function $f(x)$ is a bent function, then the function $f(x) \oplus f(x+a)$ must be a balanced function. Therefore, bent functions have not nonzero linear structure.

Given a Boolean function $f : GF(2)^n \to GF(2)$, the autocorrelation coefficient in an element $a \in GF(2)^n$ is defined as follows:

$$\Delta_f(a) = \sum_{x \in GF(2)^n} (-1)^{f(x) \oplus f(x+a)}$$

We say f satisfies the propagation criteria of order k, denoted $PC(k)$, if $\Delta_f(a) = 0$ for all $1 \leq wt(a) \leq k$. In informal terms, f satisfies the propagation criterion of order k if complementing k or less bits results in the output of f being complemented with a probability of a half. If $\Delta_f(a) = \pm 2^n$, then a is a linear structure of f which is undesirable.

Definition 2.3 ([5]). Let f be a Boolean function on $GF(2)^n$. The *additive autocorrelation* or the *absolute indicator* for the avalanche characteristic of f is defined by

$$\Delta_f = max_{a \in GF(2)^n, a \neq 0} |\Delta_f(a)|.$$

The *sum-of-squares indicator* for the characteristic of f is defined by

$$\sigma_f = \sum_{a \in GF(2)^n} \Delta_f(a)^2.$$

The smaller Δ_f and σ_f, the better the GAC of a function. Like many other nonlinearity characteristics of a function including nonlinearity, algebraic degree et. al., the two indicators for the GAC are invariant under nonsingular linear transforms on the input coordinates. $0 \leq \Delta_f \leq 2^n$, $2^{2n} \leq \sigma_f \leq 2^{3n}$. Moreover, $\Delta_f = 0$ if and only if f is bent, and $\Delta_f = 2^n$ if and only if f has a nonzero linear structure [5]. Let f be a non-bent cubic function on $GF(2^n)$, then $\Delta_f \geq 2^{(n+1)/2}$ [5].

3 The autocorrelation coefficients of semi-bent functions

3.1 General theory of autocorrelation of semi-bent functions

In [8], Guang Gong and Khoongming Khoo gave the concept of dual functions on the Boolean functions $f : F_2^n \to F_2$ to investigate the autocorrelation coefficients of 3-valued spectrum function.

Definition 3.1. Let $f(x)$ be a Boolean function on F_{2^n}. Its dual function o_f is defined as

$$o_f(\omega) = \begin{cases} 0 & \text{if } \hat{f}(\omega) = 0 \\ 1 & \text{if } \hat{f}(\omega) \neq 0 \end{cases}$$

The dual functions can be used to establish the relationship between the autocorrelation coefficients and the Walsh spectrum of $f(x)$ [8].

Lemma 3.1. *If $f(x)$ be a Boolean function on F_{2^n} with 3-valued spectrum $0, \pm 2^i$, then for all $a \neq 0$*

$$\Delta_f(a) = -2^{2i-(n+1)}\hat{o_f}(a). \tag{3.1}$$

Where $\hat{o_f}(a)$ denotes the Walsh spectrum of the dual function o_f in an element $a \in F_2^n$.

From Lemma 3.1, if $n = 2p + 1$, and $f(x)$ be a semi-bent function on F_2^n, then we have

$$\Delta_f(a) = -\hat{o_f}(a). \tag{3.2}$$

Similarly, if $n = 2p$, and $f(x)$ be a semi-bent function on F_2^n, then we have

$$\Delta_f(a) = -2\hat{o_f}(a). \tag{3.3}$$

Therefore, the autocorrelation coefficients of a semi-bent function $f(x)$ depend on the Walsh spectrum of its dual function o_f. We can give the autocorrelation coefficients by investigating the Walsh spectrum of dual function o_f.

3.2 The semi-bent functions investigated in this paper

In [9], Charpin, Pasalic and Tavernier first introduced some infinite classes of quadratic Bent and semi-bent functions with more trace form.These functions can be represented as

follows

$$f_c(x) = \bigoplus_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_i Tr(x^{2^i+1}), \quad c_i \in F_2. \tag{3.4}$$

Lemma 3.2. *Let n be even, $g(x)$ and $h(x)$ be two semi-bent functions on $GF(2^n)$. Let $f(x,y) = g(x)y \oplus h(x)(y \oplus 1)$ be the Boolean function on $GF(2^n) \times GF(2)$. Then $f(x,y)$ is semi-bent if and only if for any $\omega \in GF(2^n)$,*

$$\hat{g}(\omega) = \pm 2^{(n+2)/2} \Rightarrow \hat{h}(\omega) = 0.$$

Let n be an even integer, then $GF(4)$ is a subspace of $GF(2^n)$. Let

$$GF(4)^{\perp} = \{u \in GF(2^n) | \, Tr(uv) = 0, for\ all\ v \in GF(4)\}.$$

Obviously, $GF(4)^{\perp}$ is a subspace of $GF(2^n)$ under the addition operation and $\#GF(4)^{\perp} = 2^{n-2}$, where $\#GF(4)^{\perp}$ denotes the cardinality of the set $GF(4)^{\perp}$. A coset of $GF(4)^{\perp}$ is any subset of $GF(2^n)$ of the form of $u + GF(4)^{\perp}$, $u \in GF(2^n)$.

Lemma 3.3 ([9]). *Let $n = 2p$. We consider the $f_c(x)$ defined by (4) which is a semi-bent function. Set $I_e = \{i | \, c_i \neq 0$ and i even$\}$. Consider the function $g_\lambda(x) = f_c(x) \oplus Tr(\lambda x)$.*

- *If $\#I_e$ is even then $g_\lambda(x)$ is balanced if and only if $\lambda \notin GF(4)^{\perp}$.*
- *If $\#I_e$ is odd then $g_\lambda(x)$ is balanced if and only if $Tr(\lambda) = 1$ or $\lambda \in GF(4)^{\perp}$.*

Where $\#I_e$ denotes the cardinality of the set I_e.

This Lemma shows that the set of $\{\lambda | \hat{f}_c(\lambda) = 0\}$ can be determined by $GF(4)^{\perp}$ if $f_c(x)$ is a semi-bent function. The following Lemma 3.4 is Theorem 12 in [9].

Lemma 3.4. *Let $n = 2p$ and $f_b(x)$,$f_c(x)$ defined by (4), be two semi-bent functions on $GF(2^n)$. Let $u \in GF(2^n)$. Let us define the Boolean function on $GF(2^n) \times GF(2)$*

$$f : (x,y) \mapsto (f_b(x) \oplus Tr(ux))y \oplus f_c(x)(y \oplus 1).$$

Set $I_e(b) = \{i | \, b_i \neq 0$ and i even$\}$ and $I_e(c) = \{i | \, c_i \neq 0$ and i even$\}$. Then we have the following

1. *Assume that p is odd, $\#I_e(b)$ is odd, $\#I_e(c)$ is even and $u = 0$, then $f(x,y)$ is semi-bent.*
2. *Assume that p is even or $\#I_e(b)$ and $\#I_e(c)$ are even. Then for any $u \notin GF(4)^{\perp}$, the function f is semi-bent. Moreover, $f(x,y) \oplus Tr(\mu x) \oplus \nu y$ is balanced if and only if $u + \mu \notin GF(4)^{\perp}$.*

Moreover, $f(x,y)$ is of degree 3 if and only if $f_b(x) \oplus f_c(x) \neq 0$.

We are here to correct an error statement in Lemma 3.4 *2.*. From the proof of Theorem 12 in [9], we can know that $f(x,y) \oplus Tr(\mu x) \oplus \nu y$ is balanced if and only if $u + \mu \notin GF(4)^{\perp}$ and $\mu \notin GF(4)^{\perp}$, rather than $u + \mu \notin GF(4)^{\perp}$.

3.3 On the autocorrelation coefficients of semi-bent functions

This subsection concentrates on the autocorrelation coefficients of quadratic semi-bent functions in Lemma 3.4. The quadratic semi-bent functions have been fully studied in the form of Boolean functions [10]. However, the autocorrelation coefficients of these functions have not yet been involved in.

In the following theorem, we give the dual functions o_f of $f(x, y)$ in Lemma 3.4.

Theorem 3.1. *1. Let $f(x, y)$ be the function defined in Lemma 3.4 1., then its the dual function is*

$$o_f(\mu,\nu) = \begin{cases} 0, & \text{if } Tr(\mu)=1,\ \nu\in GF(2); \\ 1, & \text{if } Tr(\mu)=0,\ \nu\in GF(2). \end{cases} \tag{3.5}$$

$f(x, y)$ is not balanced.

2. Let $f(x, y)$ be the function defined in Lemma 3.4 2., then its the dual function is

$$o_f(\mu,\nu) = \begin{cases} 0, & \text{if } u+\mu\notin GF(4)^{\perp} \text{ and } \mu\notin GF(4)^{\perp},\ \nu\in GF(2); \\ 1, & \text{if } u+\mu\in GF(4)^{\perp} \text{ or } \mu\in GF(4)^{\perp},\ \nu\in GF(2). \end{cases} \tag{3.6}$$

$f(x, y)$ is not balanced.

Proof. Now, in order to to determine $o_f(\mu, \nu)$, we firstly find the points that the Walsh transform of $f(x, y)$ is zero and nonzero.

1. Let $f(x, y)$ be the function in Lemma 3.4 *1.*, then its Walsh transform is

$$\begin{aligned} \hat{f}(\mu,\nu) &= \sum_{\substack{x\in GF(2^n)\\ y\in GF(2)}} (-1)^{f(x,y)+Tr(\mu x)+\nu y} \\ &= \sum_{\substack{x\in GF(2^n)\\ y=0}} (-1)^{f_c(x)+Tr(\mu x)} + \sum_{\substack{x\in GF(2^n)\\ y=1}} (-1)^{f_b(x)+Tr(\mu x)+\nu} \end{aligned} \tag{3.7}$$

   (a) Since $\#I_e(b)$ is odd, from Lemma 3.3, $f_b(x) + Tr(\mu x)$ is not balanced if and only if $Tr(\mu) = 0$ and $\mu \notin GF(4)^{\perp}$. Because $f_b(x)$ is a semi-bent function, $\hat{f_b}(\mu)$ is $\pm 2^{(n+2)/2}$. By Lemma 3.2, $\hat{f_b}(\mu) = \pm 2^{(n+2)/2} \Rightarrow \hat{f_c}(x) = 0$. Therefore, $\hat{f}(\mu, \nu) = \pm 2^{(n+2)/2}$ if $Tr(\mu) = 0$ and $\mu \notin GF(4)^{\perp}$. Since $f_b(x)$ is a semi-bent function on $GF(2^n)$, where n is even, from Table 2.2, the number of μ for $\hat{f_b}(\mu) = \pm 2^{(n+2)/2}$ is 2^{n-2}. At $2^n - 2^{n-2}$ points $\hat{f_b}(\mu) = 0$. Because of $\nu \in GF(2)$, the number of (μ, ν) for $\hat{f}(\mu, \nu)$ is 2^{n-1}.

   (b) Since $\#I_c(b)$ is even, from Lemma 3.3, $f_c(x) \oplus Tr(\mu x)$ is not balanced if and only if $\mu \in GF(4)^{\perp}$. In a same method as (a), we can have $\hat{f}(\mu, \nu) = \pm 2^{(n+2)/2}$ if $\mu \in GF(4)^{\perp}$, and the number of (μ, ν) for $\hat{f}(\mu, \nu)$ is 2^{n-1}.

From (a) and (b), the number of (μ, ν) for $\hat{f}(\mu, \nu) \neq 0$, that is $\hat{f}(\mu, \nu) = \pm 2^{(n+2)/2}$, is 2^n. By noting that $n+1$ is odd and $f(x, y)$ is semi-bent, from Table 2.1, the number of (μ, ν) for $\hat{f}(\mu, \nu) \neq 0$ is exactly 2^n. Therefore, $\hat{f}(\mu, \nu) \neq 0$ if and only if $Tr(\mu) = 0$ and $\mu \notin GF(4)^{\perp}$, or $\mu \in GF(4)^{\perp}$. That is, $\hat{f}(\mu, \nu) \neq 0$ if and only if $Tr(\mu) = 0$, or $Tr(\mu) = 1$ and $\mu \in GF(4)^{\perp}$. However, by th definition of $GF(4)^{\perp}$, we can know $Tr(x) = Tr(x1) = 0$ for all $x \in GF(4)^{\perp}$, where "1" is the multiplicative identity element on $GF(4)^*$ and $GF(2^n)^*$. Therefore, the μ for $Tr(\mu) = 1$ and $\mu \in GF(4)^{\perp}$ does not exist. Thus, $\hat{f}(\mu, \nu) \neq 0$ if and only if $Tr(\mu) = 0$. $\hat{f}(0, 0) \neq 0$, so $f(x, y)$ is not balanced. From Definition 3.1, the conclusion follows.

2. Let $f(x, y)$ be the function in Lemma 3.4 2.. From Lemma 3.4 2, $f(x, y) \oplus Tr(\mu x) \oplus \nu y$ is balanced if and only if $u + \mu \notin GF(4)^{\perp}$ and $\mu \notin GF(4)^{\perp}$. That is, $\hat{f}(\mu, \nu) = 0$ if and only if $u + \mu \notin GF(4)^{\perp}$ and $\mu \notin GF(4)^{\perp}$. From Definition 3.1, the conclusion follows. □

In the following, we determine the walsh transforms at all points $(\omega, \varepsilon) \in GF(2^n) \times GF(2)^*$ of the dual function o_f.

Theorem 3.2. *Let $f(x, y)$ be the function defined in Lemma 3.4 1. or 2., then*

$$\hat{o_f}(\omega, \varepsilon) = \begin{cases} -2^{n+1}, & \text{if } (\omega, \varepsilon) = (1, 0); \\ 0, & \text{else.} \end{cases} \tag{3.8}$$

where "1" is the multiplicative identity element on $GF(4)^*$. And, $o_f(\mu, \nu)$ is an affine function.

Proof. The Walsh transform of $o_f(\mu, \nu)$ in Lemma 3.4 is

$$\begin{aligned} \hat{o_f}(\omega, \varepsilon) &= \sum_{\substack{\mu \in GF(2^n) \\ \nu \in GF(2)}} (-1)^{o_f(\mu,\nu) + Tr(\omega\mu) + \varepsilon\nu} \\ &= \sum_{\substack{\mu \in GF(2^n) \\ \nu = 0}} (-1)^{o_f(\mu,0) + Tr(\omega\mu)} + \sum_{\substack{\mu \in GF(2^n) \\ \nu = 1}} (-1)^{o_f(\mu,1) + Tr(\omega\mu) + \varepsilon} \end{aligned} \tag{3.9}$$

$GF(4)^{\perp}$ is a subspace of $GF(2^n)$ and $\#GF(4)^{\perp} = 2^{n-2}$, so we have

$$GF(2^n) = GF(4)^{\perp} \cup \{\alpha_1 + GF(4)^{\perp}\} \cup \{\alpha_2 + GF(4)^{\perp}\} \cup \{\alpha_3 + GF(4)^{\perp}\}, \tag{3.10}$$

where $\alpha_1, \alpha_2, \alpha_3 \in GF(2^n)^*$. And $\alpha_1 + \alpha_2 = \alpha_3$, otherwise Eq. (3.10) does not hold.

$Tr(x) = 0$ for all $x \in GF(4)^{\perp}$, and a linear function $Tr(x)$ is balanced on $GF(2^n)$. From Eq. (3.10) and $Tr(0) = 0$, without loss of generality, it is possible to suppose that $Tr(\alpha_1) = 0, Tr(\alpha_2) = 1, Tr(\alpha_3) = 1$.

If $\mu \in \alpha_1 + GF(4)^{\perp}$, let $\mu = \alpha_1 + \mu'$, where $\mu' \in GF(4)^{\perp}$, then $Tr(\mu) = Tr(\alpha_1 + \mu') = Tr(\alpha_1) \oplus Tr(\mu') = Tr(\alpha_1) = 0$. And, when $\omega \in GF(4)$, $Tr(\omega\mu) = Tr(\omega(\alpha_1 + \mu')) = Tr(\omega\alpha_1) \oplus Tr(\omega\mu') = Tr(\omega\alpha_1)$; In a similar way, we can get if $\mu \in \alpha_2 + GF(4)^{\perp}$, then $Tr(\mu) = Tr(\alpha_2) = 1$, $Tr(\omega\mu) = Tr(\omega\alpha_2)$ when $\omega \in GF(4)$; if $\mu \in \alpha_3 + GF(4)^{\perp}$, then $Tr(\mu) = Tr(\alpha_3) = 1$, $Tr(\omega\mu) = Tr(\omega\alpha_3)$ when $\omega \in GF(4)$.

1. Let $f(x, y)$ be the function defined in Lemma 3.4 *1.*. Suppose $\omega \in GF(4)$, substituting Eq. (3.5) to the right side of Eq. (3.9), we have

$$\sum_{\substack{\mu \in GF(2^n) \\ \nu=0}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)} = \sum_{\substack{\mu \in GF(4)^{\perp} \\ \nu=0}} (-1)^{1+0} + \sum_{\substack{\mu \in \alpha_1 + GF(4)^{\perp} \\ \nu=0}} (-1)^{1+Tr(\omega\alpha_1)} + \sum_{\substack{\mu \in \alpha_2 + GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_2)} + \sum_{\substack{\mu \in \alpha_3 + GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_3)}$$

$$\sum_{\substack{\mu \in GF(2^n) \\ \nu=1}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)+\varepsilon} = \sum_{\substack{\mu \in GF(4)^{\perp} \\ \nu=1}} (-1)^{1+0+\varepsilon} + \sum_{\substack{\mu \in \alpha_1 + GF(4)^{\perp} \\ \nu=0}} (-1)^{1+Tr(\omega\alpha_1)+\varepsilon} + \sum_{\substack{\mu \in \alpha_2 + GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_2)+\varepsilon} + \sum_{\substack{\mu \in \alpha_3 + GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_3)+\varepsilon}$$

Since $\alpha_1 + \alpha_2 = \alpha_3$, $Tr(\alpha_3) = Tr(\alpha_1) \oplus Tr(\alpha_2)$. Let $(\omega, \varepsilon) = (1, 0)$. When $\omega = 1$, $Tr(\omega\alpha_1) = Tr(\alpha_1) = 0$, $Tr(\omega\alpha_2) = Tr(\alpha_2) = 1$, $Tr(\omega\alpha_3) = Tr(\alpha_3) = 1$. Therefore, we have

$$\sum_{\substack{\mu \in GF(2^n) \\ \nu=0}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)} = -2^{n-2} + (-2^{n-2}) + (-2^{n-2}) + (-2^{n-2}) = -2^n,$$

$$\sum_{\substack{\mu \in GF(2^n) \\ \nu=1}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)+\varepsilon} = -2^{n-2} + (-2^{n-2}) + (-2^{n-2}) + (-2^{n-2}) = -2^n.$$

Substituting these into Eq. (3.9), we get $\hat{o_f}(1, 0) = -2^{n+1}$. Thus, $\hat{o_f}(\omega, \varepsilon)$ is not zero only if $(\omega, \varepsilon) = (1, 0)$, else $\hat{o_f}(\omega, \varepsilon) = 0$. Otherwise, Parseval's equation can not been met: $\sum_{\mu \in GF(2^n)} W_f(\mu)^2 = 2^{2n}$ for any Boolean function $f(x)$ on $GF(2^n)$. From the Walsh spectrum of $o_f(\mu, \nu)$, we can have $o_f(\mu, \nu)$ is an affine function.

2. Let $f(x,y)$ be the function in Lemma 3.4 *2.*. $u \notin GF(4)^{\perp}$, so

$$u \in \{\alpha_1 + GF(4)^{\perp}\} \cup \{\alpha_2 + GF(4)^{\perp}\} \cup \{\alpha_3 + GF(4)^{\perp}\}.$$

Suppose $\omega \in GF(4) = \{0, 1, b_1, b_2\}$.

(a) If $u \in \{\alpha_1 + GF(4)^{\perp}\}$, substitutuing Eq. (3.6) to the right side of Eq. (3.9), we have

$$\begin{aligned}\sum_{\substack{\mu\in GF(2^n)\\ \nu=0}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)} &= \sum_{\substack{\mu\in GF(4)^{\perp}\\ \nu=0}} (-1)^{1+0} \\ &+ \sum_{\substack{\mu\in\alpha_1+GF(4)^{\perp}\\ \nu=0}} (-1)^{1+Tr(\omega\alpha_1)} \\ + \sum_{\substack{\mu\in\alpha_2+GF(4)^{\perp}\\ \nu=0}} (-1)^{0+Tr(\omega\alpha_2)} &+ \sum_{\substack{\mu\in\alpha_3+GF(4)^{\perp}\\ \nu=0}} (-1)^{0+Tr(\omega\alpha_3)} \end{aligned} \quad (3.11)$$

$$\begin{aligned}\sum_{\substack{\mu\in GF(2^n)\\ \nu=1}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)+\varepsilon} &= \sum_{\substack{\mu\in GF(4)^{\perp}\\ \nu=1}} (-1)^{1+0+\varepsilon} \\ &+ \sum_{\substack{\mu\in\alpha_1+GF(4)^{\perp}\\ \nu=0}} (-1)^{1+Tr(\omega\alpha_1)+\varepsilon} \\ + \sum_{\substack{\mu\in\alpha_2+GF(4)^{\perp}\\ \nu=0}} (-1)^{0+Tr(\omega\alpha_2)+\varepsilon} &+ \sum_{\substack{\mu\in\alpha_3+GF(4)^{\perp}\\ \nu=0}} (-1)^{0+Tr(\omega\alpha_3)+\varepsilon} \end{aligned} \quad (3.12)$$

Since $\alpha_1 + \alpha_2 = \alpha_3$, $Tr(\omega\alpha_3) = Tr(\omega\alpha_1) \oplus Tr(\omega\alpha_2)$.
Let $(\omega, \varepsilon) = (1, 0)$. If $\omega = 1$, then $Tr(\omega\alpha_1) = Tr(\alpha_1) = 0$, $Tr(\omega\alpha_2) = Tr(\alpha_2) = 1$, $Tr(\omega\alpha_3) = Tr(\alpha_3) = 1$. Therefore,

$$\begin{aligned}\sum_{\substack{\mu\in GF(2^n)\\ \nu=0}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)} &= (-2^{n-2}) + (-2^{n-2}) \\ &+(-2^{n-2}) + (-2^{n-2}) = -2^n,\end{aligned}$$

$$\begin{aligned}\sum_{\substack{\mu\in GF(2^n)\\ \nu=1}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)+\varepsilon} &= (-2^{n-2}) + (-2^{n-2}) \\ &+(-2^{n-2}) + (-2^{n-2}) = -2^n.\end{aligned}$$

Substituting these into Eq. (3.9), we get $\hat{o_f}(1,0) = -2^{n+1}$. From Parseval's equation, $\hat{o_f}(\omega,\varepsilon)$ is not zero only if $(\omega,\varepsilon) = (1,0)$, else $\hat{o_f}(\omega,\varepsilon) = 0$.

(b) If $u \in \{\alpha_2 + GF(4)^{\perp}\}$, by Eq. (3.6), we have

$$\sum_{\substack{\mu \in GF(2^n) \\ \nu=0}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)} = \sum_{\substack{\mu \in GF(4)^{\perp} \\ \nu=0}} (-1)^{1+0} + \sum_{\substack{\mu \in \alpha_1+GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_1)} + \sum_{\substack{\mu \in \alpha_2+GF(4)^{\perp} \\ \nu=0}} (-1)^{1+Tr(\omega\alpha_2)} + \sum_{\substack{\mu \in \alpha_3+GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_3)}$$

$$\sum_{\substack{\mu \in GF(2^n) \\ \nu=1}} (-1)^{o_f(\mu,\nu)+Tr(\omega\mu)+\varepsilon} = \sum_{\substack{\mu \in GF(4)^{\perp} \\ \nu=1}} (-1)^{1+0+\varepsilon} + \sum_{\substack{\mu \in \alpha_1+GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_1)+\varepsilon} + \sum_{\substack{\mu \in \alpha_2+GF(4)^{\perp} \\ \nu=0}} (-1)^{1+Tr(\omega\alpha_2)+\varepsilon} + \sum_{\substack{\mu \in \alpha_3+GF(4)^{\perp} \\ \nu=0}} (-1)^{0+Tr(\omega\alpha_3)+\varepsilon}$$

Similarly, $\hat{o_f}(\omega,\varepsilon)$ is not zero, that is -2^{n+1}, only if $(\omega,\varepsilon) = (1,0)$, else $\hat{o_f}(\omega,\varepsilon) = 0$.

(c) If $u \in \{\alpha_3 + GF(4)^{\perp}\}$, we can also have the same conclusions.

From the Walsh spectrum of $o_f(\mu,\nu)$, we can have $o_f(\mu,\nu)$ is an affine function. □

Let $f : GF(2^n) \to GF(2)$ be a polynomial function with 3-valued spectrum $0, \pm 2^i$. Then there exists a basis of $GF(2^n)$ such that the Boolean representation of $f(x)$ is 1th order correlation immune if and only if o_f is not affine [8]. Therefore, by Theorem 3.2 and equation (3.2), we have the following theorem.

Theorem 3.3. *Let $f(x,y)$ be the function defined in Lemma 3.4 1. or 2., then*

$$\Delta_f(\omega,\varepsilon) = \begin{cases} 2^{n+1}, & \text{if } (\omega,\varepsilon) = (1,0) \text{ or } (0,0); \\ 0, & \text{else.} \end{cases} \tag{3.13}$$

where "1" is the multiplicative identity element on $GF(4)^*$. $\Delta_f = 2^{n+1}$, $\sigma_f = 2 \cdot 2^{2(n+1)}$. And, there exists a basis of $GF(2^n)$ such that the Boolean representation of $f(x,y)$ has not correlation immune.

Remark 3.1. Comparing $\sigma_f = 2 \cdot 2^{2(n+1)}$ with $2^{2(n+1)}$ and $2^{3(n+1)}$, we can see that the sum-of-squares avalanche characteristic of the function is extremely good. However, from Theorem 3.3, we known that the two classes of functions $f(x,y)$ have the worst additive autocorrelation 2^{n+1}. So, $(1,0)$ is their linear structure.

4 Conclusion

We have given all the autocorrelation coefficients of the two classes of semi-bent functions constructed by Charpin et al., and obtain their absolute indicators $\Delta_f = 2^{n+1}$ and sum of square indicators $\sigma_f = 2 \cdot 2^{2(n+1)}$. Our results show that these semi-bent functions have the worst autocorrelation coefficients at nonzero point $(1, 0)$, which make these functions suffer from differential-like cryptanalysis. Therefore, in stream ciphers, these functions can not be used alone. Before using these functions, we have to consider these potential weakness to avoid the differential-like cryptanalysis..

Acknowledgements

This work was supported in part by 973 Project of China (No. 2007CB311201), the Notional Natural Science Foundation(No. 60833008, 60803149), and the Foundation of Guangxi Key Laboratory of Information and Communication(No. 20902).

References

[1] M. Matsui, *Linear cryptanalysis method for DES cipher*, In: Advances in Cryptology-Eurocrypt'93, Springer, Berlin, 1994, 386–397.

[2] T. Siegenthaler, Decrypting a class of stream cipher using ciphertext only, *IEEE Transactions on Computers*, **34(1)**(1985): 81–85.

[3] Y. Tarannikov, P. Korolev and A. Botev, *Autocorrelation coefficients and correlation immunity of Boolean functions*, In: Advances in Cryptology-Asiacrypt'01, Springer, Berlin, 1994, 460–479.

[4] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, **4(1)**(1991): 3–72.

[5] X. M. Zhang and Y. Zheng, GAC-The criterion for global acalanche criteria of cryptographic functions. *Journal for Universal Computer Science*, **1(5)**(1995): 316–333.

[6] H. Eleuch, Quantum Trajectories and Autocorrelation Function in Semiconductor Microcavity, *Appl. Math.Inf. Sci*, **3(2)**(2009): 185–196.

[7] H. Eleuch, Photon statistics of light in semiconductor microcavities, *J. Phys. B: At. Mol. Opt. Phys.* **41**(2008), 055502.

[8] G. Guang and K. Khoongming, *Additive Autocorrelation of Resilient Boolean Functions*, In: Selected Areas in Cryptography 2003, Springer, Berlin, 2004, 275–290.

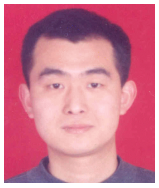
[9] P. Charpin, E. Pasalic and C. Tavernier, On bent and semi-bent quadratic Boolean functions. *IEEE Transactions on Information Theory*, **51(12)**(2005): 4286–4298.

[10] R. J. McEliece, *Finite fields for computer scientists and engineers*, Kluwer Academic Publishers, Dordrecht, 1987.

[11] O. Verta, C. Mastroianni and D. Talia, A super-peer model for resource discovery services in large-scale grids. *Future Generation Computer Systems*, **21(8)**(2005): 1235–1248.
[12] H. Zhuge, *The knowledge grid. singapore*, World Scientific Publishing Co., 2004.
[13] D. Schlessinger and M. Schaechter, *Bacterial toxins*, 2nd ed. Williams and Wilkins, Baltimore, 1993, 162–175.
[14] D. Karger and M. Ruhl, *Simple efficient load balancing algorithms for peer-to-peer systems*, In: Proceedings of the Sixteenth Annual ACM Symposium on Parallelism in Algorithm and Architectures. ACM Press, New York, 2004, 36–43.
[15] P. Charpin, A. Canteaut, C. Carlet and C. Fontaine, *Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions*, In: Advances in Cryptology-EUROCRYPT'2000, LNCS 1807, Springer-Verlag, Berlin, Heidelberg, 2000, 507–522,

Xuelian Li is a Ph.D student at the Department of applied mathematics, Xidian University, Xi'an, China. She is a Lecture in the Department of applied mathematics, Xidian University. She recieved BS degree in mathematics in 2001. In 2004 she earned M.S. (Master of Science) Degree in mathematics from Xidian University. Her research interests include information security and cryptographic functions.

Yupu Hu is a professor in the Xidian University. He received his Master's degree in Probability and Statistics, and received his Ph.D. degrees in cryptography from Xidian University. Currently he serves as a doctoral advisor. His research interests include Information security, Cryptography and Network security.



Juntao Gao is a Doctor in Xidian University, and is a associate professor in the School of Telecommunication and Engineering, Xidian University, Xi'an, China. His Master's and Ph.D. degrees both from Xidian University, all in Cryptography. His research interests include stream cipher, information security, pseudo-random sequences and cryptographic functions.