Proceedings of International Conference
on Cryptology and Information Security

Semi-bent Functions and Strict Uncorrelated Criterion Revisited

Sangwoo Park, Seongtaek Chee, Kwangjo Kim

Section 0710, Electronics and Telecommunications Research Institute
161 Kajong-Dong, Yusong-Gu, Taejon, 305-350, KOREA
E-mail : {psw,chee,kkj}@dingo.etri.re.kr

Abstract

In Asiacrypt'94, Chee et al. proposed a new class of cryptographic primitive, semi-bent functions and discussed a cryptographic relationship between two Boolean functions, strict uncorrelated criterion(SUC). But their functions exist on only odd dimensional vector spaces. And SUC is a very weak condition when we guarantee S(ubstitution)-box to be resistant against differential analysis and linear analysis. In this paper, we define new semi-bent functions which exist on any dimensional vector spaces. Furthermore, we extend the concept of SUC from the relation of two Boolean functions to that of m-tuples of Boolean functions, where $m \geq 2$.

1 Introduction

Cryptographic techniques for information authentication and data encryption require cryptographic strong Boolean functions. In open literatures, various criteria each of which indicates the strength or weakness of cryptographic Boolean functions have been proposed, such as balancedness, nonlinearity, correlation immunity [16] and propagation criterion [10]. Also, several methods for constructing cryptographic good Boolean functions have been proposed in a specific way. Camion *et al.* [3] suggested a recursive method for constructing correlation immune functions. And, Seberry *et al.* [14] proposed a method for constructing highly nonlinear balanced functions which are correlation immune functions. They proved that their method could generate exactly the same set of correlation immune functions as that obtained using Camion *et al.*'s method and analysed the nonlinearity and propagation characteristics of them. However, considering the well-known Parseval's theorem [12], the correlation immune function is not always sufficient solution against correlation attack [16]. From the global point of view, there always exists some correlation between correlation immune functions and some of linear functions. This problem can be solved by introducing bent functions [11]. Bent functions have cryptographic good properties but are not balanced. Meier and Staffelbach [7] proposed a method to randomly select a bent function and to complement an arbitrary set of ones(or zeros) in the truth table of the bent function in order to overcome the unbalancedness of bent functions. Later, their method was extended by Seberry *et al.*'s another result [13]. In [13], the authors proposed systematic methods for constructing highly nonlinear balanced functions satisfying the propagation criterion using bent functions. But they did not mention correlation property of the functions which they constructed. In [5], Chee *et al.* proposed another method for constructing Boolean functions, using bent functions and call the functions constructed by their methods, semi-bent functions. Semi-bent functions are balanced, have the maximal nonlinearity that balanced functions could obtained, exhibit almost uniform correlation values to all linear functions, and satisfy the propagation criterion. But they exist on only odd dimensional vector spaces. In the same paper, they proposed strict uncorrelated criterion(SUC), which is a cryptographic relationship between two Boolean functions [5]. But, this criterion is a very weak condition in a sense that we have to consider cryptographic properties for all linear combinations of component functions when designing an S-box.

In this paper, we define new semi-bent functions by using Walsh-Hadamard transformation of functions. That is, semi-bent functions are functions which have specific values of Walsh-Hadamard transformation. In that way, we can define semi-bent functions on any dimensional vector spaces. Semi-bent functions which are defined in this paper has the same cryptographic properties as Chee *et al.*'s. We also present methods for constructing semi-bent functions. The definition of semi-bent functions in [5] is considered to be a method for constructing our semi-bent functions on odd dimensional vector spaces. A new method for constructing them on even dimensional vector spaces is proposed. And, we extend the concept of SUC from the relationship of two Boolean functions to that of m-tuples of Boolean functions, $m \geq 2$. Also, we present an example of m-tuples of semi-bent functions fulfilling SUC.

The organization of the rest of this paper is as follows : Section 2 introduces basic notions, definitions of essential criteria for cryptographic Boolean functions and useful tools obtained by Walsh-Hadamard transformation to analyse Boolean functions. After restating the previous results of semi-bent functions in section 3, we define new semi-bent functions by using Walsh-Hadamard transformation and analyse their cryptographic properties in section 4. In section 5, we present two methods for constructing them. Also, we present the propagation characteristic of semi-bent

functions according to their construction methods, in the same section. In section 6, we discuss the concept of SUC and its cryptographic significance. Finally, we make some concluding remarks.

2 Preliminary

We first introduce basic notions, definitions of essential criteria for cryptographic Boolean functions and useful tools obtained by Walsh-Hadamard transformation to analyse Boolean functions.

Denote by Z_2^n the vector space of n tuples of elements from $Z_2 = \{0, 1\}$. Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ be two vectors in Z_2^n. The scalar product of $\mathbf{x}$ and $\mathbf{y}$, denoted by $(\mathbf{x}, \mathbf{y})$, is defined by $(\mathbf{x}, \mathbf{y}) = x_1 y_1 \oplus \cdots \oplus x_n y_n$, where multiplication and addition are over Z_2. A Boolean function f is a function whose domain is Z_2^n and takes the value 0 or 1. The set of all Boolean functions on Z_2^n will be denoted as $\mathcal{B}_n$. A Boolean function f is said to be affine if there exist a vector $\mathbf{w} \in Z_2^n$ and $c \in Z_2$ such that $f(\mathbf{x}) = l_{\mathbf{w}}(\mathbf{x}) \oplus c = (\mathbf{x}, \mathbf{w}) \oplus c = x_1 w_1 \oplus \ldots \oplus x_n w_n \oplus c$. In particular, f will be called linear if $c = 0$. The set of all affine functions and linear functions on Z_2^n will be denoted by $\mathcal{A}_n$ and $\mathcal{L}_n$, respectively. The Hamming weight of a vector $\mathbf{x} \in Z_2^n$, denoted by $wt(\mathbf{x})$, is the number of ones in $\mathbf{x}$ and the Hamming weight of $f \in \mathcal{B}_n$, $wt(f)$, is the number of function values equal to one. The Hamming distance $d(f, g)$ between two functions f and g is the number of function values in which they differ. If $wt(\mathbf{x}) = 1$, then $\mathbf{x}$ is called a unit vector. Let $f \oplus g$ be a function on Z_2^n obtained by bit-wise exclusive-or of two function values of f and g, and $f||g$ be a function on Z_2^{n+1} whose truth table is the concatenation of the truth tables of f and g. That is, $(f \oplus g)(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x})$ and $(f||g)(\mathbf{x}^*) = (f||g)(\mathbf{x}, x_{n+1}) = (1 \oplus x_{n+1}) f(\mathbf{x}) \oplus x_{n+1} g(\mathbf{x})$. Now we introduce the definition of Walsh-Hadamard transformation [10].

Definition 1 *For $f \in \mathcal{B}_n$, the Walsh-Hadamard transformation $\hat{\mathcal{F}}_f : Z_2^n \longrightarrow \mathcal{R}$ of $\hat{f}$, is defined as*

$$\hat{\mathcal{F}}_f(\mathbf{w}) = \sum_{\mathbf{x} \in Z_2^n} \hat{f}(\mathbf{x}) \cdot (-1)^{(\mathbf{w}, \mathbf{x})},$$

where $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$ and $\mathcal{R}$ is a set of all real numbers.

The balancedness is basically required to guarantee good statistical properties of cryptographic Boolean functions [10].

Definition 2 *For $f \in \mathcal{B}_n$, if $\#\{\mathbf{x} \in Z_2^n | f(\mathbf{x}) = 0\} = \#\{\mathbf{x} \in Z_2^n | f(\mathbf{x}) = 1\}$, then f is balanced.*

Lemma 1 *For $f \in \mathcal{B}_n$, f is balanced if and only if $\hat{\mathcal{F}}_f(\mathbf{0}) = 0$.*

The next definition is usually called nonlinearity that indicates the Hamming distance between a function and all affine functions [10].

Definition 3 *The nonlinearity of $f \in \mathcal{B}_n$, denoted by $\mathcal{N}_f$, is the minimal Hamming distance between f and all affine functions on Z_2^n, i.e.,*

$$\mathcal{N}_f = \min_{\lambda_n \in \mathcal{A}_n} d(f, \lambda_n).$$

High nonlinearity is essential to design DES-like block encryption algorithms, because linear cryptanalysis, put forward by Matsui [6], can be applied in attacking FEAL and DES whose S-boxes have low nonlinearity. An S-box is immune to linear cryptanalysis if the nonlinearity of each nonzero linear combination of its component functions is high enough [15].

Lemma 2 *For $f \in \mathcal{B}_n$,*

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{\mathbf{w} \in Z_2^n} |\hat{\mathcal{F}}_f(\mathbf{w})|.$$

In most stream ciphers, nonlinear Boolean functions play an important role for combining the output of linear feedback shift registers. In order to immunize them against a correlation attack [16], the Boolean functions must be well chosen. Siegenthaler [16], for the first time, introduced a correlation immune function.

Definition 4 *A function $f \in \mathcal{B}_n$ is said to be m-th order correlation immune, $1 \le m \le n$, if*

$$d(f, l_{\mathbf{w}}) = 2^{n-1}$$

holds for any $\mathbf{w} \in Z_2^n$ with $1 \le wt(\mathbf{w}) \le m$. Furthermore, the correlation value between f and g is defined by

$$c(f, g) = 1 - \frac{d(f, g)}{2^{n-1}}.$$

The propagation criterion is an extended concept of the strict avalanche criterion [10].

Definition 5 *A function $f \in \mathcal{B}_n$ satisfies the propagation criterion(PC) with respect to a non-zero $\alpha \in Z_2^n$, if*

$$\sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \alpha) = 2^{n-1}.$$

f satisfies the propagation criterion of degree k($PC(k)$), if it satisfies the propagation criterion with respect to all $\alpha \in Z_2^n$ such that $1 \le wt(\alpha) \le k$.

Definition 6 *For $f \in \mathcal{B}_n$, the autocorrelation function $\hat{\mathcal{A}}_f : Z_2^n \longrightarrow \mathcal{R}$ of $\hat{f}$, is defined as*

$$\hat{\mathcal{A}}_f(\mathbf{s}) = \sum_{\mathbf{x} \in Z_2^n} \hat{f}(\mathbf{x}) \cdot \hat{f}(\mathbf{x} \oplus \mathbf{s}).$$

For $f_0, f_1 \in \mathcal{B}_n$, the crosscorrelation function $\hat{\mathcal{C}}_{f_0, f_1} : Z_2^n \longrightarrow \mathcal{R}$ of $\hat{f}_0$ and $\hat{f}_1$, is defined as

$$\hat{\mathcal{C}}_{f_0, f_1}(\mathbf{s}) = \sum_{\mathbf{x} \in Z_2^n} \hat{f}_0(\mathbf{x}) \cdot \hat{f}_1(\mathbf{x} \oplus \mathbf{s}).$$

Lemma 3 *[10] For $f_0, f_1 \in \mathcal{B}_n$, we have*

$$\hat{C}_{\hat{f}_0,\hat{f}_1}(\mathbf{s}) = \frac{1}{2^n}\sum_{\mathbf{w}\in Z_2^n} \hat{\mathcal{F}}_{\hat{f}_0}(\mathbf{w})\cdot\hat{\mathcal{F}}_{\hat{f}_1}(\mathbf{w})\cdot(-1)^{(\mathbf{s},\mathbf{w})}.$$

Lemma 4 *[10] Let $f \in \mathcal{B}_n$. Then f satisfies $PC(k)$ if and only if*

$$\hat{\mathcal{A}}_{\hat{f}}(\mathbf{s}) = 0$$

holds for all $\mathbf{s} \in Z_2^n$ with $1 \le wt(\mathbf{s}) \le k$.

Theorem 1 (Parseval's Theorem) *For $f \in \mathcal{B}_n$, we have*

$$\sum_{\mathbf{w}\in Z_2^n} \hat{\mathcal{F}}_{\hat{f}}^2(\mathbf{w}) = 2^{2n}$$

Now we introduce the bent function which is an important combinatorial concept introduced by Rothaus [11].

Definition 7 *A function $f \in \mathcal{B}_n$ is called a bent function if*

$$|\hat{\mathcal{F}}_{\hat{f}}(\mathbf{w})| = 2^{\frac{n}{2}},$$

for any $\mathbf{w} \in Z_2^n$.

From this definition, it can be seen that bent functions on Z_2^n exist only when n is even. Another fact is that bent functions are not balanced. Bent function $f \in \mathcal{B}_n$ satisfies $PC(n)$ and has uniform correlation values to all linear functions, i.e., for any $\mathbf{w} \in Z_2^n$, the correlation value between f and $l_{\mathbf{w}}$ is $\pm 2^{-\frac{n}{2}}$. And the nonlinearity of bent functions is $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. In view of propagation characteristic, correlation immunity and nonlinearity, bent functions have ideal cryptographic properties but, since bent functions are not balanced and exist only on the even dimensional vector spaces, they are not directly applicable in most computer and communications security practices.

For $f \in \mathcal{B}_n$, its Walsh-Hadamard transformation and autocorrelation function are very useful tools to analyse its cryptographic behavior by employing the affine transformation of $\mathbf{x}$ and an addition of an affine function to $f(\mathbf{x})$ [10].

Theorem 2 *For $f \in \mathcal{B}_n, \mathbf{a}, \mathbf{b} \in Z_2^n, c \in Z_2$ and $n \times n$ nonsingular matrix A, define $g \in \mathcal{B}_n$ by*

$$g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{a}) \oplus l_{\mathbf{b}}(\mathbf{x}) \oplus c.$$

Then we have

$$\hat{\mathcal{F}}_{\hat{g}}(\mathbf{w}) = (-1)^c(-1)^{(A^{-1}\mathbf{a},\mathbf{w}\oplus\mathbf{b})}\hat{\mathcal{F}}_{\hat{f}}((A^{-1})^t(\mathbf{w}\oplus\mathbf{b}))$$

and

$$\hat{\mathcal{A}}_{\hat{g}}(\mathbf{s}) = (-1)^{(\mathbf{s},(A^{-1})^t\mathbf{b})}\hat{\mathcal{A}}_{\hat{f}}(A\mathbf{s}).$$

Theorem 3 *For $f_0, f_1 \in \mathcal{B}_n, \mathbf{w}^*, \mathbf{s}^* \in Z_2^{n+1}$ and $\mathbf{w}, \mathbf{s} \in Z_2^n$, let $g = f_0||f_1$, then we have*

$$\hat{\mathcal{F}}_{\hat{g}}(\mathbf{w}^*) = \hat{\mathcal{F}}_{\hat{f}_0}(\mathbf{w}) + (-1)^{w_{n+1}}\hat{\mathcal{F}}_{\hat{f}_1}(\mathbf{w})$$

and

$$\hat{\mathcal{A}}_{\hat{g}}(\mathbf{s}^*) = \begin{cases} \hat{\mathcal{A}}_{\hat{f}_0}(\mathbf{s}) + \hat{\mathcal{A}}_{\hat{f}_1}(\mathbf{s}) & \text{if } s_{n+1} = 0 \\ 2\cdot\hat{C}_{\hat{f}_0,\hat{f}_1}(\mathbf{s}) & \text{if } s_{n+1} = 1. \end{cases}$$

3 Previous Semi-bent functions

Chee *et al.* [5] proposed a new method for constructing new class of Boolean functions, using bent functions. Their construction method is as follows : Let $f_0 \in \mathcal{B}_{2n}$ be a bent function, $\mathbf{a} \in Z_2^{2n}$ and A be a $2n \times 2n$ nonsingular matrix. Define $f_1 \in \mathcal{B}_{2n}$ by

$$f_1(\mathbf{x}) = f_0(A\mathbf{x} \oplus \mathbf{a}) \oplus 1.$$

Then the concatenation of f_0 and f_1 results in a new Boolean function, namely,

$$g = f_0||f_1$$

and such a function $g \in \mathcal{B}_{2n+1}$ is called by semi-bent function. Semi-bent functions have cryptographic good properties but they exist on only odd dimensional vector spaces. In the following theorem, cryptographic properties of semi-bent functions are summarized.

Theorem 4 *[5] Let $g \in \mathcal{B}_{2n+1}$ be a semi-bent function. Then g has the following properties.*

1) g is balanced.

2) $\mathcal{N}_g = 2^{2n} - 2^n$

3) For any $\mathbf{w}^* \in Z_2^{2n+1}$, the correlation value between g and $l_{\mathbf{w}^*}$ is 0 or $\pm 2^{-n}$. And, $\#\{\mathbf{w}^* \in Z_2^{2n+1} | c(g, l_{\mathbf{w}^*}) = 0\}$ and $\#\{\mathbf{w}^* \in Z_2^{2n+1} | c(g, l_{\mathbf{w}^*}) = \pm 2^{-n}\}$ equal to 2^{2n}.

4) g satisfies the PC with respect to all non-zero $\mathbf{s}^* \in Z_2^{2n+1}$, with $s_{2n+1} = 0$.

5) If A is a $2n \times 2n$ identity matrix, g satisfies the PC with respect to all non-zero $\mathbf{s}^* \in Z_2^{2n+1}$ with $\mathbf{s} \neq \mathbf{a}$.

6) If A is a $2n \times 2n$ identity matrix and $\mathbf{a} = (1, \ldots, 1)$, g satisfies $PC(2n)$.

4 Semi-bent functions

Now, we define new semi-bent functions by using Walsh-Hadamard transformation of functions. Chee *et al.*'s semi-bent functions are examples of our semi-bent functions.

Definition 8 *For $f \in \mathcal{B}_n$, if $|\hat{\mathcal{F}}_f(\mathbf{w})| = 0$ or $2^{\lfloor \frac{n}{2} \rfloor + 1}$, and $\hat{\mathcal{F}}_f(\mathbf{0}) = 0$, then we call f semi-bent function, where $\lfloor m \rfloor$ means the largest integer less than or equal to m.*

In the rest of this paper, semi-bent functions mean functions defined by definition 8 unless otherwise stated. We analyse their basic cryptographic properties include balancedness, nonlinearity and correlation immunity.

Theorem 5 *Let $f \in \mathcal{B}_n$ be a semi-bent function. Then f has the following properties.*

1) f is balanced.

2) $\mathcal{N}_f = 2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$.

3) For any $\mathbf{w} \in Z_2^n$, the correlation value between f and $l_{\mathbf{w}}$ is 0 or $\pm 2^{-\frac{n-2+(n \bmod 2)}{2}}$, and $\#\{\mathbf{w} \in Z_2^n | c(f, l_{\mathbf{w}}) = \pm 2^{-\frac{n-2+(n \bmod 2)}{2}}\} = 2^{n-2+(n \bmod 2)}$.

Proof.

1) Trivial.

2) By lemma 2, if $n = 2k+1$,

$$2^{(2k+1)-1} - \frac{1}{2} \cdot 2^{k+1} = 2^{2k} - 2^k,$$

and, if $n = 2k+2$,

$$2^{(2k+2)-1} - \frac{1}{2} \cdot 2^{k+2} = 2^{2k+1} - 2^{k+1}.$$

3) If $n = 2k+1$, for any $\mathbf{w} \in Z_2^n$,

$$c(f, l_{\mathbf{w}}) = \frac{\hat{\mathcal{F}}_f(\mathbf{w})}{2^{2k+1}} = \frac{0 \text{ or } \pm 2^{k+1}}{2^{2k+1}} = 0 \text{ or } \pm 2^{-k}$$

and let N_1 be the number of $\mathbf{w} \in Z_2^{2k+1}$ such that $c(f, l_{\mathbf{w}}) = \pm 2^{-k}$, then, by Parseval's theorem, $N_1 = 2^{2k}$.
If $n = 2k+2$, then, for any $\mathbf{w} \in Z_2^n$,

$$c(f, l_{\mathbf{w}}) = \frac{\hat{\mathcal{F}}_f(\mathbf{w})}{2^{2k+2}} = \frac{0 \text{ or } \pm 2^{k+2}}{2^{2k+2}} = 0 \text{ or } \pm 2^{-k}$$

and let N_2 be the number of $\mathbf{w} \in Z_2^{2k+2}$ such that $c(f, l_{\mathbf{w}}) = \pm 2^{-k}$, then, by Parseval's theorem, $N_2 = 2^{2k}$.

□

By theorem 5, if $f \in \mathcal{B}_{2k+1}$ is a semi-bent function, then $\mathcal{N}_f = 2^{2k} - 2^k$. Pieprzyk and Finkelstein [9] claimed that this is the maximal nonlinearity that balanced Boolean functions in $\mathcal{B}_{2k+1}$ could have. And if $f \in \mathcal{B}_{2k+2}$ is a semi-bent function, then $\mathcal{N}_f = 2^{2k+1} - 2^{k+1}$ and it is known that this nonlinearity is the maximal value that balanced Boolean functions in $\mathcal{B}_{2k+2}$ could have [1]. And semi-bent function f has almost uniform correlation values in the sense that if $f \in \mathcal{B}_{2k+1}$, then f is correlation immune to the half of all linear functions and uniform correlation values to the others, and if $f \in \mathcal{B}_{2k+2}$, then f is correlation immune to three quaters of all linear functions and uniform correlation values to the others.

5 Construction Methods and PC characteristics

In this section, we suggest two methods for constructing semi-bent functions in definition 8. First, we restate the previous Chee *et al.*'s method [5].

Method 1 *Let $f_0 \in \mathcal{B}_{2k}$ be a bent function, $\mathbf{a} \in Z_2^{2k}$ and A be a $2k \times 2k$ nonsingular matrix. Define $f_1 \in Z_2^{2k}$ by*

$$f_1(\mathbf{x}) = f_0(A\mathbf{x} \oplus \mathbf{a}) \oplus 1,$$

and $g \in \mathcal{B}^{2k+1}$ by

$$g = f_0 || f_1 \tag{1}$$

By theorems 2 and 3,

$$\begin{aligned} |\hat{\mathcal{F}}_{\hat{g}}(\mathbf{w}^*)| &= |\hat{\mathcal{F}}_{\hat{f}_0}(\mathbf{w}) + (-1)^{w_{2k+1}} \hat{\mathcal{F}}_{\hat{f}_1}(\mathbf{w})| \\ &= |\pm 2^k \mp (-1)^{((A^{-1})^t \mathbf{a}, \mathbf{w})} 2^k| \\ &= 0 \text{ or } 2^{k+1} \\ &= 0 \text{ or } 2^{\lfloor \frac{n}{2} \rfloor + 1}. \end{aligned}$$

and $\hat{\mathcal{F}}_{\hat{g}}(\mathbf{0}) = 0$. Thus a function g constructed by Method 1 is a semi-bent function on Z_2^{2k+1}. We search all semi-bent functions on Z_2^5, exhaustively, i.e., all balanced functions on Z_2^5 whose Walsh-Hadamard transformation values are 0 or ± 8. And, we generate all semi-bent functions on Z_2^5 by Method 1. Table 1 describes the number of semi-bent functions on Z_2^5. We can see that there are many semi-bent functions of the different form from the functions defined in (1). Next, we suggest a method for generating semi-bent functions on the even dimensional vector spaces.

Table 1: The number of semi-bent functions on Z_2^5

exhaustive search	constructed by Method 1
$7,027,328 = 2^{22.75}$	$172,032 = 2^{17.39}$

Method 2 *Let $g_0 \in \mathcal{B}_{2k+1}$ be a semi-bent function obtained by (1) and $\mathbf{a}^* \in Z_2^{2k+1}$. Define $g_1 \in \mathcal{B}_{2k+1}$ by*

$$g_1(\mathbf{x}^*) = g_0(\mathbf{x}^* \oplus \mathbf{a}^*) \oplus 1,$$

and $h \in \mathcal{B}_{2k+2}$ by

$$h = g_0 || g_1. \tag{2}$$

By theorems 2 and 3,

$$\begin{aligned}
&\hat{\mathcal{F}}_{\hat{h}}(\mathbf{w}^{**}) \\
&= \hat{\mathcal{F}}_{\hat{g}_0}(\mathbf{w}^*)+(-1)^{w_{2k+2}}\hat{\mathcal{F}}_{\hat{g}_1}(\mathbf{w}^*) \\
&= \hat{\mathcal{F}}_{\hat{g}_0}(\mathbf{w}^*)+(-1)^{w_{2k+2}}\cdot(-1)\cdot(-1)^{(\mathbf{a}^*,\mathbf{w}^*)}\hat{\mathcal{F}}_{\hat{g}_0}(\mathbf{w}^*),
\end{aligned}$$

for any $\mathbf{w}^{**} \in Z_2^{2k+2}$. Since $|\hat{\mathcal{F}}_{\hat{g}_0}(\mathbf{w}^*)| = 0$ or 2^{k+1}, $|\hat{\mathcal{F}}_{\hat{h}}(\mathbf{w}^{**})| = 0$ or $2^{k+2} = 0$ or $2^{\lfloor\frac{n}{2}\rfloor}+1$, and $\hat{\mathcal{F}}_{\hat{h}}(\mathbf{0}) = 0$. Therefore, h is a semi-bent function on Z_2^{2k+2}.

We now discuss PC characteristics of semi-bent functions defined in (1) and (2). The PC characteristics of functions defined in (1) has already been in 4),5) and 6) of theorem 4. In the case of function $h \in \mathcal{B}_{2k+2}$ defined in (2), the situation is somewhat different. Let $\mathbf{s}^{**} = (\mathbf{s}^*, s_{2k+2}) = (\mathbf{s}, s_{2k+1}, s_{2k+2})$ be a non-zero element in Z_2^{2k+2}. If $s_{2k+1} = s_{2k+2} = 0$, then by theorems 2 and 3, we have

$$\begin{aligned}
\mathcal{A}_{\hat{h}}(\mathbf{s}^{**}) &= \mathcal{A}_{\hat{g_0}}(\mathbf{s}^*)+\mathcal{A}_{\hat{g_1}}(\mathbf{s}^*) \\
&= \mathcal{A}_{\hat{g_0}}(\mathbf{s}^*)+(-1)^{(\mathbf{s}^*,0)}\mathcal{A}_{\hat{g_0}}(\mathbf{s}^*).
\end{aligned}$$

Since $s_{2k+1} = 0$, $\mathcal{A}_{\hat{g_0}}(\mathbf{s}^*) = 0$ by 4) of theorem 4, and hence $\mathcal{A}_{\hat{h}}(\mathbf{s}^{**}) = 0$. It gives us the following :

Theorem 6 *Let $h \in \mathcal{B}_{2k+2}$ be a semi-bent function defined in (2) with the $2k\times 2k$ identity matrix A. Then h satisfies the PC with respect to all non-zero $\mathbf{s}^{**} \in Z_2^{2k+2}$ with $s_{2k+1} = s_{2k+2} = 0$.*

Functions satisfying PC for all but one nonzero point is useful, and those functions are used in defining the SUC, which will be defined in the next section. In the even dimensional vector spaces, however, it seems too difficult to find such a specific function. But if we consider points with their most significant bits are '1', we have the following :

Theorem 7 *Let $h \in \mathcal{B}_{2k+2}$ be a semi-bent function defined in (2). Then h satisfies PC with respect to all $\mathbf{s}^{**} \in Z_2^{2k+2}$ with $s_{2k+2} = 1$ and $\mathbf{s}^* \neq \mathbf{a}^*$.*

Proof. Let $\mathbf{s}^{**} = (\mathbf{s}^*, s_{2k+2})$ be an element in Z_2^{2k+2} with $s_{2k+2} = 1$ and $\mathbf{s}^* \neq \mathbf{a}^*$. By lemma 3, and theorems 2 and 3, we have

$$\begin{aligned}
&\mathcal{A}_{\hat{h}}(\mathbf{s}^{**}) \\
&= 2\cdot\hat{\mathcal{C}}_{\hat{g}_0,\hat{g}_1}(\mathbf{s}^*) \\
&= \frac{1}{2^{2k}}\sum_{\mathbf{w}^*\in Z_2^{2n+1}}\hat{\mathcal{F}}_{\hat{g}_0}(\mathbf{w}^*)\cdot\hat{\mathcal{F}}_{\hat{g}_1}(\mathbf{w}^*)\cdot(-1)^{(\mathbf{s}^*,\mathbf{w}^*)} \\
&= -\frac{1}{2^{2k}}\sum_{\mathbf{w}^*\in Z_2^{2n+1}}\hat{\mathcal{F}}^2_{\hat{g}_0}(\mathbf{w}^*)\cdot(-1)^{(\mathbf{a}^*\oplus\mathbf{s}^*,\mathbf{w}^*)} \\
&= 0.
\end{aligned}$$

□

If we let the matrix A by the identity matrix and $s_{2k+2} = 0$, then by 5) of theorem 4, for all non-zero $\mathbf{s}^* \in Z_2^{2k+1}$ with $\mathbf{s} \neq \mathbf{a}$, $\mathcal{A}_{\hat{g_0}}(\mathbf{s}^*) = 0$. Thus, $\mathcal{A}_{\hat{h}}(\mathbf{s}^{**}) = 0$. Hence we have the following :

Theorem 8 *Let $h \in \mathcal{B}_{2k+2}$ be a semi-bent function defined in (2) with the $2k\times 2k$ identity matrix A. Then h satisfies the PC with respect to all $\mathbf{s}^{**} \in Z_2^{2k+2}$ with $s_{2k+2} = 0$ and $\mathbf{s} \neq \mathbf{a}$.*

6 Strict Uncorrelated Criterion

Biham and Shamir introduced differential cryptanalysis to attack DES-like cryptosystems [2]. Let $F = (f_1, f_2, \ldots, f_m)$ be an m-tuples of Boolean functions, where $f_i \in \mathcal{B}_n, i = 1, 2, \ldots, m, m \geq 2$. If we use the differential cryptanalysis to cryptanalyse F, we need to compute non-empty sets :

$$\mathcal{D}_F(\mathbf{a}, \mathbf{b}) = \{\mathbf{x} \in Z_2^n | F(\mathbf{x}\oplus\mathbf{a})\oplus F(\mathbf{x}) = \mathbf{b}\},$$

where, $\mathbf{a} \in Z_2^n - \{0\}$ and $\mathbf{b} \in Z_2^m$. The efficiency of differential cryptanalysis based upon a set $\mathcal{D}_F(\mathbf{a}, \mathbf{b})$ is measured by its cardinality

$$\delta_F(\mathbf{a}, \mathbf{b}) = \#\mathcal{D}_F(\mathbf{a}, \mathbf{b}).$$

Hence the resistance of the function F against differential cryptanalysis can be measured by $\Delta(F) = \max\delta_F(\mathbf{a}, \mathbf{b})$ and if $\Delta(F)$ is minimal, F is said to be differential resistant [4]. If all linear combinations of component functions in F are balanced and satisfy PC(1), then $\delta_F(\mathbf{a}, \mathbf{b})$ can be minimized, where $wt(\mathbf{a}) = 1$. And if all linear combinations of component functions in F are balanced and satisfy PC of higher degree then $\delta_F(\mathbf{a}, \mathbf{b})$ can be minimized, for all $\mathbf{a} \in Z_2^n$ for which all linear combinations of component functions satisfy PC. So, when designing S-box, it is necessary to consider the cryptographic relations of all linear combinations of component functions in S-box.

In [5], authors proposed a concept of cryptographic relationship between two Boolean functions, SUC, which gives totally output uncorrelatedness between two Boolean functions when one of input bits is changed. The definition they proposed is as follow : Two functions f and g in $\mathcal{B}_n$ are said to satisfy the strict uncorrelated criterion(SUC) if f, g and $f \oplus g$ are all balanced and satisfy $PC(1)$. But SUC is a very weak condition because the degree of PC under consideration is only 1 and SUC is defined over a relationship between only two Boolean functions. So, in order to make SUC more meaningful against differential cryptanalysis, it is necessary to extend the number of Boolean functions from 2 to m as many as possible and the degree of PC from 1 to k as high as possible. But, extending the degree of PC has some limitations, because the degree of the PC of a balanced Boolean function in $\mathcal{B}_n$ is depends on the value of the integer n. So, we define SUC as follow :

Definition 9 *Let $F = (f_1, f_2, \ldots, f_m)$ be an m-tuples of Boolean functions, where $f_i \in \mathcal{B}_n, i = 1, 2, \ldots, m, m \geq 2$. If all linear combinations of f_i in F are balanced and satisfy PC for all but nonzero one point, then F satisfies $SUC(n, m)$.*

If F satisfies SUC(n,m), $\delta_F(\mathbf{a},\mathbf{b})$ could be close to uniform, where $\mathbf{a} \in Z_2^n - \{0\}$ and $\mathbf{b} \in Z_2^m$. This means that $\Delta(F)$ approaches to the minimal value. We find an example of F satisfying SUC(n,m) by computer search, where n=m=5 and each component function of F is a semi-bent functions.

Example 1 *Let*

$$\begin{aligned}
f_1(\mathbf{x}) &= x_1 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_5 \\
f_2(\mathbf{x}) &= x_1x_2 \oplus x_3 \oplus x_4 \oplus x_1x_4 \oplus x_5 \oplus x_4x_5 \\
f_3(\mathbf{x}) &= x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_5 \oplus x_1x_5 \oplus x_3x_5 \\
&\quad \oplus x_4x_5 \\
f_4(\mathbf{x}) &= x_2 \oplus x_3 \oplus x_4 \oplus x_3x_4 \oplus x_5 \oplus x_1x_5 \oplus x_3x_5 \\
f_5(\mathbf{x}) &= x_1x_3 \oplus x_2x_3 \oplus x_4 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_5 \\
&\quad \oplus x_2x_5 \oplus x_3x_5 \oplus x_4x_5,
\end{aligned}$$

where $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) \in Z_2^5$. *Then,* $F = (f_1, f_2, f_3, f_4, f_5)$ *satisfies SUC*$(5,5)$ *and each* $f_i \in \mathcal{B}_5, i = 1, 2, \ldots 5$ *is a semi-bent function. Futhermore, differential uniformity* $\Delta(F)$ *of* F *equals to 2, so,* F *is differential resistant.*

If n is even, it is not easy to find F satisfying SUC(n,n). In fact, for even m=n, the minimum differential uniformity is unknown and it was shown that, for even m=n, there is no quadratic permutation whose differential uniformity is 2 [15]. Also, it was shown that, for m=n even, there is no permutation with partially bent components whose differential uniformity is 2 [8]. In the context of these results, it may be hard problem to find F which satisfies SUC(n,n) for even n. So, for even n, it may be preferable to consider SUC(n,m) where $m < n$, for example, $m \leq \frac{n}{2}$.

7 Conclusions

We proposed a new class of cryptographic Boolean functions which are highly nonlinear balanced functions with 2-valued correlations to linear functions and satisfy the propagation criterion. Our semi-bent functions have the same cryptographic properties as Chee *et al.*'s functions in [5], but our functions exist on any dimensional vector spaces while their functions exist on only odd dimensional vector spaces. In fact, Chee *et al*'s definition is considered to be a method by which we can construct semi-bent functions on odd dimensional vector spaces. And, we extended the concept of SUC from the relationship of two Boolean functions to that of m-tuples of Boolean functions, $m \geq 2$. Also, we presented an example of m-tuples of semi-bent functions in $\mathcal{B}_5$ fulfilling SUC$(5,5)$. Furthermore, the differential uniformity of this example is found to be 2.

A future research direction is to find the largest m such that m-tuples of semi-bent functions fulfilling SUC(n,m), for even n, m. Another directions are to design construction methods to generate all semi-bent functions in $\mathcal{B}_n$ and to show the relation between m-tuples of Boolean functions fulfilling SUC(n,m) and its differential resistance. Also, we will add the concept of nonlinearity in defining the SUC because the property of PC of an S-box not sufficient to the linear cryptanalysis.

References

[1] Carlisle M. Adams and Stafford E. Tavares. The structured design of cryptographically good S-boxes. *Journal of Cryptology*, volume 3, number 1, pages 27–41, 1990.

[2] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, volume 4, number 1, pages 3–72, 1991.

[3] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In Joan Feigenbaum, editor, *Advances in Cryptology: CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 86–100. Springer-Verlag, Berlin, 1992.

[4] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Alfredo De Santis, editor, *Advances in Cryptology: EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365. Springer-Verlag, Berlin, 1995.

[5] Seongtaek Chee, Sangjin Lee, and Kwangjo Kim. Semi-bent functions. In Josef Pieprzyk, editor, *Advances in Cryptology: ASIACRYPT'94*, volume 917 of *Lecture Notes in Computer Science*, pages 107–118. Springer-Verlag, Berlin, 1995.

[6] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology: EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, 1994.

[7] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In J. J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology: EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, 1990.

[8] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, *Fast Software Encryption : Second International Workshop*, volume 1008 of *Lecture Notes in Computer Science*, pages 111–130. Springer-Verlag, Berlin, 1995.

[9] J. Pieprzyk and G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEE Proceedings, Part E : Computers and Digital Techniques*, volume 135, pages 325–335, 1988.

[10] Bart Preneel. *Analysis and Design of Cryptographic Hash Functions.* Ph.D thesis, Katholieke Universiteit Leuven, 1993.

[11] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory(A)*, volume 20, pages 300–305, 1976.

[12] Rainer A. Rueppel. Stream ciphers. In Gustavus J. Simmons, editor, *Contemporary Cryptology : The Science of Information Integrity*, chapter 2, pages 65–134. IEEE Press, 1992.

[13] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Nonlinearly balanced boolean functions and their propagation characteristics. In Douglas R. Stinson, editor, *Advances in Cryptology - CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 49–60. Springer-Verlag, New York, 1994.

[14] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. On constructions and nonlinearity of correlation immune functions. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 181–199. Springer-Verlag, Berlin, 1994.

[15] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Relationships among nonlinearity criteria(extended abstract). In Alfredo De Santis, editor, *Advances in Cryptology: EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 376–388. Springer-Verlag, Berlin, 1995.

[16] T. Siegenthaler. Correlation immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, volume IT-30, number 5, pages 776–780, September 1984.