PAPER Special Section on Cryptography and Information Security

Propagation Characteristics of Boolean Functions and Their Balancedness

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

SUMMARY This paper discusses Boolean functions satisfying the propagation criterion(PC) and their balancedness. Firstly, we discuss Boolean functions with n variables that satisfy the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. For even $n \geq 4$, a necessary and sufficient condition is presented for Boolean functions with n variables to satisfy the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. From this condition, it is proved that all of these Boolean functions are constructed from all perfectly nonlinear Boolean functions with $n-2$ variables. For odd $n \geq 3$, it is shown that Boolean functions with n variables satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ satisfy the PC with respect to all but one elements in it. Secondly, Boolean functions satisfying the PC of degree $n-2$ and their balancedness are considered. For even $n \geq 4$, it is proved that an upper bound on the degree of the PC is $n-3$ for balanced Boolean functions with n variables. This bound is optimal for $n = 4, 6$. It is also proved that, for odd $n \geq 3$, balanced Boolean functions with n variables satisfying the PC of degree $n-2$ satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

key words: *Boolean functions, nonlinearity criteria, propagation criterion, balancedness, symmetric cryptosystems*

1. Introduction

Cryptographic transformations should be nonlinear to be secure against various attacks. Propagation criterion(PC) is one of the nonlinearity criteria, which was proposed by Preneel, Leekwijk, Linden, Govaerts and Vandewalle[4]. It is an extended notion of perfect nonlinearity, which was defined by Meier and Staffelbach[3].

The PC is a measure of randomness of the difference of outputs to the difference of inputs. It is one of the most important nonlinearity criteria because the differential cryptanalysis[1], which is one of the successful attacks and which is applicable to symmetric cryptosystems and one-way hash functions, utilizes the bias of the distribution of the difference of outputs and the difference of inputs. It is valuable to investigate Boolean functions that satisfy the PC for the systematic generation of cryptographically useful Boolean functions.

This paper discusses single-output Boolean functions that satisfy the PC. A necessary condition for a multiple-output Boolean function to satisfy the PC is that each of its output functions satisfies the PC. The discussion in this paper is a commencement of the discussion of multiple-output Boolean functions that satisfy the PC although it may not be directly applicable to multiple-output Boolean functions.

Seberry, Zhang and Zheng[7] presented methods for the construction of balanced Boolean functions satisfying the PC of high degrees. For odd $n \geq 3$, they proposed a method for constructing balanced Boolean functions with n variables satisfying the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ and constructed balanced Boolean functions satisfying the PC of degree $n-1$. For even $n \geq 4$, they proposed a method for constructing balanced Boolean functions with n variables satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ and constructed balanced Boolean functions satisfying the PC of degree about $2n/3$.

For odd $n \geq 3$, a necessary and sufficient condition was presented for Boolean functions with n variables to satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$[2]. It was also shown that all of these Boolean functions were constructed from all perfectly nonlinear Boolean functions with $n-1$ variables. For even $n \geq 4$, the result in Ref.[7] is optimal in the sense that Boolean functions with n variables satisfying the PC with respect to all but less than three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ are perfectly nonlinear[2] and that perfectly nonlinear Boolean functions are not balanced.

This paper firstly discusses Boolean functions that satisfy the PC with respect to all but three elements. It presents, for even $n \geq 4$, a necessary and sufficient condition for Boolean functions with n variables to satisfy the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. From this condition, it is proved that all of these Boolean functions are constructed from all perfectly nonlinear Boolean functions with $n-2$ variables. It is also shown, for odd $n \geq 3$, that Boolean functions with n variables satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

Secondly, we consider Boolean functions satisfying the PC of degree $n-2$ and their balancedness. For even $n \geq 4$, we show that there exist no balanced Boolean functions satisfying the PC of degree $n-2$. This result is optimal for $n = 4, 6$. For odd $n \geq 3$, we prove that

Manuscript received March 30, 1994.
Manuscript revised July 18, 1994.

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

balanced Boolean functions with n variables satisfying the PC of degree $n-2$ satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

Section 2 contains the definitions of nonlinearity criteria. Section 3 is devoted to the discussion of Boolean functions with n variables satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. Section 4 presents the theorems on Boolean functions with n variables satisfying the PC of degree $n-2$.

2. Preliminaries

2.1 Walsh Transform and Boolean Functions

Let $\mathbf{R}$ and $\mathbf{N}$ denote the set of reals and the set of integers, respectively.

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 [6]. 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 $f : \{0,1\}^n \to \{0,1\}^m$. 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 are 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 $f \in \mathrm{B}_n$ 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 $x \oplus z$ denotes $(x_1 \oplus z_1,\ldots, x_n \oplus z_n)$. □

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

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

2.2 Nonlinearity Criteria for Boolean Functions

For a set S, let $|\mathrm{S}|$ denote the number of elements in S.

Definition 3: A Boolean function $f \in \mathrm{B}_n$ is *balanced* if and only if $|\{x|f(x)=0\}| = |\{x|f(x)=1\}| = 2^{n-1}$. □

An *affine* Boolean function $h \in \mathrm{B}_n$ is a Boolean function of the form of $h(x_1,\ldots,x_n) = \alpha_0 \oplus \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n$, where $\alpha_i \in \{0,1\}$ for $0 \le i \le n$. The *distance* between two Boolean functions, f and g, with the same number of variables, is $d(f,g) = |\{x|f(x) \neq g(x)\}|$.

Definition 4: The *nonlinearity* of $f \in \mathrm{B}_n$ is $\min_{h\in\mathrm{A}_n} d(f,h)$, where A_n denotes the set of affine Boolean functions in B_n. □

Proposition 3: The nonlinearity of $f \in \mathrm{B}_n$ is $\min_{\omega\in\{0,1\}^n}(2^{n-1} \pm \hat{F}(\omega)/2)$. □

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

Definition 5 [3]: 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 $1 \le W(a) \le n$. □

Meier and Staffelbach [3] proved that the set of perfectly nonlinear Boolean functions coincides with the set of Boolean *bent* functions defined by Rothaus [5]. $f \in \mathrm{B}_n$ is defined to be a Boolean bent function if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$.

Proposition 4: $f \in \mathrm{B}_n$ is perfectly nonlinear if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}$. □

Preneel, et al.[4] extended the notion of the perfect nonlinearity and defined the propagation criterion.

Definition 6: 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 $1 \le W(a) \le k$. □

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

Definition 7: A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *propagation criterion(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 $a \in \mathrm{A}$. □

3. Boolean Functions Satisfying the PC with Respect to All But Three Elements

3.1 The Case Where the Number of Variables Is Even

Seberry, et al.[7] presented a method for constructing balanced Boolean functions satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ for every even $n \geqq 4$, and showed the following theorem.

Theorem 1 [7]**:** Let $n \geqq 4$ be even. For any pair of $b_1, b_2 \in \{0,1\}^n - \{(0,\ldots,0)\}$ such that $b_1 \neq b_2$, there exist balanced Boolean functions in B_n satisfying the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_1, b_2, b_1 \oplus b_2\}$. □

The above theorem is optimal in the sense that, for every even $n \geqq 4$, Boolean functions in B_n which satisfy the PC with respect to all but one or two elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ are perfectly nonlinear[2]. Perfectly nonlinear Boolean functions are not balanced.

In this section, for even $n \geqq 4$, a necessary and sufficient condition is presented for balanced Boolean functions in B_n satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. Before proving the theorem, we present three simple lemmas.

Lemma 1 [2]**:** Let $x \geqq y \geqq 0$ and $m \geqq 0$ be integers. $x^2 + y^2 = 2^m$ if and only if

- when m is even, $x = 2^{m/2}$, $y = 0$,
- when m is odd, $x = y = 2^{(m-1)/2}$. □

Lemma 2: There exist no positive integers x, y, z and m such that $x^2 + y^2 + z^2 = 2^m$.

Proof: x, y, z can be represented as

$$x = 2^{e_1} q_1,\ y = 2^{e_2} q_2,\ z = 2^{e_3} q_3,$$

where $e_1, e_2, e_3 \geqq 0$, and q_1, q_2, q_3 are odd integers. Without loss of generality, we may assume that $0 \leqq e_1 \leqq e_2 \leqq e_3$. If $x^2 + y^2 + z^2 = 2^m$, then

$$2^{2e_1} {q_1}^2 + 2^{2e_2} {q_2}^2 + 2^{2e_3} {q_3}^2 = 2^m$$
$${q_1}^2 + 2^{2(e_2 - e_1)} {q_2}^2 + 2^{2(e_3 - e_1)} {q_3}^2 = 2^{m-2e_1}.$$

Since the left-hand side of the above equation is greater than 3, $m - 2e_1 \geqq 2$, which implies that the left-hand side is even. Thus, $e_2 - e_1 = 0$ and $e_3 - e_1 \geqq 1$. Then,

$${q_1}^2 + {q_2}^2 = 2^{m-2e_1} - 2^{2(e_3 - e_1)} {q_3}^2.$$

Since both of q_1 and q_2 are odd, ${q_1}^2 + {q_2}^2$ is a multiple of 2 but not of 4. This contradicts that $m - 2e_1 \geqq 2$ and $2(e_3 - e_1) \geqq 2$. Hence, the lemma has been proved. □

Lemma 3: Let w, x, y, z and m be positive integers. $w^2 + x^2 + y^2 + z^2 = 2^m$ if and only if m is even and $w = x = y = z = 2^{(m-2)/2}$.

Proof: w, x, y, z can be represented as

$$w = 2^{e_1} q_1,\ x = 2^{e_2} q_2,\ y = 2^{e_3} q_3,\ z = 2^{e_4} q_4,$$

where $e_1, \ldots, e_4 \geqq 0$, and $q_1, \ldots, q_4$ are odd integers. Without loss of generality, we may assume that $0 \leqq e_1 \leqq e_2 \leqq e_3 \leqq e_4$. Since $w^2 + x^2 + y^2 + z^2 = 2^m$,

$${q_1}^2 + 2^{2(e_2 - e_1)} {q_2}^2 + 2^{2(e_3 - e_1)} {q_3}^2 + 2^{2(e_4 - e_1)} {q_4}^2 = 2^{m-2e_1}.$$

Since the left-hand side of the above equation is greater than 4, $m - 2e_1 \geqq 2$. Since the right-hand side is even, $e_2 - e_1 = 0$. Thus,

$${q_1}^2 + {q_2}^2 + 2^{2(e_3 - e_1)} {q_3}^2 + 2^{2(e_4 - e_1)} {q_4}^2 = 2^{m-2e_1}.$$

Since both of q_1 and q_2 are odd, ${q_1}^2 + {q_2}^2$ is a multiple of 2 but not of 4, which implies $e_3 - e_1 = e_4 - e_1 = 0$ and ${q_1}^2 + {q_2}^2 + {q_3}^2 + {q_4}^2 = 2^{m-2e_1}$.

For $i = 1, 2, 3, 4$, q_i can be represented as $q_i = 2r_i + 1$, where $r_i \geqq 0$ is an integer. Hence,

$${q_1}^2 + {q_2}^2 + {q_3}^2 + {q_4}^2 = 2^{m-2e_1}$$
$$4\left(\sum_{i=1}^{4} r_i(r_i + 1) + 1\right) = 2^{m-2e_1}.$$

$m - 2e_1 = 2$ because $\sum_{i=1}^{4} r_i(r_i + 1) + 1$ is odd. Hence, m is even and $w = x = y = z = 2^{(m-2)/2}$. □

The following theorem presents a necessary and sufficient condition for $f \in \mathrm{B}_n$ to satisfy the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ for even $n \geqq 4$.

Theorem 2: Let $n \geqq 4$ be even. Let b_1, b_2, b_3 be different elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. $f \in \mathrm{B}_n$ satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_1, b_2, b_3\}$ if and only if

- $f \in \mathrm{PC}_n(n)$, or
- $b_1 \oplus b_2 \oplus b_3 = (0,\ldots,0)$ and

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{n/2+1} & \text{if } b_1 \cdot \omega = b_2 \cdot \omega = \\ & b_3 \cdot \omega = 0 \\ 0 & \text{otherwise} \end{cases}$$

or, for different $i, j, k \in \{1, 2, 3\}$,

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

Proof: Let $H_n = [v_0, \ldots, v_{2^n-1}]$. Since $f \in \mathrm{B}_n$ satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_1, b_2, b_3\}$, $\left[\hat{F}^2\right]$ can be represented as $\left[\hat{F}^2\right] = c_0 u_0 + c_1 u_1 + c_2 u_2 + c_3 u_3$, where $u_0 = {v_0}^{\mathrm{T}}$, $u_i = (v_0 + v_{dec(b_i)})^{\mathrm{T}}/2$ for $i = 1, 2, 3$.

For the case where $b_1 \oplus b_2 \oplus b_3 \neq (0,\ldots,0)$: Since $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$,

$$\begin{aligned} c_0 + (c_0 + c_1 + c_2 + c_3) &= 2^{n+1}, \\ (c_0 + c_1) + (c_0 + c_2 + c_3) &= 2^{n+1}, \\ (c_0 + c_2) + (c_0 + c_1 + c_3) &= 2^{n+1}, \\ (c_0 + c_3) + (c_0 + c_1 + c_2) &= 2^{n+1}. \end{aligned}$$

For each of the eight terms in the left-hand sides of the above four equations, it is easily proved that there exist 2^{n-3} $\hat{F}^2(\omega)$'s that are represented as it. This implies that all of the eight terms are square numbers, and, from Lemma 1, are equal to 2^n. Thus, $\hat{F}^2(\omega) = 2^n$ for every $\omega \in \{0,1\}^n$ and $f \in \mathrm{PC}_n(n)$.

For the case where $b_1 \oplus b_2 \oplus b_3 = (0,\ldots,0)$: It is easily proved that there exist 2^{n-2} $\hat{F}^2(\omega)$'s that are represented as each one of $c_0 + c_1 + c_2 + c_3$, $c_0 + c_1$, $c_0 + c_2$ and $c_0 + c_3$. Since

$$(c_0 + c_1 + c_2 + c_3) + (c_0 + c_1) + (c_0 + c_2) + (c_0 + c_3) = 2^{n+2},$$

from Lemma 1, 2, 3,

(Case 1) $c_0 + c_1 + c_2 + c_3 = c_0 + c_1 = c_0 + c_2 = c_0 + c_3 = 2^n$,

(Case 2) only one of $c_0 + c_1 + c_2 + c_3$, $c_0 + c_1$, $c_0 + c_2$ and $c_0 + c_3$ is 2^{n+2} and the others are 0.

For Case 1, $f \in \mathrm{PC}_n(n)$.

For Case 2, if $c_0 + c_1 + c_2 + c_3 = 2^{n+2}$, then $\hat{F}^2(\omega) = 2^{n+2}$ when $b_1 \cdot \omega = b_2 \cdot \omega = b_3 \cdot \omega = 0$. If $c_0 + c_i = 2^{n+2}$, then $\hat{F}^2(\omega) = 2^{n+2}$ when $b_i \cdot \omega = 0$ and $b_j \cdot \omega = b_k \cdot \omega = 1$ for different i, j, k.

Hence, the theorem has been proved. □

From the above theorem, for $f \in \mathrm{B}_n$ that satisfies the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ and that is not perfectly nonlinear, the number of non-zero $\hat{F}(\omega)$'s are 2^{n-2}. Let $b_1, b_2 \in \{0,1\}^n - \{(0,\ldots,0)\}$ such that $b_1 \neq b_2$. Let $\omega^0, \ldots, \omega^{2^{n-2}-1} \in \{0,1\}^n$ such that $b_1 \cdot \omega^i = b_1 \cdot \omega^j$, $b_2 \cdot \omega^i = b_2 \cdot \omega^j$, and $dec(\omega^i) < dec(\omega^j)$ for $0 \leqq i < j \leqq 2^{n-2} - 1$. $f \in \mathrm{B}_n$ satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_1, b_2, b_1 \oplus b_2\}$ and is not perfectly nonlinear if and only if there exists $g \in \mathrm{PC}_{n-2}(n-2)$ such that $\hat{F}(\omega^i)/2^{n/2+1} = \hat{g}(i)$ for $i = 0, \ldots, 2^{n-2} - 1$, and $\hat{F}(\omega) = 0$ if $\omega \neq \omega^i$. This fact is guaranteed by the following lemma and the definition of the Boolean bent functions.

Lemma 4: Let $n \geqq 2$, $b, c \in \{0,1\}^n - \{(0,\ldots,0)\}$ such that $b \neq c$ and $d_b, d_c \in \{0,1\}$. Let $G_n(b, c; d_b, d_c)$ be a $2^{n-2} \times 2^n$ matrix that is constructed by removing all $dec(\omega)$-th rows of H_n, where $b \cdot \omega \neq d_b$ or $c \cdot \omega \neq d_c$. Then, for each column v of H_{n-2},

- $G_n(b, c; 0, 0)$ has four columns that is equal to v,
- $G_n(b, c; d_b, d_c)$ has two columns that is equal to v and two columns that is equal to $-v$ for $(d_b, d_c) \neq (0, 0)$.

Proof: This lemma can be proved by induction. □

The following corollary can be easily derived from Theorem 2. This presents a spectral property of the balanced Boolean functions satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ for every even $n \geqq 4$.

Corollary 1: Let $n \geqq 4$ be even. Let b_1, b_2, b_3 be different elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. $f \in \mathrm{B}_n$ is balanced and satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_1, b_2, b_3\}$ if and only if $b_1 \oplus b_2 \oplus b_3 = (0,\ldots,0)$ and, for different $i, j, k \in \{1, 2, 3\}$,

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

□

Corollary 2: Let $n \geqq 4$ be even. The nonlinearity of any balanced Boolean function in B_n satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ is $2^{n-1} - 2^{n/2}$.

Proof: This corollary directly follows from Proposition 3 and Theorem 2. □

The following corollary presents the relationship between the number of balanced Boolean functions satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ and that of perfectly nonlinear Boolean functions. The number of perfectly nonlinear Boolean functions is an open question.

Corollary 3: Let $n \geqq 4$ be even. The number of balanced Boolean functions in B_n satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ is $\begin{pmatrix} 2^n - 1 \\ 2 \end{pmatrix} |\mathrm{PC}_{n-2}(n-2)|$. □

3.2 The Case Where The Number of Variables Is Odd

The following theorem shows that, for odd $n \geqq 3$, Boolean functions satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ if they satisfy the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

Theorem 3: Let $n \geqq 3$ be odd. Let b_1, b_2, b_3 be different elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. If $f \in \mathrm{B}_n$ satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_1, b_2, b_3\}$, then f satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_i\}$ for $i = 1, 2$, or 3.

Proof: Since $f \in \mathrm{B}_n$ satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b_1, b_2, b_3\}$, $\left[\hat{F}^2\right]$ can be rep-

resented as $\left[\hat{F}^2\right] = c_0u_0 + c_1u_1 + c_2u_2 + c_3u_3$, where $u_0 = {v_0}^{\mathrm{T}}$, $u_i = (v_0 + v_{dec(b_i)})^{\mathrm{T}}/2$ for $i = 1, 2, 3$.

For the case where $b_1 \oplus b_2 \oplus b_3 \neq (0, \ldots, 0)$: Since $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$,

$$\begin{aligned} c_0 + (c_0 + c_1 + c_2 + c_3) &= 2^{n+1}, \\ (c_0 + c_1) + (c_0 + c_2 + c_3) &= 2^{n+1}, \\ (c_0 + c_2) + (c_0 + c_1 + c_3) &= 2^{n+1}, \\ (c_0 + c_3) + (c_0 + c_1 + c_2) &= 2^{n+1}. \end{aligned}$$

For each of the eight terms in the left-hand sides of the above four equations, it is easily proved that there exist 2^{n-3} $\hat{F}^2(\omega)$'s that are represented as it. From Lemma 1, it is easily derived that two of c_1, c_2, c_3 are 0.

For the case where $b_1 \oplus b_2 \oplus b_3 = (0, \ldots, 0)$: It is easily proved that there exist 2^{n-2} $\hat{F}^2(\omega)$'s that are represented as each one of $c_0 + c_1 + c_2 + c_3$, $c_0 + c_1$, $c_0 + c_2$ and $c_0 + c_3$. Since

$$\begin{aligned} &(c_0 + c_1 + c_2 + c_3) + (c_0 + c_1) \\ &\quad + (c_0 + c_2) + (c_0 + c_3) = 2^{n+2}, \end{aligned}$$

from Lemma 1, 2, 3, two of $c_0 + c_1 + c_2 + c_3$, $c_0 + c_1$, $c_0 + c_2$, and $c_0 + c_3$ are 2^{n+1}, and the others are 0. For this case, it is also derived that two of c_1, c_2, c_3 are 0.

From the above discussion, $\left[\hat{F}^2\right]$ can be represented as $\left[\hat{F}^2\right] = c_0u_0 + c_iu_i$ for $i = 1, 2$, or 3. Hence, the theorem has been proved. □

4. Balanced Boolean Functions Satisfying the PC of Degree $n-2$

4.1 The Case Where n Is Even

In this section, it is proved that, for even $n \geq 4$, there exist no n-input balanced Boolean functions satisfying the PC of degree $n - 2$.

Firstly, we present a simple lemma.

Lemma 5: Let $n \geq 2$. Let $H_n = [v_0, \ldots, v_{2^n-1}]$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \{0, 1\}^n$. Then, for $v_{2^n-1-2^{n-1-i}}$ for $i = 0, 1, \ldots, n-1$ and v_{2^n-1},

- if $W(\alpha)$ is even, then
  - the $dec(\alpha)$-th element of v_{2^n-1} is 1,
  - the $dec(\alpha)$-th element of $v_{2^n-1-2^{n-1-i}}$ is 1 if and only if $\alpha_{n-i} = 0$,
- if $W(\alpha)$ is odd, then
  - the $dec(\alpha)$-th element of v_{2^n-1} is -1,
  - the $dec(\alpha)$-th element of $v_{2^n-1-2^{n-1-i}}$ is 1 if and only if $\alpha_{n-i} = 1$.

Proof: This lemma can be proved from the fact that, for each i such that $0 \leq i \leq n-1$, the $dec(\omega)$-th element of $v_{2^n-1-2^{n-1-i}}$ is $(-1)^{\omega_1 \oplus \cdots \oplus \omega_{n-i-1} \oplus \omega_{n-i+1} \oplus \cdots \oplus \omega_n}$, and that the $dec(\omega)$-th element of v_{2^n-1} is $(-1)^{\omega_1 \oplus \cdots \oplus \omega_n}$, where $\omega = (\omega_1, \ldots, \omega_n) \in \{0, 1\}^n$. □

Theorem 4: For even $n \geq 4$, there exist no n-input balanced Boolean functions that satisfy the PC of degree $n - 2$.

Proof: We assume that $f \in \mathrm{PC}_n(n-2)$ and f is balanced. Let $H_n = [v_0, \ldots, v_{2^n-1}]$. Then, from Proposition 1, $\left[\hat{F}^2\right] v_{dec(a)} = 0$ for every $a \in \{0, 1\}^n$ such that $1 \leq W(a) \leq n-2$. Thus, $\left[\hat{F}^2\right]$ is able to be represented as a linear combination of the transposes of $v_0, v_{2^n-1-2^{n-1}}, v_{2^n-1-2^{n-2}}, \ldots, v_{2^n-2}, v_{2^n-1}$. For every $1 \leq i \leq n$, let

$$u_i = ({v_0}^{\mathrm{T}} + {v_{2^n-1-2^{n-i}}}^{\mathrm{T}})/2,$$

and $u_0 = {v_0}^{\mathrm{T}}$, $u_{n+1} = ({v_0}^{\mathrm{T}} + {v_{2^n-1}}^{\mathrm{T}})/2$. Then,

$$\left[\hat{F}^2\right] = c_0u_0 + c_1u_1 + \cdots + c_{n+1}u_{n+1}.$$

Hence, from Lemma 5,

- $\hat{F}^2(0) = c_0 + c_1 + \cdots + c_{n+1}$,
- $\hat{F}^2(2^i) = c_0 + c_{n-i}$ for $i = 0, 1, \ldots, n-1$,
- $\hat{F}^2(\sum_{k=2j}^{n-1} 2^k) = c_0 + \sum_{l=n+1-2j}^{n+1} c_l$ for $j = 0, 1, \ldots, n/2-1$,
- $\hat{F}^2(2^i + 2^j + 2^k) = c_0 + c_{n-i} + c_{n-j} + c_{n-k}$ for $0 \leq i < j < k \leq n-1$.

Since $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$,

$$\begin{aligned} 2^n c_0 + 2^{n-1}(c_1 + \cdots + c_{n+1}) &= 2^{2n} \\ c_0 + (c_0 + c_1 + \cdots + c_{n+1}) &= 2^{n+1}. \end{aligned}$$

$\hat{F}(0) = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} = 0$, because f is balanced. Hence, $c_0 = 2^{n+1}$.

$$\begin{aligned} &\hat{F}^2(2^{n-1}) + \hat{F}^2(2^{n-2}) + \hat{F}^2(2^{n-2} + 2^{n-1}) \\ &= (c_0 + c_1) + (c_0 + c_2) + (c_0 + c_3 + \cdots + c_{n+1}) \\ &= 2c_0 + (c_0 + c_1 + \cdots + c_{n+1}) \\ &= 2^{n+2}. \end{aligned}$$

From Lemma 1, 2,

1. $c_0 + c_1 = 2^{n+2}$, $c_0 + c_2 = 0$, $c_0 + c_3 + \cdots + c_{n+1} = 0$,
2. $c_0 + c_1 = 0$, $c_0 + c_2 = 2^{n+2}$, $c_0 + c_3 + \cdots + c_{n+1} = 0$,

or

Table 1 Bounds of the degree of the PC of balanced Boolean functions.

number of variables	4	6	8	10	12	14	16	18	20	22	24	26
upper bound	1	3	5	7	9	11	13	15	17	19	21	23
lower bound	1	3	4	5	7	8	9	11	12	13	15	16

3. $c_0+c_1=0$, $c_0+c_2=0$, $c_0+c_3+\cdots+c_{n+1}=2^{n+2}$.

Since $c_0=2^{n+1}$, these three cases are summarized as follows:

(Case 1) One of c_1 and c_2 is -2^{n+1}, the other is 2^{n+1}, and $c_0+c_3+\cdots+c_{n+1}=0$,

(Case 2) $c_1=c_2=-2^{n+1}$, and $c_0+c_3+\cdots+c_{n+1}=2^{n+2}$.

For Case 1: Since $c_0+c_3+\cdots+c_{n+1}=0$, for $\hat{F}^2(2^{n-3})=c_0+c_3$, $\hat{F}^2(2^{n-4})=c_0+c_4$, and $\hat{F}^2(2^{n-4}+2^{n-3}+2^{n-2}+2^{n-1})=c_0+c_5+\cdots+c_{n+1}$, the same argument as the above one shows that

(Case 1.1) One of c_3 and c_4 is -2^{n+1}, the other is 2^{n+1}, and $c_0+c_5+\cdots+c_{n+1}=0$,

(Case 1.2) $c_3=c_4=-2^{n+1}$, and $c_0+c_5+\cdots+c_{n+1}=2^{n+2}$.

For Case 1.1, if $n=4$, then $c_0+c_5=0$ and $c_5=-2^{n+1}=-32$. Thus, three of $c_1,\ldots,c_5$ are -32, which implies that, from Lemma 5, there exists some ω such that $\hat{F}^2(\omega)=-32$. This is a contradiction.

If $n\geqq 6$, then it can be shown that at least one of c_5 and c_6 is -2^{n+1}, which means that at least three of $c_1,\ldots,c_6$ are -2^{n+1}.

For Case 1.2, three of $c_1,\ldots,c_4$ is -2^{n+1}.

For Case 2: Since $c_0+c_3+\cdots+c_{n+1}=2^{n+2}$,

$$\begin{aligned}&(c_0+c_3)+(c_0+c_4)+(c_0+c_5+\cdots+c_{n+1})\\&=2c_0+(c_0+c_3+\cdots+c_{n+1})\\&=2^{n+3}.\end{aligned}$$

From Lemma 1, 2,

(Case 2.1) One of c_3 and c_4 is -2^{n+1}, the other is 2^{n+1}, and $c_0+c_5+\cdots+c_{n+1}=2^{n+2}$,

(Case 2.2) $c_3=c_4=2^{n+1}$, and $c_0+c_5+\cdots+c_{n+1}=0$.

For Case 2.1, three of $c_1,\ldots,c_4$ are -2^{n+1}.

For Case 2.2, when $n=4$, $c_1=c_2=-2^{n+1}$ and, since $c_0+c_5=0$, $c_5=-2^{n+1}$. When $n\geqq 6$, at least one of c_5 and c_6 is -2^{n+1}.

Hence, the theorem has been proved. □

Theorem 4 implies that n-input balanced Boolean functions satisfy the PC of degree at most $n-3$. As for the lower bound, the following theorem has been proved.

Theorem 5 [7]: Let $n\geqq 4$ be even. Suppose that $n=3t+c$, where $c=0,1$, or 2. Then there exist balanced Boolean functions in B_n that satisfy the PC of degree $2t-1$ when $c=0,1$ or $2t$ when $c=2$. □

From the above two theorems, the bounds are tight for $n=4,6$. Table 1 shows the bounds on the degree of the PC of balanced Boolean functions.

4.2 The Case Where n Is Odd

In this section, it is shown that, for odd $n\geqq 3$, every balanced $f\in \mathrm{PC}_n(n-2)$ satisfies the PC with respect to all but one elements in $\{0,1\}^n-\{(0,\ldots,0)\}$.

Lemma 6: Let $x,y,z\geqq 0$ be integers and $m\geqq 0$ be an even integer. $x^2+y^2+z^2=3\cdot 2^m$ if and only if $x=y=z=2^{m/2}$.

Proof: x,y,z can be represented as

$$x=2^{e_1}q_1,\ y=2^{e_2}q_2,\ z=2^{e_3}q_3,$$

where $e_1,e_2,e_3\geqq 0$, and each of q_1,q_2,q_3 is 0 or odd.

(i) If we assume that $y=z=0$, then $x^2=3\cdot 2^m$, which contradicts that x is an integer.

(ii) Suppose that $x\neq 0$, $y\neq 0$, $z=0$. Then, $2^{2e_1}{q_1}^2+2^{2e_2}{q_2}^2=3\cdot 2^m$. Since, without loss of generality, we can assume that $e_2\geqq e_1\geqq 0$,

$${q_1}^2+2^{2(e_2-e_1)}{q_2}^2=3\cdot 2^{m-2e_1}.$$

If $e_1=e_2$, then ${q_1}^2+{q_2}^2$ is a multiple of 2 but not of 4. This implies that $m-2e_1=1$, which contradicts that m is even.

If $e_1<e_2$, then the left-hand side is odd and $m-2e_1=0$. Thus, ${q_1}^2+2^{2(e_2-e_1)}{q_2}^2=3$, which implies that $2(e_2-e_1)=1$. This contradicts that e_1 and e_2 are integers.

(iii) Suppose that none of x,y,z is 0. Without loss of generality, we may assume that $0\leqq e_1\leqq e_2\leqq e_3$.

$$\begin{aligned}2^{2e_1}{q_1}^2+2^{2e_2}{q_2}^2+2^{2e_3}{q_3}^2&=3\cdot 2^m\\{q_1}^2+2^{2(e_2-e_1)}{q_2}^2+2^{2(e_3-e_1)}{q_3}^2&=3\cdot 2^{m-2e_1}.\end{aligned}$$

If we assume that $e_1\neq e_2$ and $e_1\neq e_3$, or $e_1=e_2=e_3$, then the left-hand side is odd. This implies that $m-2e_1=0$ and

$${q_1}^2+2^{2(e_2-e_1)}{q_2}^2+2^{2(e_3-e_1)}{q_3}^2=3.$$

Since $q_1,q_2,q_3\geqq 1$, $e_1=e_2=e_3=m/2$ and $q_1=q_2=q_3=1$.

If we assume that $e_1=e_2$ and $e_1\neq e_3$, then

${q_1}^2+{q_2}^2 = 3\cdot 2^{m-2e_1} - 2^{2(e_3-e_1)}{q_3}^2$. Since ${q_1}^2+{q_2}^2$ is a multiple of 2 but not of 4, $m-2e_1 = 1$ or $2(e_3-e_1) = 1$. This situation cannot occur because m is even.

Hence, the lemma has been proved. □

Theorem 6: For every odd $n \geqq 3$, if $f \in \mathrm{PC}_n(n-2)$ is balanced, then, for some $b \in \{0,1\}^n$ such that $W(b) \geqq n-1$, f satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b\}$.

Proof: We assume that $f \in \mathrm{PC}_n(n-2)$ and f is balanced. Then, $\left[\hat{F}^2\right]$ is able to be represented as

$$\left[\hat{F}^2\right] = c_0u_0 + c_1u_1 + \cdots + c_{n+1}u_{n+1},$$

where for every $1 \leqq i \leqq n$,

$$u_i = ({v_0}^{\mathrm{T}} + {v_{2^n-1-2^{n-i}}}^{\mathrm{T}})/2,$$

$u_0 = {v_0}^{\mathrm{T}}$, and $u_{n+1} = ({v_0}^{\mathrm{T}} + {v_{2^n-1}}^{\mathrm{T}})/2$.

Hence, from Lemma 5,

- $\hat{F}^2(0) = c_0 + c_1 + \cdots + c_{n+1}$,
- $\hat{F}^2(2^i) = c_0 + c_{n-i}$ for $i = 0,1,\ldots,n-1$,
- $\hat{F}^2(\sum_{k=2j}^{n-1} 2^k) = c_0 + \sum_{l=n+1-2j}^{n+1} c_l$ for $j = 0,1,\ldots,n/2-1$,
- $\hat{F}^2(2^i + 2^j + 2^k) = c_0 + c_{n-i} + c_{n-j} + c_{n-k}$ for $0 \leqq i < j < k \leqq n-1$.

Since

$$\sum_{\omega\in\{0,1\}^n} \hat{F}^2(\omega) = 2^{2n} \text{ and } \hat{F}(0) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)} = 0,$$

$c_0 + c_1 + \cdots + c_{n+1} = 0$ and $c_0 = 2^{n+1}$.

Since

$$\begin{aligned}&\hat{F}^2(2^{n-1}) + \hat{F}^2(2^{n-2}) + \hat{F}^2(2^{n-2}+2^{n-1})\\ &= (c_0+c_1) + (c_0+c_2) + (c_0+c_3+\cdots+c_{n+1})\\ &= 2c_0 + (c_0+c_1+\cdots+c_{n+1})\\ &= 2^{n+2},\end{aligned}$$

from Lemma 1, 2,

1. $c_0+c_1 = 0$, $c_0+c_2 = 2^{n+1}$, $c_0+c_3+\cdots+c_{n+1} = 2^{n+1}$,
2. $c_0+c_1 = 2^{n+1}$, $c_0+c_2 = 0$, $c_0+c_3+\cdots+c_{n+1} = 2^{n+1}$, or
3. $c_0+c_1 = 2^{n+1}$, $c_0+c_2 = 2^{n+1}$, $c_0+c_3+\cdots+c_{n+1} = 0$.

Since $c_0 = 2^{n+1}$, these three cases are summarized as follows:

(Case 1) One of c_1 and c_2 is -2^{n+1} the other is 0, and $c_0+c_3+\cdots+c_{n+1} = 2^{n+1}$,

(Case 2) $c_1 = c_2 = c_0+c_3+\cdots+c_{n+1} = 0$.

For Case 1: When $n = 3$, $c_0+c_3+c_4 = 2^4$ and $(c_0+c_3)+(c_0+c_4) = 2^5$. Thus $c_3 = c_4 = 0$.

When $n \geqq 5$, since $c_0+c_3+\cdots+c_{n+1} = 2^{n+1}$, for $\hat{F}^2(2^{n-3}) = c_0+c_3$, $\hat{F}^2(2^{n-4}) = c_0+c_4$, and $\hat{F}^2(2^{n-4}+2^{n-3}+2^{n-2}+2^{n-1}) = c_0+c_5+\cdots+c_{n+1}$,

$$\begin{aligned}&(c_0+c_3)+(c_0+c_4)+(c_0+c_5+\cdots+c_{n+1})\\ &= 2c_0 + (c_0+c_3+\cdots+c_{n+1})\\ &= 3\cdot 2^{n+1}.\end{aligned}$$

Thus, from Lemma 6, $c_3 = c_4 = c_0+c_5+\cdots+c_{n+1} = 0$.

For Case 2: When $n = 3$, $(c_0+c_3)+(c_0+c_4) = 2^4$. Thus one of c_3 and c_4 is -2^4 and the other is 0.

When $n \geqq 5$, since $c_0+c_3+\cdots+c_{n+1} = 0$,

$$\begin{aligned}&(c_0+c_3)+(c_0+c_4)+(c_0+c_5+\cdots+c_{n+1})\\ &= 2c_0 + (c_0+c_3+\cdots+c_{n+1})\\ &= 2^{n+2}.\end{aligned}$$

(Case 2.1) One of c_3 and c_4 is -2^{n+1} and the other is 0, and $c_0+c_5+\cdots+c_{n+1} = 2^{n+1}$.

(Case 2.2) $c_3 = c_4 = c_0+c_5+\cdots+c_{n+1} = 0$.

From the above discussion, each of $c_1,\ldots,c_{n+1}$ is 0 or -2^{n+1} and at least one of $c_1,\ldots,c_{n+1}$ is -2^{n+1}. Thus, only one of $c_1,\ldots,c_{n+1}$ is -2^{n+1} since $\hat{F}^2(0,\ldots,0) = c_0+c_1+\cdots+c_{n+1} = 0$. Hence, the theorem has been proved. □

The following theorem has been proved for Boolean functions satisfying the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

Theorem 7[2]: Let $n \geqq 3$ odd and $b \in \{0,1\}^n - \{(0,\ldots,0)\}$. Balanced $f \in \mathrm{B}_n$ satisfies the PC with respect to $\{0,1\}^n - \{(0,\ldots,0)\} - \{b\}$ if and only if

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

□

The following corollaries can be derived from the above two theorems.

Corollary 4: For every odd $n \geqq 3$, the number of balanced Boolean functions in $\mathrm{PC}_n(n-2)$ is $(n+1)|\mathrm{PC}_{n-1}(n-1)|$. □

Corollary 5: For every odd $n \geqq 3$, the nonlinearities of balanced Boolean functions in $\mathrm{PC}_n(n-2)$ is $2^{n-1} - 2^{(n-1)/2}$. □

5. Conclusion

This paper has discussed Boolean functions satisfying the PC and their balancedness.

Firstly, we have discussed Boolean functions with n variables satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. For even $n \geqq$

4, a necessary and sufficient condition has been presented for Boolean functions with n variables to satisfy the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. This implies that all of these Boolean functions can be constructed from all perfectly nonlinear Boolean functions with $n-2$ variables. For odd $n \geqq 3$, it has been also shown that Boolean functions with n variables satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ satisfy the PC with respect to all but one elements in it.

Secondly, Boolean functions in $\mathrm{PC}_n(n-2)$ has been considered. For even $n \geqq 4$, an upper bound of $n-3$ has been given to the degree of the PC of balanced Boolean functions with n variables. This bound is optimal for $n = 4, 6$. For odd $n \geqq 3$, it has been proved that balanced Boolean functions in $\mathrm{PC}_n(n-2)$ satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

An open question is whether there exist balanced Boolean functions with n variables satisfying the PC of degree $n-3$ for even n.

References

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

[2] Hirose, S. and Ikeda, K., "Relationships among nonlinearity criteria of Boolean functions," *Submitted to IEICE Trans. Fundamentals*, 1994.

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

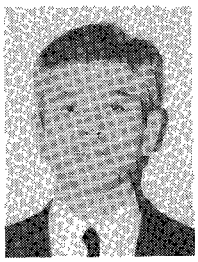
[4] Preneel, B., Leekwijk, W.V., Linden, L.V., Govaerts, R. and Vandewalle, J., "Propagation characteristics of Boolean functions," *Proc. EUROCRYPT'90, LNCS*, no.473, pp.161–173, 1991.

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

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

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

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, IECEJ, 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).