The Nonhomomorphicity of S-boxes

Yuliang Zheng[1] and Xian-Mo Zhang[2]

[1] School of Comp & Info Tech, Monash University, McMahons Road, Frankston, Melbourne, VIC 3199, Australia. E-mail: yuliang@pscit.monash.edu.au
URL: http://www.pscit.monash.edu.au/links/

[2] School of Info Tech & Comp Sci, the University of Wollongong, Wollongong NSW 2522, Australia. E-mail: xianmo@cs.uow.edu.au

Abstract. In this paper, we introduce the concept of kth-order *nonhomomorphicity* of mappings or S-boxes as an alternative indicator that forecasts nonlinearity characteristics of an S-box, where $k \geq 4$ is even. Main results of this paper include: (1) we show that nonhomomorphicity, especially the 4th order nonhomomorphicity, can be precisely expressed by using other important nonlinear indicators of an S-box. (2) we establish tight lower and upper bounds on the nonhomomorphicity of S-boxes, (3) we identify the mean of nonhomomorphicity over all the S-boxes with the same size and the relative nonhomomorphicity of an S-box, both of which are useful in estimating, statistically, the nonhomomorphicity of an S-box.

Key Words

Sequences, Boolean Functions, S-boxes, Cryptanalysis, Cryptography, Nonhomomorphicity.

1 Motivation of this Research

The so-called S-boxes, which are functionally identical to mappings or tuples of Boolean functions, are of critical importance to the strength of a block cipher. In the past decade, the analysis and design of S-boxes has attracted a tremendous amount of attention. This paper focuses on new methods or perspectives for the analysis of S-boxes. More specifically, it deals with a new nonlinearity indicator called *nonhomomorphicity*.

To understand the motivation behind the new concept, let us first note that a mapping F from V_n to V_m is affine, i.e., $F(x) = xB \oplus \beta$ where $x \in V_n$, B is a fixed $n \times m$ matrix, if and only if F satisfies such property that for any even number k with $k \geq 4$, $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$.

Now consider a non-affine function F on V_n. If $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ then F satisfies the affine property at the particular vector $(u_1, \ldots, u_k)$. On the other hand, if $F(u_1) \oplus \cdots \oplus F(u_k) \neq 0$ then F behaves in a way that is against the affine property at $(u_1, \ldots, u_k)$.

The above discussions indicate that $F(u_1) \oplus \cdots \oplus F(u_k) \neq 0$ is a useful characteristic that differentiates a non-affine function from an affine one. This leads us to considering the number of vectors in V_n, $(u_1, \ldots, u_k)$ with $u_1 \oplus \cdots \oplus u_k = 0$ satisfying $F(u_1) \oplus \cdots \oplus F(u_k) \neq 0$ as a new nonlinearity criterion. We call this new criterion the kth-order nonhomomorphicity of F.

Nonhomomorphicity has several interesting properties including (1) it explores a new non-affine property; (2) it can be precisely calculated by other indicators; (3) the mean of nonhomomorphicity over all the S-boxes with the same size can be precisely identified; (4) there exists a fast statistical method to estimate the nonhomomorphicity of an S-box.

In this paper we restrict our attention to the 4th-order nonhomomorphicity of S-boxes, due to the fact that 4 is the smallest order and hence it is easy to handle. Furthermore, the 4th-order nonhomomorphicity of S-boxes is closely related to many other criteria, a property apparently not shared by a higher order nonhomomorphicity.

[9] has studied a special case when the mapping F degenerates to a Boolean function, i.e., a mapping from V_n to V_1. It turns out that the analysis of the nonhomomorphicity of a general mapping from V_n to V_m is far more complex than what we thought as first. As the analysis employs a number of new techniques, the results in this paper represent non-trivial generalization of those in [9].

The rest of this paper is organized as follows: In Section 2, we introduce the basic definitions and notations used in this paper. In Section 3, we explain reasons why we study the nonhomomorphicity of S-boxes. In Section 4, we give three precise characterizations of the nonhomomorphicity of S-boxes by the use of other indicators. These characterizations indicate close relationships between nonhomomorphicity and other important criteria. This is followed by Section 5 where we establish tight upper and lower bounds on the nonhomomorphicity of S-boxes. In Section 6, we establish the mean of nonhomomorphicity of all the S-boxes with the same size. In Section 7, we show that the mean of nonhomomorphicity and the relative nonhomomorphicity are relevant to a statistical method for estimating the nonhomomorphicity of S-boxes. An example application of nonhomomorphicity is given in Section 8.

2 Basic Definitions

Definition 1. *Denote by V_n the vector space of n tuples of elements from $GF(2)$. The* truth table *of a function f from V_n to $GF(2)$ (or simply functions on V_n) is a $(0,1)$-sequence defined by $(f(\alpha_0),\ f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$, and the* sequence *of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$, where $\alpha_0 = (0, \ldots, 0, 0)$, $\alpha_1 = (0, \ldots, 0, 1)$, ..., $\alpha_{2^{n-1}-1} = (1, \ldots, 1, 1)$. f is said to be* balanced *if its truth table contains an equal number of ones and zeros.*

Definition 2. *A function f on V_n is called an* affine *function if $f(x) = c \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$ where each a_j and c are constant in $GF(2)$. In particular, f is called a* linear *function if $c = 0$. A mapping from V_n to V_m, F, is an* affine (linear) *if all the component functions of F are affine (linear).*

Definition 3. *The* Hamming weight *of a* $(0,1)$*-sequence* ξ *is the number of ones in the sequence. Given two functions* f *and* g *on* V_n*, the* Hamming distance $d(f,g)$ *between them is defined as the Hamming weight of the truth table of* $f(x) \oplus g(x)$*, where* $x = (x_1, \ldots, x_n)$*. The* nonlinearity *of* f*, denoted by* N_f*, is the minimal Hamming distance between* f *and all affine functions on* V_n*, i.e.,* $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \varphi_i)$ *where* φ_1*,* φ_2*, …,* $\varphi_{2^{n+1}}$ *are all the affine functions on* V_n*.*

Given two sequences $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$, their component-wise product is denoted by $a*b$, while the scalar product (sum of component-wise products) is denoted by $\langle a, b\rangle$.

The *Sylvester-Hadamard matrix (or Walsh-Hadamard matrix)* of order 2^n, denoted by H_n, is generated by the recursive relation $H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$, $n = 1, 2, \ldots,$ $H_0 = 1$. Each row (column) of H_n is a linear sequence of length 2^n.

A function f on V_n is called a *bent function* [7] if $\langle \xi, \ell_i\rangle^2 = 2^n$ for every $i = 0, 1, \ldots, 2^n - 1$, where ξ is the sequence of f and ℓ_i is a row in H_n. A bent function on V_n exists only when n is a positive even number, and it achieves the highest possible nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$.

The nonlinearity of f on V_n can be expressed by

$$N_f = 2^{n-1} - \frac{1}{2}\max\{|\langle \xi, \ell_i\rangle|, 0 \le i \le 2^n - 1\} \tag{1}$$

where ξ is the sequence of f and ℓ_0, …, ℓ_{2^n-1} are the rows of H_n, namely, the sequences of linear functions on V_n. The proof can be found in, for instance, [4].

Definition 4. *Let* f *be a function on* V_n*. For a vector* $\alpha \in V_n$*, denote by* $\xi(\alpha)$ *the sequence of* $f(x \oplus \alpha)$*. Thus* $\xi(0)$ *is the sequence of* f *itself and* $\xi(0) * \xi(\alpha)$ *is the sequence of* $f(x) \oplus f(x \oplus \alpha)$*. Let* $\Delta(\alpha)$ *be the scalar product of* $\xi(0)$ *and* $\xi(\alpha)$*. Namely* $\Delta(\alpha) = \langle \xi(0), \xi(\alpha)\rangle$ $\Delta(\alpha)$ *is called the* auto-correlation of f *with a shift* α*.*

The following formula is well known to the researchers. A simple proof together with applications can be found, for instance, in [8]

$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (\langle \xi, \ell_0\rangle^2, \langle \xi, \ell_1\rangle^2, \ldots, \langle \xi, \ell_{2^n-1}\rangle^2)$ where α_i is the binary representation of an integer i and ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Hence it is easy to verify

$$2^n \sum_{i=0}^{2^n-1} \Delta^2(\alpha_i) = \sum_{i=0}^{2^n-1} \langle \xi, \ell_i\rangle^4 \tag{2}$$

Definition 5. *An* $n \times m$ S-box or substitution box *is a mapping from* V_n *to* V_m*, i.e.,* $F = (f_1, \ldots, f_m)$*, where* n *and* m *are integers with* $n \ge m \ge 1$ *and each component function* f_j *is a function on* V_n*. In this paper, we use the terms of mapping and S-box interchangeably.* F *is an affine mapping if it can be written as* $F(x) = xB \oplus \beta$*, where* $x = (x_1, \ldots, x_n)$*,* B *is an* $n \times m$ *matrix on* $GF(2)$*, and* β *a vector in* V_m*. When* β *is the zero vector,* F *is said to be linear.*

The concept of nonlinearity can be extended to the case of an S-box [6].

Definition 6. *The* nonlinearity *of $F = (f_1, \dots, f_m)$ is defined as*

$$N_F = min_g\{N_g | g = \bigoplus_{j=1}^{m} c_j f_j,\ c_j \in GF(2), (c_1, \dots, c_m) \neq (0, \dots, 0)\}.$$

3 Nonhomomorphicity of S-boxes

The following lemma is important in this paper, as it explores a characteristic property of affine mappings which will be useful in studying nonhomomorphicity.

Lemma 1. *Let F be an $n \times m$ mapping.*

(i) If F is an affine mapping then F satisfies such property that for any even number k with $k \geq 4$, $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$,
(ii) if there exists an even number k with $k \geq 4$ such that $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$, then F is an affine mapping.

Proof. We first prove Part (ii) of the lemma. Assume that there exists an even number k with $k \geq 4$ such that $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$. We now prove that F is affine. Let u_1 and u_2 be any two vectors in V_n. Obviously, the k vectors u_1, u_2, $u_1 \oplus u_2$, $0, \dots, 0$ satisfy $u_1 \oplus u_2 \oplus (u_1 \oplus u_2) \oplus 0 \oplus \cdots \oplus 0 = 0$. From the assumption,

$$F(u_1) \oplus F(u_2) \oplus F(u_1 \oplus u_2) \oplus F(0) \oplus \cdots \oplus F(0) = 0 \tag{3}$$

There are two cases to be examined: $F(0) = 0$ and $F(0) \neq 0$.

Case 1: $F(0) = 0$. In this case $F(c\alpha) = cF(\alpha)$ holds for any vector $\alpha \in V_n$ and any value $c \in GF(2)$. Hence (3) can be rewritten as

$$F(u_1 \oplus u_2) = F(u_1) \oplus F(u_2) \tag{4}$$

where u_1 and u_2 are arbitrary.

Let e_j denote the vector in V_n, whose the jth component is one and others are zero. For any fixed value x_j in $GF(2)$, $j = 1, \dots, n$, from (4), $F(x_1 e_1 \oplus \cdots \oplus x_n e_n) = F(x_1 e_1) \oplus F(x_2 e_2 \oplus \cdots \oplus x_n e_n)$. Applying (4) repeatedly, we have $F(x_1 e_1 \oplus \cdots \oplus x_n e_n) = F(x_1 e_1) \oplus F(x_2 e_2) \oplus \cdots \oplus F(x_n e_n)$. Note that $F(0) = 0$ implies $F(c\alpha) = cF(\alpha)$ where c is any value in $GF(2)$ and α is any vector in V_n. Hence

$$F(x_1 e_1 \oplus \cdots \oplus x_n e_n) = x_1 F(e_1) \oplus \cdots \oplus x_n F(e_n) \tag{5}$$

From the definition of e_j, $x_1 e_1 \oplus \cdots \oplus x_n e_n = (x_1, \dots, x_n)$. On the other hand, if we write $F(e_j) = \beta_j$ where $\beta_j \in V_m$, $j = 1, \dots, n$. Then (5) can be rewritten as $F(x_1, \dots, x_n) = x_1 \beta_1 \oplus \cdots \oplus x_n \beta_n$ or $F(x_1, \dots, x_n) = (x_1, \dots, x_n)B$ where

$B = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$ where B is an $n \times m$ matrix over $GF(2)$ and each β_i regarded as a row vector of B.

Case 2: $F(0) = \beta$ with $\beta \neq 0$. Set $G(x) = \beta \oplus F(x)$. Then G is linear. By using the result in Case 1, $G(x_1, \ldots, x_n) = (x_1, \ldots, x_n)B$ where B is an $n \times m$ matrix over $GF(2)$. Hence $F(x_1, \ldots, x_n) = (x_1, \ldots, x_n)B \oplus \beta$. This proves that F is affine.

We now prove Part (i) of the lemma. Assume that F is affine. From Definition 5, it is easy to check that for any even number k with $k \geq 4$, $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$. □

From the characteristic property shown in Lemma 1, if a mapping F on V_n satisfies $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ for a large number of k-tuples $(u_1, \ldots, u_k)$ of vectors in V_n with $u_1 \oplus \cdots \oplus u_k = 0$, then the mapping behaves more like an affine function. This leads us to introduce a new nonlinearity criterion.

Notation 1. *Let F be a mapping from V_n to V_m and k an even number with $4 \leq k \leq 2^n$. Denote by $\mathcal{H}_{F,\beta}^{(k)}$ the collection of ordered k-tuples $(u_1, u_2, \ldots, u_k)$ of vectors in V_n such that*

$$\begin{aligned} \mathcal{H}_{F,\beta}^{(k)} = \{(u_1, u_2, \ldots, u_k) | u_j \in V_n,\ & u_1 \oplus u_2 \oplus \cdots \oplus u_k = 0, \\ & F(u_1) \oplus F(u_2) \oplus \cdots \oplus F(u_k) = \beta\} \end{aligned}$$

where $\beta \in V_m$. Let $\tilde{q}_{F,\beta}^{(k)}$ denote the number of elements in $\mathcal{H}_{F,\beta}^{(k)}$, i.e., $\tilde{q}_{F,\beta}^{(k)} = \#\mathcal{H}_{F,\beta}^{(k)}$.

Definition 7. *Let F be a mapping from V_n to V_m and k an even number with $4 \leq k \leq 2^n$. Write*

$$\begin{aligned} Q_F^{(k)} = \{(u_1, \ldots, u_k) | u_j \in V_n,\ & u_1 \oplus u_2 \oplus \cdots \oplus u_k = 0, \\ & F(u_1) \oplus F(u_2) \oplus \cdots \oplus F(u_k) \neq 0\} \end{aligned} \tag{6}$$

Let $\tilde{q}_F^{(k)}$ be the number of elements in $Q_F^{(k)}$, i.e., $\tilde{q}_F^{(k)} = \#Q_F^{(k)}$. We call $\tilde{q}_F^{(k)}$ the kth-order nonhomomorphicity *of F.*

Note that there exist $2^{(k-1)n}$ k-tuples of vectors in V_n, $(u_1, \ldots, u_k)$, satisfying $u_1 \oplus \cdots \oplus u_k = 0$. Hence

Lemma 2. *Let F be an $n \times m$ mapping. Then $\sum_{\beta \in V_n} \tilde{q}_{F,\beta}^{(k)} = 2^{(k-1)n}$ or $\tilde{q}_F^{(k)} + \tilde{q}_{F,0}^{(k)} = 2^{(k-1)n}$.*

Lemma 1 indicates that when discussing the nonhomomorphic characteristics of a mapping, we may focus on a single even number k, rather than on all even number k. Therefore we will focus on $\tilde{q}_F^{(4)}$. An obvious advantage of restricting to a small $k = 4$ is that it would make the task of computing or estimating $\tilde{q}_F^{(4)}$ easier. Another reason why we prefer $\tilde{q}_F^{(4)}$ to a general $\tilde{q}_F^{(k)}$ is that we have found interesting relationships between $\tilde{q}_F^{(4)}$ and many other criteria. Furthermore, this case has the following interesting property.

Notation 2. *Let $O_n^{(4)}$ denote the collection of ordered 4-tuples (u_1, u_2, u_3, u_4) of vectors in V_n, satisfying $u_{j_1} = u_{j_2}$ and $u_{j_3} = u_{j_4}$, where the 4-tuple $(u_{j_1}, u_{j_2}, u_{j_3}, u_{j_4})$ is a rearrangement of (u_1, u_2, u_3, u_4). Denote by $D_n^{(3)}$ the collection of 3-tuples (u_1, u_2, u_3) of vectors in V_n with distinct u_1, u_2 and u_3.*

Obviously if $u_1 \oplus u_2 \oplus u_3 \oplus u_4 = 0$ then either $(u_1, u_2, u_3, u_4) \in O_n^{(4)}$ or $(u_1, u_2, u_3) \in D_n^{(3)}$ with $u_1 \oplus u_2 \oplus u_3 = u_4$. It is easy to verify

$$\#O_n^{(4)} = 3 \cdot 2^{2n} - 2^{n+1}, \; \#D_n^{(3)} = 2^n(2^n - 1)(2^n - 2) = 2^{3n} - 3 \cdot 2^{2n} + 2^{n+1} \quad (7)$$

In addition, if $(u_1, u_2, u_3, u_4) \in O_n^{(4)}$, then $(u_1, u_2, u_3, u_4) \in \mathcal{H}_{F,0}^{(4)}$. In other words, $(u_1, u_2, u_3, u_4) \in \mathcal{H}_{F,\beta}^{(4)}$ with $\beta \neq 0$ implies $(u_1, u_2, u_3) \in D_n^{(3)}$ and $u_1 \oplus u_2 \oplus u_3 = u_4$. These properties will be useful later when we count $\tilde{q}_F^{(4)}$.

We note that Lemma 1 cannot be extended to the case of odd k. This is the reason why we have not defined nonhomomorphicity for an odd order.

4 Calculating 4th-order Nonhomomorphicity of S-boxes using Other Indicators

To calculate or express a criterion, we must need other information or conditions. This section has two aims: (1) to give three precise expressions of nonhomomorphicity by using other indicators, (2) to explore the relationships between nonhomomorphicity and other criteria.

4.1 Expressing Nonhomomorphicity by Difference Distribution

Definition 8. *Let $F = (f_1, \ldots, f_m)$ be an $n \times m$ mapping, $\alpha \in V_n$, and β_j be the vector in V_m that corresponds to the binary representation of an integer j. Define $k_\beta(\alpha)$ as the number of times $F(x) \oplus F(x \oplus \alpha)$ runs through $\beta \in V_m$ while x runs through all the vectors in V_n once, The* difference distribution table *of F is a matrix specified as follows:*

$$K = \begin{bmatrix} k_{\beta_0}(\alpha_0) & k_{\beta_1}(\alpha_0) & \ldots & k_{\beta_{2^m-1}}(\alpha_0) \\ k_{\beta_0}(\alpha_1) & k_{\beta_1}(\alpha_1) & \ldots & k_{\beta_{2^m-1}}(\alpha_1) \\ & & \vdots & \\ k_{\beta_0}(\alpha_{2^n-1}) & k_{\beta_1}(\alpha_{2^n-1}) & \ldots & k_{\beta_{2^m-1}}(\alpha_{2^n-1}) \end{bmatrix}$$

where α_j is the vector in V_n that corresponds to the binary representation of j.

Two properties of the difference distribution table K are (i) $\sum_{j=0}^{2^m-1} k_{\beta_j}(\alpha_i) = 2^n$, $i = 0, 1, \ldots, 2^n - 1$, (ii) $k_{\beta_0}(\alpha_0) = 2^n$ and $k_{\beta_j}(\alpha_0) = 0$, $j = 1, \ldots, 2^m - 1$.

Consider an even number s with $s \geq 4$ and an ordered s-tuple $(u_1, u_2, \ldots, u_s)$ of vectors in V_n satisfying $\bigoplus_{j=1}^{s} u_j = 0$. Note that

$$\begin{aligned}\bigoplus_{j=1}^{s} F(u_j) &= \bigoplus_{j=1}^{s-1} F(u_j) \oplus F(\bigoplus_{j=1}^{s-1} u_j) \\ &= \bigoplus_{j=1}^{s-2} F(u_j) \oplus F(u_{s-1}) \oplus F(u_{s-1} \oplus \bigoplus_{j=1}^{s-2} u_j). \qquad (8)\end{aligned}$$

Fix $u_1, \ldots, u_{s-2} \in V_n$ while letting u_{s-1} run through vectors in V_n. Then $\bigoplus_{j=1}^{s} F(u_j)$ runs through a vector $\beta \in V_m$ if and only if $F(u_{s-1}) \oplus F(u_{s-1} \oplus \bigoplus_{j=1}^{s-2} u_j)$ runs through $\beta \bigoplus_{j=1}^{s-2} F(u_j)$ while u_{s-1} runs through all the vectors in V_n once. Hence, for fixed $u_1, \ldots, u_{s-2} \in V_n$, the number of times for $\bigoplus_{j=1}^{s} F(u_j)$ to run through $\beta \in V_m$ is determined by the quantity of $k_{\beta \oplus F(u_1) \oplus \cdots \oplus F(u_{s-2})}(u_1 \oplus \cdots \oplus u_{s-2})$.

Now we remove the restriction that $u_1, \ldots, u_{s-2} \in V_n$ are fixed. Then the number of times for $\bigoplus_{j=1}^{s} F(u_j)$ to run through $\beta \in V_m$ while $(u_1, \ldots, u_s)$ satisfying $\bigoplus_{j=1}^{s} u_j = 0$ runs through all the vectors in V_n once, is determined by $\sum_{u_1, \ldots, u_{s-2} \in V_n} k_{\beta \oplus F(u_1) \oplus \cdots \oplus F(u_{s-2})}(u_1 \oplus \cdots \oplus u_{s-2})$. Hence we have

Lemma 3. *Let F be an $n \times m$ mapping and k be an even number with $k \geq 4$. Then*

$$\tilde{q}_{F,\beta}^{(s)} = \sum_{u_1, \ldots, u_{s-2} \in V_n} k_{\beta \oplus F(u_1) \oplus \cdots \oplus F(u_{s-2})}(u_1 \oplus \cdots \oplus u_{s-2})$$

where $\tilde{q}_{F,\beta}^{(k)}$ is defined in Notation 1 and $k_\beta(\alpha)$ is defined in Definition 8.

In particular, when $s = 4$ and $\beta = 0$, Lemma 3 is specialized as

Corollary 1. *Let F be an $n \times m$ mapping. Then*

$$\tilde{q}_{F,0}^{(4)} = \sum_{u_1, u_2 \in V_n} k_{F(u_1) \oplus F(u_2)}(u_1 \oplus u_2)$$

where $\tilde{q}_{F,0}^{(k)}$ is defined in Notation 1 and $k_\beta(\alpha)$ is defined in Definition 8.

Corollary 2. *Let F be an $n \times m$ mapping. Then*

$$\tilde{q}_{F,0}^{(4)} = \sum_{\alpha \in V_n} \sum_{\beta \in V_m} k_\beta^2(\alpha)$$

where $\tilde{q}_{F,0}^{(k)}$ is defined in Notation 1 and $k_\beta(\alpha)$ is defined in Definition 8.

Proof. Write $u_1 \oplus u_2 = \alpha$. Hence Corollary 1 can be rewritten as

$$\tilde{q}_{F,0}^{(4)} = \sum_{\alpha \in V_n} \sum_{u_1 \in V_n} k_{F(u_1)\oplus F(u_1 \oplus \alpha)}(\alpha) \tag{9}$$

By the definition of $k_\beta(\alpha)$, if $F(u_1) \oplus F(u_1 \oplus \alpha) = \beta$, then we have

$$k_{F(u_1)\oplus F(u_1 \oplus \alpha)}(\alpha) = k_\beta(\alpha)$$

Again, recall that $k_\beta(\alpha)$ denotes the number of times $F(u_1) \oplus F(u_1 \oplus \alpha)$ runs through $\beta \in V_m$ while u_1 runs through all the vectors in V_n once. From (9), we have

$$\tilde{q}_{F,0}^{(4)} = \sum_{\alpha \in V_n} \sum_{u_1 \in V_n} k_{F(u_1)\oplus F(u_1 \oplus \alpha)}(\alpha) = \sum_{\alpha \in V_n} \sum_{\beta \in V_m} k_\beta^2(\alpha)$$

This concludes the proof. □

The above corollary, together with Lemma 2, gives rise to the following result:

Theorem 1. *Let F be an $n \times m$ mapping. Then the 4th-order nonhomomorphicity, $\tilde{q}_F^{(4)}$, satisfies*

$$\tilde{q}_F^{(4)} = 2^{3n} - \sum_{\alpha \in V_n} \sum_{\beta \in V_m} k_\beta^2(\alpha)$$

where $k_\beta(\alpha)$ is defined in Definition 8.

4.2 Expressing Nonhomomorphicity by Fourier Spectrum

Definition 9. *Let $F = (f_1, \dots, f_m)$ be an $n \times m$ mapping, $\alpha \in V_n$, $j = 0, 1, \dots, 2^m - 1$ and $\beta_j = (b_1, \dots, b_m)$ be the vector in V_m that corresponds to the binary representation of an integer j. In addition, set $g_j = \bigoplus_{u=1}^m b_u f_u$ be the jth linear combination of the component functions of F. Denote the sequence of g_j by η_j. Set*

$$P = \begin{bmatrix} \langle \eta_0, \ell_0 \rangle^2 & \langle \eta_1, \ell_0 \rangle^2 & \cdots & \langle \eta_{2^m-1}, \ell_0 \rangle^2 \\ \langle \eta_0, \ell_1 \rangle^2 & \langle \eta_1, \ell_1 \rangle^2 & \cdots & \langle \eta_{2^m-1}, \ell_1 \rangle^2 \\ & \vdots & & \\ \langle \eta_0, \ell_{2^n-1} \rangle^2 & \langle \eta_1, \ell_{2^n-1} \rangle^2 & \cdots & \langle \eta_{2^m-1}, \ell_{2^n-1} \rangle^2 \end{bmatrix}$$

where ℓ_i is the ith row of H_n, $i = 0, 1, \dots, 2^n - 1$. The matrix P is called the correlation immunity distribution table *of the mapping F.*

Since both η_0 and ℓ_0 are the all-one sequence of length 2^n and ℓ_j is $(1, -1)$ balanced for $j > 0$, we have $\langle \eta_0, \ell_0 \rangle = 2^n$, $\langle \eta_0, \ell_j \rangle = 0$, $j = 1, \dots, 2^n - 1$. The following lemma can be found in [10].

Lemma 4. *Let $F = (f_1, \ldots, f_m)$ be a mapping from V_n to V_m, where n and m are integers with $n \geq m \geq 1$ and each $f_j(x)$ is a function on V_n. Set $g_j = \bigoplus_{u=1}^{m} c_u f_u$ where $(c_1, \ldots, c_m)$ is the binary representation of an integer j, $j = 0, 1, \ldots, 2^m - 1$. Then $P = H_n K H_m$ where K and P are defined in Definitions 8 and 9 respectively.*

The following corollary can be deduced from Lemma 4 and Corollary 2.

Corollary 3. *Let F be an $n \times m$ mapping. Then*

$$\tilde{q}_{F,0}^{(4)} = 2^{-m-n}[2^{4n} + \sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^4]$$

where $\langle \eta_j, \ell_i \rangle$ is defined in Definition 9.

By noting Lemma 2, we can further prove

Theorem 2. *Let F be an $n \times m$ mapping. Then the 4th-order nonhomomorphicity of F, $\tilde{q}_F^{(4)}$, satisfies*

$$\tilde{q}_F^{(4)} = 2^{3n} - 2^{-m-n}[2^{4n} + \sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^4]$$

where $\langle \eta_j, \ell_i \rangle$ is defined in Definition 9.

4.3 Expressing Nonhomomorphicity by Auto-Correlation Distribution

Definition 10. *Let $F = (f_1, \ldots, f_m)$ be an $n \times m$ S-box, $\alpha \in V_n$, $j = 0, 1, \ldots, 2^m - 1$ and $\beta_j = (b_1, \ldots, b_m)$ be the vector in V_m that corresponds to the binary representation of j. In addition, set $g_j = \bigoplus_{u=1}^{m} b_u f_u$ be the jth linear combination of the component functions of F. Denote the auto-correlation of g_j with shift α by $\Delta_j(\alpha)$.*

Set

$$D = \begin{bmatrix} \Delta_0(\alpha_0) & \Delta_1(\alpha_0) & \ldots & \Delta_{2^m-1}(\alpha_0) \\ \Delta_0(\alpha_1) & \Delta_1(\alpha_1) & \ldots & \Delta_{2^m-1}(\alpha_1) \\ & & \vdots & \\ \Delta_0(\alpha_{2^n-1}) & \Delta_1(\alpha_{2^n-1}) & \ldots & \Delta_{2^m-1}(\alpha_{2^n-1}) \end{bmatrix}$$

Matrix D is called auto-correlation distribution table *of F.*

By using Theorem 2 and (2), we have the following result:

Theorem 3. *Let F be an $n \times m$ mapping. Then the 4th-order nonhomomorphicity of F, $\tilde{q}_F^{(4)}$, satisfies*

$$\tilde{q}_F^{(4)} = 2^{3n} - 2^{-m}[2^{3n} + \sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \Delta_j^2(\alpha_i)]$$

5 Lower and Upper Bounds on Nonhomomorphicity

We first introduce Hölder's Inequality which can be found in [2].

Lemma 5. *Let $c_j \geq 0$ and $d_j \geq 0$ be real numbers, where $j = 1, \ldots, s$, and let p and q satisfy $\frac{1}{p} + \frac{1}{q} = 1$ and $p > 1$. Then $(\sum_{j=1}^{s} c_j^p)^{1/p} (\sum_{j=1}^{s} d_j^q)^{1/q} \geq \sum_{j=1}^{s} c_j d_j$ where the equality holds if and only if $c_j = \nu d_j$, $j = 1, \ldots, s$ for a constant $\nu \geq 0$.*

When c_j, d_j, p and q satisfy the condition that $c_j \geq 0$, $d_j = \begin{cases} 1 \text{ if } c_j = 1 \\ 0 \text{ if } c_j = 0 \end{cases}$, and $p = q = \frac{1}{2}$, Hölder's Inequality will be specialized as

$$\sum_{j=1}^{s} c_j^2 \geq s^{-1} (\sum_{j=1}^{s} c_j)^2 \tag{10}$$

where the quality holds if and only if $c_1, \ldots, c_s$ are all identical. By using the specialized Hölder's Inequality, we can prove

Theorem 4. *Let F be an $n \times m$ mapping. Then the 4th-order nonhomomorphicity of F, $\tilde{q}_F^{(4)}$, satisfies*

$$0 \leq \tilde{q}_F^{(4)} \leq 2^{2n-m}(2^n - 1)(2^m - 1)$$

where the first equality holds if and only if F is affine, and the second equality holds if and only if every nonzero linear combination of the component functions of F is bent.

Proof. By the definition of the 4th-order nonhomomorphicity of F, the first inequality is true, and the equality holds if and only if F is affine.

Now we consider the second inequality. From Theorem 2,

$$\tilde{q}_F^{(4)} = 2^{3n} - 2^{-m-n}[2^{4n} + \sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^4]$$

By using (10), we have

$$\begin{aligned} \tilde{q}_F^{(4)} &= 2^{3n} - 2^{-m-n}[2^{4n} + \sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^4] \\ &\leq 2^{3n} - 2^{-m-n}[2^{4n} + \frac{1}{(2^m-1)2^n} (\sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^2)^2] \end{aligned}$$

According to Parseval's equation (Page 416 of [3]), we have $\sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^2 = 2^{2n}$ for each j, $1 \leq j \leq 2^m - 1$. Hence

$$\tilde{q}_F^{(4)} \leq 2^{3n} - 2^{-m-n}[2^{4n} + \frac{1}{(2^m-1)2^n} ((2^m-1)2^{2n})^2] \tag{11}$$

This proves the second inequality. Again by using (10), the equality in (11) holds if and only if $\langle \eta_j, \ell_i \rangle^2$ are identical for all $j = 1, \ldots, 2^m - 1$ and $i = 0, 1, \ldots, 2^n - 1$. Parseval's equation implies that, in this case, $\langle \eta_j, \ell_i \rangle^2 = 2^n$ for all $j = 1, \ldots, 2^m - 1$ and $i = 0, 1, \ldots, 2^n - 1$. Recall the definition of a bent function, we have proved that the equality in (11) holds if and only if each g_j (see Definition 9) is bent, where $1 \leq j \leq 2^m - 1$. □

If an $n \times m$ mapping, F, has the property that every nonzero linear combination of the component functions of F is bent, then F is called a *perfect nonlinear* [5]. From a corollary of [5], perfect nonlinear $n \times m$ mappings exist only when $m \leq \frac{1}{2}n$.

6 Mean of Nonhomomorphicity

To measure the nonhomomorphic characteristics of a mapping, it is reasonable to compare it with the mean of the 4th-order nonhomomorphicity over all the mappings from V_n to V_m. Hence we want to find out an explicit expression for $2^{-m \cdot 2^n} \sum_F \tilde{q}_F^{(4)}$.

Recall that if $(u_1, u_2, u_3, u_4) \in O_n^{(4)}$, then $(u_1, u_2, u_3, u_4) \in \mathcal{H}_{F,0}^{(4)}$. Hence we have the following:

Proposition 1. *Let F be a mapping from V_n to V_m. Then for every nonzero vector $\beta \in V_m$,*

$$\begin{aligned} \tilde{q}_{F,\beta}^{(4)} = \#\{(u_1, u_2, u_3) | (u_1, u_2, u_3) \in D_n^{(3)}, \\ F(u_1) \oplus F(u_2) \oplus F(u_3) \oplus F(u_1 \oplus u_2 \oplus u_3) = \beta\} \end{aligned}$$

There are two cases with $(u_1, u_2, u_3, u_4) \in \mathcal{H}_{F,0}^{(4)}$. Case 1: $(u_1, u_2, u_3, u_4) \in O_n^{(4)}$. Case 2: $(u_1, u_2, u_3) \in D_n^{(3)}$ and $(u_1, u_2, u_3, u_4) \in \mathcal{H}_{F,0}^{(k)}$, where $u_4 = u_1 \oplus u_2 \oplus u_3$. This shows that the following is true.

Proposition 2. *Let F be a mapping from V_n to V_m. Then*

$$\begin{aligned} \tilde{q}_{F,0}^{(4)} = 3 \cdot 2^{2n} - 2^{n+1} + \#\{(u_1, u_2, u_3) | (u_1, u_2, u_3) \in D_n^{(3)}, \\ F(u_1) \oplus F(u_2) \oplus F(u_3) \oplus F(u_1 \oplus u_2 \oplus u_3) = 0\} \end{aligned}$$

Theorem 5. *Let F be a mapping from V_n to V_m. For a fixed nonzero $\beta \in V_m$, the mean of the $\tilde{q}_{F,\beta}^{(4)}$ over all the mappings from V_n to V_m, i.e., $2^{-m \cdot 2^n} \sum_F \tilde{q}_{F,\beta}^{(4)}$, satisfies*

$$2^{-m \cdot 2^n} \sum_F \tilde{q}_{F,\beta}^{(3)} = 2^{-m} \# D_n^{(3)} = 2^{3n-m} - 3 \cdot 2^{2n-m} + 2^{n-m+1}$$

Proof. We first note that there exist exactly $2^{m \cdot 2^n}$ mappings from V_n to V_m. For each fixed $(u_1, u_2, u_3) \in D_n^{(3)}$, a random mapping F, from V_n to V_m, $F(u_1)$,

$F(u_2)$, $F(u_3)$, and $F(u_1 \oplus u_2 \oplus u_3)$ are independent. Hence $F(u_1) \oplus F(u_2) \oplus F(u_3) \oplus F(u_1 \oplus u_2 \oplus u_3)$ takes every vector in V_m with an equal probability of 2^{-m}. Therefore we have

$$\begin{aligned} 2^{-m\cdot 2^n} \textstyle\sum_F \tilde{q}^{(4)}_{F,\beta} &= \textstyle\sum_F 2^{-m\cdot 2^n} \#\{(u_1,u_2,u_3)|(u_1,u_2,u_3) \in D^{(3)}_n, \\ &\quad F(u_1) \oplus F(u_2) \oplus F(u_3) \oplus F(u_1 \oplus u_2 \oplus u_3) = \beta\} \\ &= \textstyle\sum_{(u_1,u_2,u_3)\in D^{(3)}_n} 2^{-m} = 2^{-m}\# D^{(3)}_n \end{aligned}$$

□

Theorem 6. *Let F be a mapping from V_n to V_m. Then the mean of $\tilde{q}^{(4)}_{F,0}$ over all the mappings from V_n to V_m, i.e., $2^{-m\cdot 2^n} \sum_F \tilde{q}^{(4)}_{F,0}$, satisfies*

$$2^{-m\cdot 2^n} \sum_F \tilde{q}^{(4)}_{F,0} = 3 \cdot 2^{2n} - 2^{n+1} + 2^{3n-m} - 3 \cdot 2^{2n-m} + 2^{n-m+1}$$

Proof. Consider two cases for $(u_1,u_2,u_3,u_4) \in \mathcal{H}^{(4)}_{F,0}$:

Case 1 — $(u_1,u_2,u_3,u_4) \in O^{(4)}_n$. Recall (7), $\# O^{(4)}_n = 3 \cdot 2^{2n} - 2^{n+1}$.

Case 2 — $(u_1,u_2,u_3) \in D^{(3)}_n$ and $(u_1,u_2,u_3,u_4) \in \mathcal{H}^{(k)}_{F,0}$, where $u_4 = u_1 \oplus u_2 \oplus u_3$.

From the proof of Theorem 5, for each fixed $(u_1,u_2,u_3) \in D^{(3)}_n$, a random mapping F $F(u_1) \oplus F(u_2) \oplus F(u_3) \oplus F(u_1 \oplus u_2 \oplus u_3)$ takes every vector, in particular the zero vector, in V_m with an equal possibility of 2^{-m}. Now the theorem follows immediately from Proposition 2 and the proof of Theorem 5.

□

Taking (6) into account, from Theorem 6 we obtain the following result which is of major interest:

Theorem 7. *Let F be a mapping from V_n to V_m. Then the mean of $\tilde{q}^{(4)}_F$ over all the mappings from V_n to V_m, i.e., $2^{-m\cdot 2^n} \sum_F \tilde{q}^{(4)}_F$, satisfies*

$$2^{-m\cdot 2^n} \sum_F \tilde{q}^{(4)}_F = (2^m - 1)(2^{3n-m} - 3 \cdot 2^{2n-m} + 2^{n-m+1})$$

7 Relative Nonhomomorphicity

We now introduce the concept of "relative nonhomomorphicity". It will be useful for a statistical tool.

Recall that if $(u_1,u_2,u_3,u_4) \in O^{(4)}_n$, then $(u_1,u_2,u_3,u_4) \in \mathcal{H}^{(4)}_{F,0}$. Hence to count $Q^{(k)}_F$, we do not need to consider any 4-tuples (u_1,u_2,u_3,u_4) in $O^{(4)}_n$.

Definition 11. *Let F be a mapping from V_n to V_m. Then $\frac{\tilde{q}^{(4)}_F}{\# D^{(3)}_n}$, denoted by $\rho^{(4)}_F$, is called* the (4th-order) relative nonhomomorphicity *of F, where $\tilde{q}^{(4)}_F$ is the 4th-order nonhomomorphicity of F, while $D^{(3)}_n$ is the collection of 3-tuples (u_1,u_2,u_3) of vectors in V_n with distinct u_1, u_2 and u_3.*

Corollary 4. *The mean of* $\rho_F^{(4)}$ *over all the* $n \times m$ *S-boxes, i.e.,* $2^{-m \cdot 2^n} \sum_F \rho_F^{(4)}$*, satisfies*

$$2^{-m \cdot 2^n} \sum_F \rho_F^{(4)} = 1 - 2^{-m}$$

Proof. Note that $2^{-m \cdot 2^n} \sum_F \rho_F^{(4)} = 2^{-m \cdot 2^n} \sum_F \frac{\tilde{q}_F^{(4)}}{\# D_n^{(3)}} = \frac{2^{-m \cdot 2^n}}{\# D_n^{(3)}} \sum_F \tilde{q}_F^{(4)}$. Hence from Theorem 7, we have $2^{-m \cdot 2^n} \sum_F \rho_F^{(4)} = \frac{(2^m - 1)(2^{3n-m} - 3 \cdot 2^{2n-m} + 2^{n-m+1})}{2^{3n} - 3 \cdot 2^{2n} + 2^{n+1}} = 1 - 2^{-m}$ □

From Corollary 4, the following observation can be made:

$$\rho_F^{(4)} \begin{cases} > 1 - 2^{-m} \text{ then } F \text{ is more nonhomomorphic than the average} \\ < 1 - 2^{-m} \text{ then } F \text{ is less nonhomomorphic than the average} \end{cases} \quad (12)$$

Here the average nonhomomorphicity indicates one that has a relative nonhomomorphicity of $1 - 2^{-m}$. Clearly, if $\rho_F^{(4)}$ is much smaller than $1 - 2^{-m}$ then F should be considered to be cryptographically weak.

8 An Application of Nonhomomorphicity

We have noticed that the relative nonhomomorphicity, $\rho_F^{(4)}$ is precisely identified with "population mean" or "true mean", a terminology in statistics. This fact enables us to design a statistical method with a high reliability for estimating the nonhomomorphicity of an S-box, thank to the law of large numbers [1].

From the nonhomomorphicity, by using Theorems 1, 2 and 3, we obtain information about other criteria, for example, the nonlinearity, the maximum $k_\beta(\alpha)$ with $\alpha \in V_n$, $\alpha \neq 0$ and $\beta \in V_n$, and the maximum $\Delta_j(\alpha_i)$, $1 \leq j \leq 2^m - 1$ and $1 \leq i \leq 2^n - 1$.

Example 1. The Data Encryption Algorithm or DES employs eight 6×4 mappings or S-boxes. Consider the first mapping F. From Definition 7, we directly calculate $\tilde{q}_F^{(4)} = 231264$. (Also we can use a statistical method to find an approximate value of $\tilde{q}_F^{(4)}$).

By using Theorem 1

$$231264 = 2^{18} - \sum_{\alpha \in V_6} \sum_{\beta \in V_4} k_\beta^2(\alpha)$$

Recall the property of the difference distribution table K, $k_0(0) = 2^n$ and $k_\beta(0) = 0$, $\beta \neq 0$.

$$\sum_{\alpha \in V_6, \alpha \neq 0} \sum_{\beta \in V_4} k_\beta^2(\alpha) = 2^{18} - 2^{12} - 231264$$

Write $\max\{k_\beta(\alpha)|\alpha \in V_6.\alpha \neq 0, \beta \in V_4\} = k_M$ Hence we have

$$k_M \sum_{\alpha\in V_6,\alpha\neq 0} \sum_{\beta\in V_4} k_\beta(\alpha) \geq \sum_{\alpha\in V_6} \sum_{\beta\in V_4} k_\beta^2(\alpha) = 2^{18} - 2^{12} - 231264$$

Again, recall the property of K, $\sum_{\beta\in V_m} k_\beta(\alpha) = 2^n$, for any $\alpha \in V_n$. Hence

$$k_M(2^6-1)2^6 \geq 2^{18} - 2^{12} - 231264$$

This implies $k_M \geq 6.6$. Since k_M is even, $k_M \geq 8$. This is larger than the trivial lower bound $k_M \geq 2^{n-m} = 4$.

Write $\max\{|\langle \eta_j, \ell_i\rangle||1 \leq j \leq 2^4-1, 0 \leq i \leq 2^6-1\} = p_M$. By using Theorem 2,

$$(2^{18} - \tilde{q}_F^{(4)})2^{6+4} - 2^{24} = \sum_{j=1}^{2^4-1} \sum_{i=0}^{2^6-1} \langle \eta_j, \ell_i\rangle^4 \leq p_M^2 \sum_{j=1}^{2^4-1} \sum_{i=0}^{2^6-1} \langle \eta_j, \ell_i\rangle^2$$

By using Parseval's equation, Page 416, [3], $\sum_{i=0}^{2^6-1} \langle \eta_j, \ell_i\rangle^2 = 2^{2\cdot 6}$ for each fixed j, $j = 1, \ldots, 2^4-1$. Hence $p_M^2 \geq 2^{12} - \frac{231264}{60} > 241$. Since p_M^2 is square and multiple by 4, we have $p_M^2 \geq 256$. By using (1), we conclude that $N_F \leq 2^{6-1} - \frac{1}{2}p_M \leq 24$. Recall the maximum nonlinearity of functions on V_6 is $2^{6-1} - 2^{3-1} = 28$ that only bent functions achieve.

Write $\max\{|\Delta_j(\alpha_i)|1 \leq j \leq 2^4-1, 1 \leq i \leq 2^6-1\} = \Delta_M$. By using Theorem 3,

$$(2^{3\cdot 6} - \tilde{q}_F^{(4)})2^4 - 2^{3\cdot 6} = \sum_{j=1}^{2^4-1} \sum_{i=0}^{2^6-1} \Delta_j^2(\alpha_i)$$

Noticing $\Delta_j(\alpha_0) = 2^6$, $j = 0, 1, \ldots, 2^4-1$, hence

$$2^{3\cdot 6+4} - 2^4\tilde{q}_F^{(4)} - 2^{3\cdot 6} = 2^{2\cdot 6+4} + \sum_{j=1}^{2^4-1} \sum_{i=1}^{2^6-1} \Delta_j^2(\alpha_i) \leq (2^4-1)(2^6-1)\Delta_M^2$$

This proves

$$\Delta_M^2 \geq \frac{2^{22} - 2^{18} - 2^{16} - 2^4\tilde{q}_F^{(4)}}{(2^6-1)(2^4-1)} > 176$$

Since Δ_M^2 is square and multiple by 4, Hence $\Delta_M^2 \geq 196$ and hence $\Delta_M \geq 14$.

We note that in Example 1, the value of $\tilde{q}_F^{(4)}$ also can be estimated by a fast statistical method with a high reliability. Such a statistical method is more useful in a situation where fast analysis of S-boxes is required.

9 Concluding Remarks

The advantages of nonhomomorphicity, as a new linearity criterion, include: (1) it can be estimated by a statistical method with a high reliability due to the law of large numbers; (2) it is closely related to other criteria. More details about the statistical method, together with further applications of nonhomomorphicity, will be shown in a separate paper.

Acknowledgement

The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

1. Stephen A. Book. *Statistics.* McGraw-Hill Book Company, 1977.
2. Friedhelm Erwe. *Differential And Integral Calculus.* Oliver And Boyd Ltd, Edinburgh And London, 1967.
3. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, New York, Oxford, 1978.
4. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.
5. K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 378–386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
6. K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92*, volume 658, Lecture Notes in Computer Science, pages 92–98. Springer-Verlag, Berlin, Heidelberg, New York, 1993.
7. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
8. X. M. Zhang and Y. Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. *Design, Codes and Cryptography*, 7(1/2):111–134, 1996. special issue dedicated to Gus Simmons.
9. X. M. Zhang and Y. Zheng. The kth-order nonhomomorphicity of boolean functions. In *SAC'98*, volume Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York, 1998. to appear.
10. X. M. Zhang, Y. Zheng, and Hideki Imai. Relating differential distribution tables to other properties of substitution boxes. Designs, Codes and Cryptography (to appear), 1998.