PAPER

Relationships among Nonlinearity Criteria of Boolean Functions

Shouichi HIROSE[†] *and* **Katsuo IKEDA**[†], *Members*

SUMMARY For symmetric cryptosystems, their transformations should have nonlinear elements to be secure against various attacks. Several nonlinearity criteria have been defined and their properties have been made clear. This paper focuses on, among these criteria, the propagation criterion (PC) and the strict avalanche criterion (SAC), and makes a further investigation of them. It discusses the sets of Boolean functions satisfying the PC of higher degrees, the sets of those satisfying the SAC of higher orders and their relationships. We give a necessary and sufficient condition for an n-input Boolean function to satisfy the PC with respect to a set of all but one or two elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. From this condition, it follows that, for every even $n \geq 2$, an n-input Boolean function satisfies the PC of degree $n-1$ if and only if it satisfies the PC of degree n. We also show a method that constructs, for any odd $n \geq 3$, n-input Boolean functions that satisfy the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. This method is a generalized version of a previous one. Concerned with the SAC of higher orders, it is shown that the previously proved upper bound of the nonlinear order of Boolean functions satisfying the criterion is tight. The relationships are discussed between the set of n-input Boolean functions satisfying the PC and the sets of those satisfying the SAC.

key words: *Boolean functions, nonlinearity criteria, propagation criterion, strict avalanche criterion, symmetric cryptosystems, cryptography*

1. Introduction

For symmetric cryptosystems, their transformations should be nonlinear to be secure against various attacks. For example, the security of block ciphers, such as the DES, which consist of iterative substitutions and permutations, strongly depends on the substitutions which are the only nonlinear elements of the ciphers. Several nonlinearity criteria for Boolean functions have been proposed and investigated.

This paper mainly focuses on the extended versions of the strict avalanche criterion and the perfect nonlinearity and discusses single-output Boolean functions satisfying them. The strict avalanche criterion (SAC) was introduced as a design principle of good S boxes by Webster and Tavares [11]. Forré [2] extended the notion and defined the SAC of higher orders. The perfect nonlinearity was defined by Meier and Staffelbach [4], and Preneel, Leekwijk, Linden, Govaerts and Vandewalle [6] extended it and defined the propagation criterion (PC) of higher degrees.

There exist no Boolean function with good properties for all nonlinearity criteria and useful for all cryptographic applications. For example, perfectly nonlinear Boolean functions are not balanced and their nonlinear order is at most half of the number of inputs. It is essential to examine the relationships among nonlinearity criteria, for instance, the order of the SAC, the degree of the PC, the nonlinear order, etc. in order to design good Boolean functions for each application.

This paper presents an investigation of the PC of higher degrees, the SAC of higher orders and their relationships. First, we discuss the PC. We give a necessary and sufficient condition for an n-input Boolean function to satisfy the PC with respect to a set of all but one or two elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. From this condition, it follows that, for every even $n \geq 2$, an n-input Boolean function satisfies the PC of degree $n-1$ if and only if it satisfies the PC of degree n. We also show a method that constructs, for any odd $n \geq 3$, n-input Boolean functions which satisfy the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. This method is a generalized version of the one in Ref. [10].

Second, concerned with the SAC of higher orders, we prove that the upper bound of the nonlinear order of Boolean functions satisfying the criterion, which was presented by Preneel, et al. [6], is tight.

Finally, we show that, for odd $n \geq 3$, the set of n-input Boolean functions satisfying the PC of degree $n-1$ is contained by the set of those satisfying the SAC of order 1, while it is not the case for even $n \geq 2$. It is also shown that the set of n-input Boolean functions satisfying the PC of degree 2 does not include the set of those satisfying the SAC of order $n-3$.

Section 2 contains the definitions of nonlinearity criteria. Section 3 is devoted to the discussion of properties of Boolean functions satisfying the PC. Section 4 presents the theorems on Boolean functions satisfying the SAC. Our results about the relationships between the SAC and the PC are in Sect. 5. Section 6 is the conclusion with a comment for multiple-output Boolean functions.

Manuscript received January 28, 1994.
Manuscript revised August 22, 1994.

[†]The authors are with the Faculty of Engineering, Kyoto University, Kyoto, 606–01 Japan.

2. Preliminaries

2.1 Walsh Transform and Boolean Functions

Let $\mathbf{R}$ denote the set of reals.

Definition 1: The *Walsh transform* of a real-valued function $f : \{0,1\}^n \to \mathbf{R}$ is

$$(\mathcal{W}(f))(\omega) = \sum_{x \in \{0,1\}^n} f(x)(-1)^{\omega \cdot x},$$

where $x = (x_1, \ldots, x_n), \omega = (\omega_1, \ldots, \omega_n) \in \{0,1\}^n$ and $\omega \cdot x$ denotes the dot product $\omega_1 x_1 \oplus \cdots \oplus \omega_n x_n$. □

For simplicity, $(\mathcal{W}(f))(\omega)$ is often denoted by $F(\omega)$. The *inverse Walsh transform* is

$$f(x) = (\mathcal{W}^{-1}(F))(x) = \frac{1}{2^n} \sum_{\omega \in \{0,1\}^n} F(\omega)(-1)^{\omega \cdot x}.$$

The Walsh transform can be represented in a matrix form [9]. For $f : \{0,1\}^n \to \mathbf{R}$, let $f(i)$ denote $f(x_1, \ldots, x_n)$ when $x_1 + x_2 2 + \cdots + x_n 2^{n-1} = i$. Let $[f] = [f(0), f(1), \ldots, f(2^n - 1)]$ and $[F] = [F(0), F(1), \ldots, F(2^n - 1)]$. The Walsh transform is represented as

$$[F] = [f] H_n,$$

where H_n denotes the Hadamard matrix of order n. H_n is defined recursively by

$$H_0 = [1],$$

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}.$$

H_n is a $2^n \times 2^n$ symmetric non-singular matrix, and its inverse is $2^{-n} H_n$. The inverse Walsh transform is represented as

$$[f] = 2^{-n} [F] H_n.$$

A *Boolean function* is a function of the form $f : \{0,1\}^n \to \{0,1\}^m$. n is the number of *inputs* and m is the number of *outputs*. In this paper, only the case where $m = 1$ is considered. $f : \{0,1\}^n \to \{0,1\}$ is called n-input Boolean function or Boolean function with n variables. Let $\mathrm{B}_n = \{f \mid f : \{0,1\}^n \to \{0,1\}\}$.

The Walsh transform can be applied to Boolean functions when they considered to be real-valued functions. For the analysis of Boolean functions, it is often convenient to work with $\hat{f} : \{0,1\}^n \to \{-1,1\}$, where $\hat{f}(x) = (-1)^{f(x)}$. The Walsh transform of $\hat{f}$ is

$$\hat{F}(\omega) = \sum_{x \in \{0,1\}^n} \hat{f}(x)(-1)^{\omega \cdot x} = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus \omega \cdot x}.$$

Definition 2: The *autocorrelation function* of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is $C_f : \{0,1\}^n \to \mathbf{N}$ such that

$$C_f(z) = \sum_{x \in \{0,1\}^n} \hat{f}(x) \hat{f}(x \oplus z),$$

where $\mathbf{N}$ is the set of integers and $x \oplus z$ denotes $x_1 \oplus z_1, \ldots, x_n \oplus z_n$. □

Proposition 1: For every Boolean function f, $C_f(z) = (\mathcal{W}^{-1}(\hat{F}^2))(z)$. □

Proposition 2: If $f \in \mathrm{B}_n$, then $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$. □

Definition 3: Let $f(x_1, \ldots, x_n)$ be a Boolean function.

$$\frac{df}{dx_i} = f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \oplus f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n).$$

is the *Boolean difference* of f with respect to a variable x_i. □

2.2 Nonlinearity Criteria for Boolean Functions

For a set S, let |S| denote the number of elements in S.

Definition 4: A Boolean function $f \in \mathrm{B}_n$ is *balanced* if and only if $|\{x \mid f(x) = 0\}| = |\{x \mid f(x) = 1\}| = 2^{n-1}$. □

Definition 5: The *algebraic normal form* of a Boolean function $f \in \mathrm{B}_n$ is a type of representation of f such that

$$\bigoplus_{\{i_1, \ldots, i_k\} \in \wp(\mathrm{N})} a_{\{i_1, \ldots, i_k\}} x_{i_1} \cdots x_{i_k},$$

where $\mathrm{N} = \{1, \ldots, n\}$, $\wp(\mathrm{N})$ is the power set of N, and $a_{\{i_1, \ldots, i_k\}} \in \{0,1\}$ for every $\{i_1, \ldots, i_k\} \in \wp(\mathrm{N})$. □

Any Boolean function can be uniquely represented in an algebraic normal form, and any two different Boolean functions cannot be represented in a same algebraic normal form.

Definition 6: The *nonlinear order* of a Boolean function is the maximum order of the product terms in its algebraic normal form. □

For any $a \in \{0,1\}^n$, let $W(a)$ denote the Hamming weight of a, that is, the number of 1's in a.

Definition 7: A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *strict avalanche criterion (SAC)* if and only if $f(x) \oplus f(x \oplus a)$ is balanced for every $a \in \{0,1\}^n$ such that $W(a) = 1$. □

Let $f(x_1, \ldots, x_n) \in \mathrm{B}_n$. For any $i_1, \ldots, i_m$ such that $1 \leqq i_1 < \cdots < i_m \leqq n$ and $b_1, \ldots, b_m \in \{0,1\}$, let $f\,|_{x_{i_1}=b_1, \ldots, x_{i_m}=b_m} \in \mathrm{B}_{n-m}$ denote the sub-function of f obtained by substituting $b_1, \ldots, b_m$ for $x_{i_1}, \ldots, x_{i_m}$, respectively.

Definition 8: A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *SAC of order m* if and only if, for every $i_1, \ldots, i_m$ such that $1 \leqq i_1 < \cdots < i_m \leqq n$ and $b_1, \ldots, b_m \in \{0,1\}$, $f\,|_{x_{i_1}=b_1, \ldots, x_{i_m}=b_m} \in \mathrm{B}_{n-m}$ satisfies the SAC. □

It is obvious from the definition that the original SAC of Definition 7 is equivalent to the SAC of order 0. The value of a function satisfying the SAC depends on all of its variables. Lloyd [3] proved that every Boolean function satisfying the SAC of order m also satisfies the SAC of order $k(< m)$. Let $\mathrm{SAC}_n(m)$ denote the set of $f \in \mathrm{B}_n$ satisfying the SAC of order m. It is apparent from Definition 7 that every $f \in \mathrm{B}_0 \cup \mathrm{B}_1$ does not satisfy the SAC. $\mathrm{SAC}_n(n-1) = \mathrm{SAC}_n(n) = \phi$ for every n.

Definition 9 [4]: A Boolean function $f \in \mathrm{B}_n$ is *perfectly nonlinear* if and only if $f(x) \oplus f(x \oplus a)$ is balanced for every $a \in \{0,1\}^n$ such that $1 \leqq W(a) \leqq n$. □

Meier and Staffelbach [4] proved that the set of perfectly nonlinear Boolean functions coincides with the set of Boolean bent functions defined by Rothaus [8].

Definition 10: Let $f \in \mathrm{B}_n$. f is said to be a *bent* function if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$. □

Preneel, et al. [6] extended the notion of the perfect nonlinearity and define the propagation criterion.

Definition 11: A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *propagation criterion (PC) of degree k* if and only if $f(x) \oplus f(x \oplus a)$ is balanced for every $a \in \{0,1\}^n$ such that $1 \leqq W(a) \leqq k$. □

Let $\mathrm{PC}_n(k)$ denote the set of Boolean functions with n variables satisfying the PC of degree k. $\mathrm{PC}_n(n)$ is the set of perfectly nonlinear Boolean functions with n variables. $\mathrm{PC}_n(1) = \mathrm{SAC}_n(0)$.

Definition 12: A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *PC with respect to* $\mathrm{A} \subseteq \{0,1\}^n - \{(0,\ldots,0)\}$ if and only if $f(x) \oplus f(x \oplus a)$ is balanced for every $a \in \mathrm{A}$. □

The PC is one of the most important nonlinearity criteria because differential cryptanalysis [1] utilize the bias of the distribution of the input differences and the output differences. For example, a round-function having an S box with large number of inputs satisfying the PC with respect to a set A has no characteristics useful for the differential cryptanalysis with respect to input differences in A.

This paper discusses single-output Boolean functions. This is just a commencement of the discussion of multiple-output Boolean functions. Only some of the results can be directly extended for multiple-output Boolean functions. This matter is mentioned in Sect. 6

3. Boolean Functions Satisfying the PC of Higher Degrees

3.1 Almost Perfectly Nonlinear Boolean Functions

In this section, we investigate the Boolean functions that satisfy the PC with respect to the sets of all but a few elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. These Boolean functions may be called almost perfectly nonlinear functions.

The following theorem presents a necessary and sufficient condition for $f \in \mathrm{B}_n$ to satisfy the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

For $a = (a_1,\ldots,a_n) \in \{0,1\}^n$, let $dec(a) = a_1 + 2a_2 + \cdots + 2^{n-1}a_n$.

Lemma 1: Let $m \geqq 0$ be an integer. The integers $x, y \geqq 0$ satisfying the equation $x^2 + y^2 = 2^m$ is,

- for even m, $x = 2^{m/2}$ and $y = 0$, or $x = 0$ and $y = 2^{m/2}$,
- for odd m, $x = y = 2^{(m-1)/2}$.

Proof: If one of x and y is 0, then m is even and the other is $2^{m/2}$.

If we assume that $x \neq 0$ and $y \neq 0$, then, we can represent x and y as

$$x = 2^{e_x} q_x,\ y = 2^{e_y} q_y,$$

respectively, where $e_x \geqq 0$, $e_y \geqq 0$, and q_x, q_y are odd. Without loss of generality, it can be assumed that $e_y \geqq e_x \geqq 0$. Thus,

$$\begin{aligned} 2^{2e_x} {q_x}^2 + 2^{2e_y} {q_y}^2 &= 2^m \\ {q_x}^2 + 2^{2(e_y - e_x)} {q_y}^2 &= 2^{m-2e_x}. \end{aligned}$$

Since ${q_x}^2 + 2^{2(e_y-e_x)} {q_y}^2 \geqq 2$, $m - 2e_x \geqq 1$, which implies $e_y - e_x = 0$. Thus,

$${q_x}^2 + {q_y}^2 = 2^{m-2e_x}.$$

Since ${q_x}^2 + {q_y}^2$ is a multiple of 2 but not of 4, $m - 2e_x = 1$. Hence, $e_x = e_y = (m-1)/2$ and $q_x = q_y = 1$. This implies m is odd and $x = y = 2^{(m-1)/2}$.

The lemma has been proved. □

Theorem 1: Let $b \in \{0,1\}^n - \{(0,\ldots,0)\}$ and $\mathrm{A} = \{0,1\}^n - \{b, (0,\ldots,0)\}$. $f \in \mathrm{B}_n$ satisfies the PC with respect to A if and only if,

- for even $n \geqq 2$, $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$,
- for odd $n \geqq 3$,

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } b \cdot \omega = 0 \\ 0 & \text{if } b \cdot \omega = 1, \end{cases}$$

or

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } b \cdot \omega = 1 \\ 0 & \text{if } b \cdot \omega = 0. \end{cases}$$

Proof: Let v_i be the i-th column of the Hadamard matrix H_n for $0 \leqq i \leqq 2^n - 1$. From the definition of the autocorrelation function, it is clear that $f \in \mathrm{B}_n$ satisfies the PC with respect to A if and only if $C_f(a) = 0$ for every $a \in \mathrm{A}$. Hence, from Proposition 1, for every $a \in \mathrm{A}$

$$\left[\hat{F}^2\right] v_{dec(a)} = 0.$$

Since the rank of H_n is 2^n, $\left[\hat{F}^2\right]$ is able to be represented as

$$\left[\hat{F}^2\right] = c_0 u_0 + c_1 u_1,$$

where

$$u_0 = ({v_0}^{\mathrm{T}} + {v_{dec(b)}}^{\mathrm{T}})/2,$$

$$u_1 = ({v_0}^{\mathrm{T}} - {v_{dec(b)}}^{\mathrm{T}})/2,$$

${v_0}^{\mathrm{T}}$ and ${v_{dec(b)}}^{\mathrm{T}}$ are the transposes of v_0 and $v_{dec(b)}$, respectively, and c_0, c_1 are some integers. $u_0, u_1 \in \{0,1\}^{2^n}$ and, for every $\omega \in \{0,1\}^n$, the $dec(\omega)$-th elements of u_0 and u_1 are 1 and 0, respectively, if and only if $b \cdot \omega = 0$.

Let $\left|\hat{F}(\omega)\right| = \hat{F}_0$ for every ω such that $b \cdot \omega = 0$, and $\left|\hat{F}(\omega)\right| = \hat{F}_1$ for every ω such that $b \cdot \omega = 1$. Since $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$,

$$\hat{F}_0^2 + \hat{F}_1^2 = 2^{n+1}.$$

Hence, from Lemma 1,

- When n is even, $\hat{F}_0 = \hat{F}_1 = 2^{n/2}$.
- When n is odd, $\hat{F}_0 = 0$, $\hat{F}_1 = 2^{(n+1)/2}$, or $\hat{F}_0 = 2^{(n+1)/2}$, $\hat{F}_1 = 0$.

The theorem has been proved. □

It directly follows from the definition of Boolean bent functions that $\mathrm{PC}_n(n) = \emptyset$ for any odd n, and that $f \in \mathrm{B}_n$ is perfectly nonlinear if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$.

The next corollary presents a necessary and sufficient condition for a Boolean function $f \in \mathrm{B}_n$ to be in $\mathrm{PC}_n(n-1)$.

Corollary 1: $f \in \mathrm{PC}_n(n-1)$ if and only if,

- for even $n \geqq 2$, $f \in \mathrm{PC}_n(n)$,
- for odd $n \geqq 3$,

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } W(\omega) \text{ is even} \\ 0 & \text{if } W(\omega) \text{ is odd,} \end{cases}$$

or

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } W(\omega) \text{ is odd} \\ 0 & \text{if } W(\omega) \text{ is even.} \end{cases}$$

□

The first part of Corollary 1 says that, for every even $n \geqq 2$, $\mathrm{PC}_n(n) = \mathrm{PC}_n(n-1)$.

Theorem 2: Let $b_1, b_2 \in \{0,1\}^n - \{(0,\ldots,0)\}$ such that $b_1 \neq b_2$, and $\mathrm{A} = \{0,1\}^n - \{(0,\ldots,0), b_1, b_2\}$. For every even $n \geqq 2$, $f \in \mathrm{B}_n$ satisfies the PC with respect to A if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$.

Proof: Since $f \in \mathrm{B}_n$ satisfies the PC with respect to A, $\left[\hat{F}^2\right]$ can be represented as

$$\left[\hat{F}^2\right] = c_0 u_0 + c_1 u_1 + c_2 u_2,$$

where $u_0 = {v_0}^{\mathrm{T}}$,

$$u_1 = ({v_0}^{\mathrm{T}} + {v_{dec(b_1)}}^{\mathrm{T}})/2,$$

$$u_2 = ({v_0}^{\mathrm{T}} + {v_{dec(b_2)}}^{\mathrm{T}})/2.$$

For the above equation, it is easily proved that the value of each element in $\left[\hat{F}^2\right]$ is represented as c_0, $c_0 + c_1$, $c_0 + c_2$, or $c_0 + c_1 + c_2$, and that the number of elements in $\left[\hat{F}^2\right]$ represented as each of them is $2^n/4$. Since $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$,

$$c_0 + (c_0 + c_1) + (c_0 + c_2) + (c_0 + c_1 + c_2) = 2^{n+2}$$
$$c_0 + (c_0 + c_1 + c_2) = 2^{n+1}.$$

Since both of c_0 and $c_0 + c_1 + c_2$ are square numbers and n is even, from Lemma 1, $c_0 = c_0 + c_1 + c_2 = 2^n$. And also, since

$$(c_0 + c_1) + (c_0 + c_2) = 2^{n+1}$$

and both of $c_0 + c_1$ and $c_0 + c_2$ are square numbers, $c_0 + c_1 = c_0 + c_2 = 2^n$.

Thus, for every $\omega \in \{0,1\}^n$, $\hat{F}^2(\omega) = 2^n$, and the theorem has been proved. □

Corollary 2: Let $n \geqq 2$ be even and $\mathrm{A} \subseteqq \{0,1\}^n - \{(0,\ldots,0)\}$ such that $|\mathrm{A}| = 2^n - 3$. If $f \in \mathrm{B}_n$ satisfies the PC with respect to A, then $f \in \mathrm{PC}_n(n)$. □

Seberry, et al. [10] presented a method that, for every even $n \geqq 2$, generates balanced Boolean functions in B_n satisfying the PC with respect to a set of all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. The above corollary shows that their construction is optimal in the sense that the Boolean functions satisfying the PC with respect to a set of all but two elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ are in $\mathrm{PC}_n(n)$, because the perfectly nonlinear functions are not balanced.

3.2 A Construction Method of Boolean Functions Satisfying the PC

It is obvious from the definition that, for every n, $\mathrm{PC}_n(1) \supseteqq \cdots \supseteqq \mathrm{PC}_n(n-1) \supseteqq \mathrm{PC}_n(n)$. For odd n, the following theorem can be proved.

Theorem 3: For every odd $n \geqq 3$, $\mathrm{PC}_n(k-1) \supsetneqq \mathrm{PC}_n(k)$ for $k = 2,\ldots,n$. □

Table 1 shows the number of functions in some $\mathrm{PC}_n(k)$'s [6]. For even n, $\mathrm{PC}_n(k)$'s do not necessarily have the property in Theorem 3. For example, when $n = 4$, $\mathrm{PC}_4(2) = \mathrm{PC}_4(3)$.

Theorem 3 can be directly derived from the discussion in Ref. [10]. Seberry, et al. [10] presented a method that, for any odd $n \geqq 3$, generates balanced Boolean

functions satisfying the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

We propose a method that, for any odd $n \geqq 3$, generates Boolean functions satisfying the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. Our method is a generalized version of theirs. By a simple observation of Theorem 1 and our method, it is easily verified that one can construct all Boolean functions that satisfy the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ from all Boolean functions in $\mathrm{PC}_{n-1}(n-1)$.

From Corollary 1 and our method, the following theorems are easily derived.

Theorem 4: For every odd $n \geqq 3$, $|\mathrm{PC}_n(n-1)| = 2|\mathrm{PC}_{n-1}(n-1)|$. □

Theorem 5: For every odd $n \geqq 3$, the number of balanced functions in $\mathrm{PC}_n(n-1)$ is $|\mathrm{PC}_{n-1}(n-1)|$. □

Our proposed method makes use of a property of the Walsh transform of the Boolean functions.

Lemma 2: For every $n \geqq 2$ and $1 \leqq k \leqq n$, $f \in \mathrm{PC}_n(k)$ if and only if $\left[\hat{F}^2\right]$ is uniquely represented as a linear combination of the $dec(a)$-th row vectors of ${H_n}^{\mathrm{T}}$, where $a \in \{0,1\}^n$ and $W(a) = 0$ or $k+1 \leqq W(a) \leqq n$.

Proof: $f \in \mathrm{PC}_n(k)$ if and only if $2^{-n} \sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega)(-1)^{\omega \cdot a} = 0$ for every $a \in \{0,1\}^n$ such that $1 \leqq W(a) \leqq k$, which is equivalent to that, for every $v_{dec(a)}$ in H_n such that $1 \leqq W(a) \leqq k$, $\left[\hat{F}^2\right] v_{dec(a)} = 0$. Since H_n is non-singular, the lemma follows. □

The above lemma leads to the following.

Lemma 3: Let $a \in \{0,1\}^n$ and $W(a) = k$. If $\left[\hat{F}^2\right]$ can be represented uniquely as a linear combination of v_0 and $v_{dec(a)}$, then $f \in \mathrm{PC}_n(k-1) - \mathrm{PC}_n(k)$ and f satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0), a\}$. □

Boolean functions that are in $\mathrm{PC}_n(k-1) - \mathrm{PC}_n(k)$ and that satisfy the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ are able to be constructed with the following algorithm.

Algorithm 1:

1. Select some $a \in \{0,1\}^n$ such that $W(a) = k$.

2. Let $u = ({v_0}^{\mathrm{T}} - {v_{dec(a)}}^{\mathrm{T}})/2$. $u \cdot v_j = 0$ for every v_j of H_n such that $j \neq 0, dec(a)$. Let $L_a(\omega) = a_1\omega_1 \oplus \cdots \oplus a_n\omega_n$, then $u = [L_a(0), L_a(1), \ldots, L_a(2^n-1)]$.

Table 1 The number of functions in $\mathrm{PC}_n(k)$.

		n			
		2	3	4	5
k	1	8	64	4,128	27,522,560
	2	8	16	896	228,352
	3	–	0	896	10,752
	4	–	–	896	1,792
	5	–	–	–	0

3. Let

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if the } dec(\omega)\text{-th element of } u \text{ equals to 1} \\ 0 & \text{if the } dec(\omega)\text{-th element of } u \text{ equals to 0,} \end{cases}$$

$$\left|\hat{G}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if the } dec(\omega)\text{-th element of } u \text{ equals to 0} \\ 0 & \text{if the } dec(\omega)\text{-th element of } u \text{ equals to 1.} \end{cases}$$

□

The signs of non-zero elements in $\left[\hat{F}\right]$ and $\left[\hat{G}\right]$ are able to be determined so that f and g be Boolean functions, where $\left[\hat{f}\right] = 2^{-n}\left[\hat{F}\right] H_n$ and $[\hat{g}] = 2^{-n}\left[\hat{G}\right] H_n$. Since each element of $2^{-n}\left[\hat{F}\right] H_n$ and $2^{-n}\left[\hat{G}\right] H_n$ must be 1 or -1 for f and g to be Boolean functions, the following lemma implies that f and g are Boolean functions if and only if the non-zero elements of $\left[\hat{F}\right]/2^{(n+1)/2}$ and $\left[\hat{G}\right]/2^{(n+1)/2}$ represent Boolean bent functions.

For a matrix M, let $col(M,i)$ be the i-th column of M. For $a = (a_1,\ldots,a_n) \in \{0,1\}^n$, let $\langle a\rangle_i = (a_1,\ldots,a_i)$.

Lemma 4: For any $a \in \{0,1\}^n$ such that $a \neq (0,\ldots,0)$, let $G_n(a,0)$ and $G_n(a,1)$ be $2^{n-1} \times 2^n$ matrices that are constructed by removing all $dec(\omega)$-th rows of H_n, where $a \cdot \omega = 1$ and $a \cdot \omega = 0$, respectively. Then,

- for each column v of H_{n-1}, $G_n(a,0)$ has two columns that are equal to v, and $G_n(a,1)$ has v and $-v$,
- for every i such that $0 \leqq i \leqq 2^n - 1$,

$$col(G_n(a,0),i) = col(G_n(a,1),i)$$

or

$$col(G_n(a,0),i) = -col(G_n(a,1),i).$$

Proof: We prove the theorem by induction. When $n = 1$, since $H_0 = [1]$ and

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$G_1(1,0) = [1,1]$ and $G_1(1,1) = [1,-1]$. The theorem is proved for $n = 1$.

For the Case where $a_n = 0$: For $c = 0, 1$,

$$G_n(a,c) = \begin{bmatrix} G_{n-1}(\langle a\rangle_{n-1}, c) & G_{n-1}(\langle a\rangle_{n-1}, c) \\ G_{n-1}(\langle a\rangle_{n-1}, c) & -G_{n-1}(\langle a\rangle_{n-1}, c) \end{bmatrix}.$$

For the Case where $a_n = 1$: For $a = (0,\ldots,0,1)$, since

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix},$$

$G_n(a,0) = [H_{n-1}, H_{n-1}]$, $G_n(a,1) = [H_{n-1}, -H_{n-1}]$.

For $a \neq (0,\ldots,0,1)$, for $c = 0,1$,

$$G_n(a,c) = \begin{bmatrix} G_{n-1}(\langle a\rangle_{n-1}, c) & G_{n-1}(\langle a\rangle_{n-1}, c) \\ G_{n-1}(\langle a\rangle_{n-1}, 1\oplus c) & -G_{n-1}(\langle a\rangle_{n-1}, 1\oplus c) \end{bmatrix}.$$

Since, for every j such that $0 \leqq j \leqq 2^{n-1}-1$, $col(G_{n-1}(\langle a\rangle_{n-1}, 0), j) = col(G_{n-1}(\langle a\rangle_{n-1}, 1), j)$ or $col(G_{n-1}(\langle a\rangle_{n-1}, 0), j) = -col(G_{n-1}(\langle a\rangle_{n-1}, 1), j)$, for $c = 0, 1$, $G_n(a,c)$ is able to be transformed to

$$\begin{bmatrix} G_{n-1}(\langle a\rangle_{n-1}, c) & G_{n-1}(\langle a\rangle_{n-1}, c) \\ G_{n-1}(\langle a\rangle_{n-1}, c) & -G_{n-1}(\langle a\rangle_{n-1}, c) \end{bmatrix}$$

by permuting the columns of it.

Hence, the theorem has been proved. □

Example 1: We construct two Boolean functions $f, g \in \mathrm{PC}_3(1) - \mathrm{PC}_3(2)$.

First, we select $a = (a_1, a_2, a_3) = (0,1,1)$. Then $W(a) = 2$, and $dec(a) = 6$. The 6-th column of H_3 is $v_6 = [1,1,-1,-1,-1,-1,1,1]^{\mathrm{T}}$. Then,

$$\begin{aligned} u &= ([1,1,1,1,1,1,1,1] - {v_6}^{\mathrm{T}})/2 \\ &= [0,0,1,1,1,1,0,0]. \end{aligned}$$

For $\hat{F}(\omega_1,\omega_2,\omega_3)$ and $\hat{G}(\omega_1,\omega_2,\omega_3)$, let

$$\left[\hat{F}(0), \hat{F}(1), \ldots, \hat{F}(7)\right] = [0,0,4,4,4,-4,0,0],$$

$$\left[\hat{G}(0), \hat{G}(1), \ldots, \hat{G}(7)\right] = [4,4,0,0,0,0,4,-4],$$

respectively, where the signs of the non-zero elements of $\left[\hat{F}\right]$ and $\left[\hat{G}\right]$ are determined by the perfectly nonlinear function $h(x_1,x_2) = x_1 \wedge x_2$.

$$[h(0), h(1), h(2), h(3)] = [1,1,1,-1].$$

Then,

$$\left[\hat{f}\right] = 2^{-3}\left[\hat{F}\right] H_3 = [1,1,-1,1,1,-1,-1,-1],$$

$$[\hat{g}] = 2^{-3}\left[\hat{G}\right] H_3 = [1,1,1,-1,-1,-1,1,1],$$

and f is a balanced Boolean function.

$$f(x_1,x_2,x_3) = \overline{x_1}x_2 \vee x_1x_3 = x_2 \oplus x_1x_2 \oplus x_1x_3.$$

$$g(x_1,x_2,x_3) = x_1x_2\overline{x_3} \vee x_1\overline{x_2}x_3 = x_1x_2 \oplus x_1x_3.$$

From Table 2, for $f \in \mathrm{B}_3$, $f(x) \oplus f(a \oplus x)$ is balanced except for $a = (0,1,1)$. When $a = (0,1,1)$, $f(a \oplus x) = f(x)$. Hence, $f \in \mathrm{PC}_3(1) - \mathrm{PC}_3(2)$.

For $g \in \mathrm{B}_3$, $g(x) \oplus g(a \oplus x)$ is balanced except for $a = (0,1,1)$. When $a = (0,1,1)$, $g(a \oplus x) = 1 \oplus g(x)$. Hence, $g \in \mathrm{PC}_3(1) - \mathrm{PC}_3(2)$. □

The following theorem exhibits a property of the Boolean functions satisfying the PC with respect to a set of all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ that is disadvantageous to cryptographic use.

Table 2 $f(x) \oplus f(a \oplus x)$ and $g(x) \oplus g(a \oplus x)$.

(a_1,a_2,a_3)	$f(x) \oplus f(x \oplus a)$	$g(x) \oplus g(x \oplus a)$
(1, 0, 0)	$x_2 \oplus x_3$	$x_2 \oplus x_3$
(0, 1, 0)	$1 \oplus x_1$	$1 \oplus x_1$
(0, 0, 1)	x_1	x_1
(1, 1, 0)	$x_1 \oplus x_2 \oplus x_3$	$x_1 \oplus x_2 \oplus x_3$
(1, 0, 1)	$1 \oplus x_1 \oplus x_2 \oplus x_3$	$1 \oplus x_1 \oplus x_2 \oplus x_3$
(0, 1, 1)	1	0
(1, 1, 1)	$x_2 \oplus x_3$	$x_2 \oplus x_3$

Theorem 6: Let $n \geqq 3$ be odd and $b \in \{0,1\}^n - \{(0,\ldots,0)\}$. If $f \in \mathrm{B}_n$ satisfies the PC with respect to $\{0,1\}^n - \{b, (0,\ldots,0)\}$, then $f(x) \oplus f(x \oplus b) \equiv 0$ or 1.

Proof: From Proposition 1 and Theorem 1,

$$\begin{aligned} \sum_{x\in\{0,1\}^n} \hat{f}(x)\hat{f}(x\oplus b) &= C_f(b) \\ &= \frac{1}{2^n}\left[\hat{F}^2\right] v_{dec(b)} = \pm 2^n. \end{aligned}$$

□

4. Boolean Functions Satisfying the SAC of Higher Orders

Preneel, et al. [6] discussed the relationship between the SAC of higher order and the nonlinear order, and presented the theorem below.

Theorem 7 [6]: Let $f \in \mathrm{B}_n$.

1. If f satisfies the SAC of order $n-2$, then the nonlinear order of f is 2.
2. For each $0 \leqq m \leqq n-3$, if f satisfies the SAC of order m, then the nonlinear order of f is less than $n-m$. □

We show that the upper bound in Theorem 7 is tight.

Lemma 5: $f(x_1,\ldots,x_n) \in \mathrm{B}_n$ satisfies the SAC if and only if $\dfrac{df}{dx_i} \in \mathrm{B}_{n-1}$ is balanced for every x_i.

Proof: Let $a = (1,0,\ldots,0)$.

$$\begin{aligned} &f(x_1,x_2,\ldots,x_n) \oplus f(1\oplus x_1, x_2, \ldots, x_n) \\ &\quad = \overline{x_1}(f(0,x_2,\ldots,x_n) \oplus f(1,x_2,\ldots,x_n)) \\ &\qquad \vee x_1(f(1,x_2,\ldots,x_n) \oplus f(0,x_2,\ldots,x_n)) \\ &\quad = (\overline{x_1} \vee x_1)(f(0,x_2,\ldots,x_n) \oplus f(1,x_2,\ldots,x_n)) \\ &\quad = f(0,x_2,\ldots,x_n) \oplus f(1,x_2,\ldots,x_n). \end{aligned}$$

Since $f(x_1,x_2,\ldots,x_n) \oplus f(1\oplus x_1,x_2,\ldots,x_n)$ does not depend on x_1, it is obvious from the above equation that $f(x_1,x_2,\ldots,x_n) \oplus f(1\oplus x_1,x_2,\ldots,x_n)$ is balanced if and only if $\dfrac{df}{dx_1} = f(0,x_2,\ldots,x_n) \oplus f(1,x_2,\ldots,x_n)$ is balanced.

In the same way, it can be shown that, for every a such that $W(a) = 1$ and $a_i = 1$, $f(x) \oplus f(x \oplus a)$ is balanced if and only if $\dfrac{df}{dx_i}$ is balanced. □

Lemma 6 [6]: Let $n > 2$ and $f(x_1, \ldots, x_n) \in B_n$. If the nonlinear order of f is 2, then for each m such that $0 \leqq m \leqq n-2$, $f \in SAC_n(m)$ if and only if every x_i occurs in at least $m+1$ second order terms of the algebraic normal form. □

For $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, let $\langle x \rangle_j^i := (x_i, \ldots, x_j)$ for every i, j such that $1 \leqq i < j \leqq n$.

Theorem 8: For each $0 \leqq m \leqq n-3$, there exists $f \in B_n$ which satisfies the SAC of order m and whose nonlinear order is exactly $n-m-1$.

Proof: Let $q_n(x_1, \ldots, x_n) = \bigoplus_{1 \leqq i < j \leqq n} x_i x_j$ and

$$f_n(x_1, \ldots, x_n) = x_1 \cdots x_{n-m-1} \oplus q_n(x_1, \ldots, x_n).$$

This proof demonstrates that $f_n \in SAC_n(m)$.

Let k be an integer such that $0 \leqq k \leqq \min\{n-m-1, m\}$. When we fix m of $x_1, \ldots, x_n$ constant, without loss of generality, we can fix $x_1, \ldots, x_k$ and $x_{n-(m-k)+1}, \ldots, x_n$ constant.

We consider the following two case: (1) when at least one of $x_1, \ldots, x_k$ are fixed 0, and (2) when $k = 0$ or all of $x_1, \ldots, x_k$ are fixed 1.

(1) Let $(a_1, \ldots, a_k, a_{k+1}, \ldots, a_m) \in \{0,1\}^m$ and at least one of $a_1, \ldots, a_k$ are 0. Then,

$$f_n(\langle a \rangle_k^1, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}) = q_n(\langle a \rangle_k^1, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}).$$

Since $q_n \in SAC_n(n-2)$ and $m \leqq n-3$,

$$f_n(\langle a \rangle_k^1, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}) \in SAC_{n-m}(0).$$

(2) If $k = n-m-1$,

$$f_n(\underbrace{1, \ldots, 1}_{k}, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}) = 1 \oplus q_n(1, \ldots, 1, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}).$$

This shows

$$f_n(1, \ldots, 1, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}) \in SAC_{n-m}(0).$$

If $0 \leqq k < n-m-1$,

$$f_n(\underbrace{1, \ldots, 1}_{k}, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}) = x_{k+1} \cdots x_{n-m-1} \oplus q_n(1, \ldots, 1, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1})$$

$$= \begin{cases} x_{k+1} \cdots x_{n-m-1} \oplus q_{n-m}(\langle x \rangle_{n-m+k}^{k+1}) \oplus b \\ \quad \text{if } 1, \ldots, 1, a_{k+1}, \ldots, a_m \text{ contain even number of 1's,} \\ x_{k+1} \cdots x_{n-m-1} \oplus q_{n-m}(\langle x \rangle_{n-m+k}^{k+1}) \\ \oplus x_{k+1} \oplus \cdots \oplus x_{n-m+k} \oplus c \\ \quad \text{if } 1, \ldots, 1, a_{k+1}, \ldots, a_m \text{ contain odd number of 1's,} \end{cases}$$

where $b, c \in \{0,1\}$. Let $g_{n-m}(x_{k+1}, \ldots, x_{n-m+k}) = x_{k+1} \cdots x_{n-m-1} \oplus q_{n-m}(x_{k+1}, \ldots, x_{n-m+k}) \oplus b$. The following argument shows that g_{n-m} satisfies the SAC of order 0.

(i) When we check whether the Boolean difference of g_{n-m} with respect to each one of $x_{k+1}, \ldots, x_{n-m-1}$ is balanced, it suffices to check only with respect to x_{k+1} because g_{n-m} is symmetric with respect to $x_{k+1}, \ldots, x_{n-m-1}$.

$$\frac{dg_{n-m}}{dx_{k+1}} = x_{k+2} \oplus \cdots \oplus x_{n-m+k} \oplus x_{k+2} \cdots x_{n-m-1}.$$

For every $b_1, \ldots, b_{n-(m+k+2)} \in \{0,1\}$, if $x_{k+2} = b_1, \ldots, x_{n-m-1} = b_{n-(m+k+2)}$, then

$$\frac{dg_{n-m}}{dx_{k+1}}(\langle b \rangle_{n-(m+k+2)}^1, \langle x \rangle_{n-m+k}^{n-m}) = x_{n-m} \oplus \cdots \oplus x_{n-m+k} \oplus b_1 \oplus \cdots \oplus b_{n-(m+k+2)} \oplus b_1 \cdots b_{n-(m+k+2)},$$

and

$$\left| \left\{ (\langle b \rangle_{n-(m+k+2)}^1, \langle x \rangle_{n-m+k}^{n-m}) \mid \frac{dg_{n-m}}{dx_{k+1}}(\langle b \rangle_{n-(m+k+2)}^1, \langle x \rangle_{n-m+k}^{n-m}) = 0 \right\} \right| = \left| \left\{ (\langle b \rangle_{n-(m+k+2)}^1, \langle x \rangle_{n-m+k}^{n-m}) \mid \frac{dg_{n-m}}{dx_{k+1}}(\langle b \rangle_{n-(m+k+2)}^1, \langle x \rangle_{n-m+k}^{n-m}) = 1 \right\} \right|.$$

Hence $\dfrac{dg_{n-m}}{dx_{k+1}}$ is balanced.

(ii) When we check whether the Boolean difference of g_{n-m} with respect to each one of $x_{n-m}, \ldots, x_{n-m+k}$ is balanced, it suffices to check only with respect to x_{n-m+k}.

$$\frac{dg_{n-m}}{dx_{n-m+k}} = x_{k+1} \oplus \cdots \oplus x_{n-m+k-1}$$

is balanced.

For the case that $\underbrace{1, \ldots, 1}_{k}, a_{k+1}, \ldots, a_m$ contain odd number of 1's, that

$$f_n(1, \ldots, 1, \langle x \rangle_{n-m+k}^{k+1}, \langle a \rangle_m^{k+1}) \in SAC_{n-m}(0)$$

can be shown in the same manner. □

5. Relationships Between the SAC and the PC

Forré [2] characterized the spectral property of the Boolean functions satisfying the SAC of higher orders. For $1 \leqq i \leqq n$, let $c^i \in \{0,1\}^n$, only of whose i-th element is 1.

Lemma 7 [2]: For every $f \in B_n$, $f \in SAC_n(1)$ if and only if $f \in SAC_n(0)$ and

$$\sum_{\omega} \hat{F}(\omega)\hat{F}(\omega \oplus c^i)(-1)^{\omega_j} = 0$$

for every $i, j \in \{1, \ldots, n\}$ such that $i \neq j$. □

Rothaus [8] presented a few methods for constructing Boolean bent functions. One of them gives Boolean bent functions of the form

$$f(x_1, \ldots, x_n) = \bigoplus_{i=1}^{m} x_i x_{m+i} \oplus g(x_1, \ldots, x_m),$$

where $n = 2m$ and g is an arbitrary m-input Boolean function.

The following theorem shows that all the Boolean functions with odd number of inputs satisfying the PC of the maximum degree satisfy the SAC of order 1, while the Boolean functions with even number of inputs satisfying it necessarily not. The latter case is proved by using Boolean bent functions constructed with Rothaus's method.

Theorem 9:

- For every even $n \geqq 2$, $\mathrm{PC}_n(n) = \mathrm{PC}_n(n-1) \not\subseteq \mathrm{SAC}_n(1)$.
- For every odd $n \geqq 3$, $\mathrm{PC}_n(n-1) \subsetneqq \mathrm{SAC}_n(1)$.

Proof: For the case where n is even: Let $n = 2m$ and

$$f(x_1, \ldots, x_n) = \bigoplus_{i=1}^{m} x_i x_{m+i}.$$

Then $f \in \mathrm{PC}_n(n)$, and $f|_{x_n=1}(x_1, \ldots, x_{n-1}) = \bigoplus_{i=1}^{m-1} x_i x_{m+i} \oplus x_m$. Whenever x_m changes, the value of $f|_{x_n=1}(x_1, \ldots, x_{n-1})$ also changes. Hence, $f \notin \mathrm{SAC}_n(1)$.

For the case where n is odd: It is clear from the definition that $g \in \mathrm{SAC}_n(0)$ if $g \in \mathrm{PC}_n(n-1)$. If n is odd, then, for every $g \in \mathrm{PC}_n(n-1)$, either for every $\omega \in \{0,1\}^n$ whose Hamming weight is even or for every $\omega \in \{0,1\}^n$ whose Hamming weight is odd, $\hat{G}(\omega) = 0$. Hence, for every $c^i \in \{0,1\}^n$ whose Hamming weight is 1, $\hat{G}(\omega)\hat{G}(\omega \oplus c^i) = 0$. □

It is obvious that $\mathrm{SAC}_n(n-3) \subsetneq \mathrm{PC}_n(1)$, and it is implicitly described in Ref. [6] that $\mathrm{SAC}_n(n-2) \subsetneq \mathrm{PC}_n(n-1)$. These results are optimal in the sense of the theorem below.

Theorem 10: $\mathrm{SAC}_n(n-3) \not\subseteq \mathrm{PC}_n(2)$ for every $n \geqq 3$.

Proof: Let $g_n(x_1, \ldots, x_n) = \bigoplus_{1 \leqq i < j \leqq n, i \leqq n-2} x_i x_j$. It is sufficient to show that $g_n \notin \mathrm{PC}_n(2)$ because $g_n \in \mathrm{SAC}_n(n-3)$ from Lemma 6.

Since $g_n(x_1, \ldots, x_n) = q_{n-2}(x_1, \ldots, x_{n-2}) \oplus \bigoplus_{1 \leqq i \leqq n-2} x_i(x_{n-1} \oplus x_n)$, for $a = (0, \ldots, 0, 1, 1)$, $g_n(x_1, \ldots, x_n) \oplus g_n(x_1 \oplus a_1, \ldots, x_n \oplus a_n) \equiv 0$. Hence, $g_n \notin \mathrm{PC}_n(2)$. □

6. Concluding Remarks

We discussed the PC of higher degrees, the SAC of higher orders and their relationships.

The theorems and the corollaries in Sect. 3.1 can be easily extended for multiple-output Boolean functions along the following definition and the proposition, which are easily derived from Ref. [5]. Let $f : \{0,1\}^n \to \{0,1\}^m$ and $\mathrm{A} \subseteq \{0,1\}^n - \{(0, \ldots, 0)\}$.

Definition f is said to satisfy the PC with respect to A if and only if, for every $a \in \mathrm{A}$, $f(x) \oplus f(x \oplus a)$ is balanced, that is, for every $b \in \{0,1\}^m$, $|\{x \mid f(x) \oplus f(x \oplus a) = b\}| = 2^{n-m}$. □

Proposition Let $f = (f_1, \ldots, f_m)$. f satisfies the PC with respect to A if and only if, for every $c = (c_1, \ldots, c_m) \in \{0,1\}^m - \{(0, \cdots, 0)\}$, $c \cdot f = c_1 f_1 \oplus \cdots \oplus c_m f_m \in \mathrm{B}_n$ satisfies the PC with respect to A. □

Most results in the other parts, however, cannot be easily extended for multiple-output Boolean functions because the correlation between outputs must be considered for them.

We will study tradeoffs among more than two nonlinearity criteria and investigate methods for constructing Boolean functions with desirable nonlinearity to design good symmetric cryptosystems.

References

[1] Biham, E. and Shamir, A., *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[2] Forré, R., "The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition," *Proc. CRYPTO'88, LNCS*, no.403, pp.450–468, 1990.

[3] Lloyd, S., "Properties of binary functions," *Proc. EUROCRYPT'90, LNCS*, no.473, pp.124–139, 1991.

[4] Meier, W. and Staffelbach, O., "Nonlinearity criteria for cryptographic functions," *Proc. EUROCRYPT'89, LNCS*, no.434, pp.549–562, 1990.

[5] Nyberg, K., "Perfect nonlinear S-boxes," *Proc. EUROCRYPT'91, LNCS*, no.547, pp.378–386, 1991.

[6] Preneel, B., Leekwijk, W.V., Linden, L.V., Govaerts, R. and Vandewalle, J., "Propagation characteristics of Boolean functions," *Proc. EUROCRYPT'90, LNCS*, no.473, pp.161–173, 1991.

[7] Preneel, B., Govaerts, R. and Vandewalle, J., "Boolean functions satisfying higher order propagation criteria," *Proc. EUROCRYPT'91, LNCS*, no.547, pp.141–152, 1992.

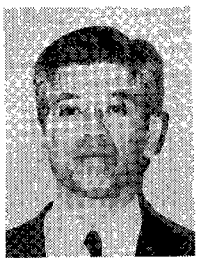
[8] Rothaus, O.S., "On 'bent' functions," *J. Combinatorial Theo. (A)*, vol.20, pp.300–305, 1976.

[9] Rueppel, R.A., "Stream ciphers," in *Contemporary cryptology: The science of information integrity*, G. Simmons, ed., pp.65–134, IEEE Press, 1991.

[10] Seberry, J., Zhang, X.-M. and Zhang, Y., "Highly nonlinear balanced Boolean functions satisfying high degree propagation criterion," *Tech. Rep. The Univ. Wollongong*, tr-93-1, 1993.

[11] Webster, A.F. and Tavares, S.E., "On the design of S-boxes," *Proc. CRYPTO'85, LNCS*, no.218, pp.523–534, 1986.

Shouichi Hirose was born in Kyoto, Japan, on December 30, 1965. He received the B.E. and M.E. degrees in information science from Kyoto University, Kyoto, Japan, in 1988 and 1990, respectively. He is an Instructor at the Department of Information Science, Faculty of Engineering, Kyoto University. His current interests include cryptography, computer security, computational complexity and Boolean functions. He is a member of IPSJ.



Katsuo Ikeda was born in 1937 in Shiga, Japan. He received the B.E. and M.E. degrees in electronic engineering and the D.E. degree in information science from Kyoto University in 1960, 1962 and 1978, respectively. He is currently a Professor of the Department of Information Science, Kyoto University. From 1965 to 1971 he was a Research Associate and from 1971 to 1978 an Associate Professor of the Faculty of Engineering, Kyoto University. From 1978 to 1988 he was a Professor of the Science Information Center and the Department of Information Science, University of Tsukuba. He was a guest researcher at the University of Utah and the Massachusetts Institute of Technology in the academic year 1971–1972, and at the Swiss Federal Institute of Technology (ETH) for two months in 1983. His primary research interests include construction of intelligent information media environment. He is the author of *Structure of a Computer Utility* (in Japanese; Shokodo, 1974) and *Data Communication* (in Japanese; Shokodo, 1993), and the translator of *System Programming* (J.J. Donovan, 1974) and *Operating System* (J.J. Donovan, 1976). He is a member of IPSJ, IEEE, ACM and the editorial board of *Information Processing Letters*, Elsevier. He is also working as a leader of standardization activities related to the Japanese national body of the SC18 of ISO/IEC JTC1 (Document processing and related communication).