The kth-Order Nonhomomorphicity of S-Boxes

Yuliang Zheng
(School of Network Computing
Monash University
McMahons Road, Frankston, VIC 3199, Australia
yuliang.zheng@infotech.monash.edu.au)

Xian-Mo Zhang
(School of Information Technology & Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia
xianmo@uow.edu.au)

Abstract: Nonhomomorphicity is a new nonlinearity criterion of a mapping or S-box used in a private key encryption algorithm. An important advantage of nonhomomorphicity over other nonlinearity criteria is that the value of nonhomomorphicity is easy to estimate by the use of a fast statistical method. Due to the Law of Large Numbers, such a statistical method is highly reliable. Major contributions of this paper are (1) to explicitly express the nonhomomorphicity by other nonlinear characteristics, (2) to identify tight upper and lower bounds on nonhomomorphicity, and (3) to find the mean of nonhomomorphicity over all the S-boxes with the same size. It is hoped that these results on nonhomomorphicity facilitate the analysis and design of S-boxes.

Key Words: Boolean Functions, Cryptanalysis, Cryptography, Nonhomomorphicity, S-boxes.

Categories: E3

1 Introduction

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 encryption algorithm or 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 a property that for any even number k with $k \geq 4$, we have $F(u_1) \oplus \cdots \oplus F(u_k) = 0$ 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 consider the number of vectors $(u_1, \ldots, u_k)$ in V_n, satisfying $u_1 \oplus \cdots \oplus u_k = 0$ and $F(u_1) \oplus \cdots \oplus F(u_k) \neq 0$, 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 non-affinity from a new perspective; (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.

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 survey previously known results on the nonhomomorphicity of S-boxes. In Section 4, give a formula to calculate the nonhomomorphicity of S-boxes by other indicators. This formula shows a close relationship between nonhomomorphicity and other important criteria. In Section 5, we establish tight upper and lower bounds on the nonhomomorphicity of S-boxes. In Section 6, we establish the mean of nonhomomorphicity over all the S-boxes with the same size. In Sections 7 and 8 we show that the mean of nonhomomorphicity and the relative nonhomomorphicity are relevant to a statistical method for estimating the nonhomomorphicity of S-boxes. In Section 9, we compare nonhomomorphicity with nonlinearity, highlighting once again the importance of studying the nonhomomorphicity of S-boxes. In Section 10, we examine nonhomomorphicity in some special cases and show applications of nonhomomorphicity using a concrete example. Section 11 closes the paper.

2 Boolean Functions and S-boxes

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 1. *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 and 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 2. *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

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix},\ n = 1, 2, \ldots,\ H_0 = 1.$$

The ith row (column) of H_n, $i = 0, 1, \ldots, 2^n - 1$, is the sequence of linear function φ_i on V_n, where $\varphi_i = \langle \alpha_i, x\rangle$ and α_i is the binary representation of integer i.

Definition 3. *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]

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (\langle \xi, \ell_0\rangle^2, \langle \xi, \ell_1\rangle^2, \ldots, \langle \xi, \ell_{2^n-1}\rangle^2) \quad (1)$$

where α_i is the binary representation of an integer i and ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.

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 $2^{n-1} - 2^{\frac{1}{2}n-1}$.

Definition 4. *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 $n \geq m \geq 1$ 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.

In cryptography we are interested primarily in *regular* S-boxes. A mapping $F = (f_1, \ldots, f_m)$ is said to be regular if $F(x)$ runs through each vector in V_m 2^{n-m} times while x runs through V_n once. Clearly $n \times m$ S-boxes exist only for $n \geq m$.

A useful conclusion, which appears many times in the literature, for example, in binary case in Corollary 7.39 of [3], can be described as follows:

Lemma 1. *Let $F = (f_1, \ldots, f_m)$ be an $n \times m$ mapping, where n and m are integers with $n \geq m \geq 1$ and each $f_j(x)$ is a function on V_n. Then F is regular i.e., F runs through all the m-dimensional vectors each 2^{n-m} times while x runs through all the n-dimensional vectors each once if and only if any nonlinear combination of $f_1, \ldots, f_m$, $f(x) = \bigoplus_{j=1}^{m} c_j f_j(x)$, is balanced.*

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

Definition 5. *The standard definition of the nonlinearity of $F = (f_1, \ldots, f_m)$ is*

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

Notation 1 *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.

Let $\beta_j = (b_1, \ldots, b_m)$ be the vector in V_m that corresponds to the binary representation of an integer j, $j = 0, 1, \ldots, 2^m - 1$. 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, $i = 0, 1, \ldots, 2^n - 1$.

Denote the auto-correlation of g_j with shift α by $\Delta_j(\alpha)$. Set

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

Two interesting properties of the difference distribution table K are

$$\sum_{j=0}^{2^m-1} k_{\beta_j}(\alpha_i) = 2^n, i = 0, 1, \ldots, 2^n - 1, \text{ and} \tag{2}$$

$$k_{\beta_0}(\alpha_0) = 2^n, \quad k_{\beta_j}(\alpha_0) = 0, \quad j = 1, \ldots, 2^m - 1 \tag{3}$$

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

$$\langle \eta_0, \ell_0 \rangle = 2^n,\ \langle \eta_0, \ell_j \rangle = 0,\ j = 1, \dots, 2^n - 1. \tag{4}$$

3 Introduction to Nonhomomorphicity

The following lemmas can be found in [11].

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

1. *If F is an affine mapping then for any even number k with $k \geq 4$, we have $F(u_1) \oplus F(u_2) \oplus \cdots \oplus F(u_k) = 0$ whenever $u_1 \oplus u_2 \oplus \cdots \oplus u_k = 0$,*
2. *if there exists an even number k with $k \geq 4$ such that $F(u_1) \oplus F(u_2) \oplus \cdots \oplus F(u_k) = 0$ whenever $u_1 \oplus u_2 \oplus \cdots \oplus u_k = 0$, then F is an affine mapping.*

Lemma 2 explores a characterization of affine mappings. From the lemma, if an $n \times m$ mapping satisfies $F(u_1) \oplus F(u_2) \oplus \cdots \oplus F(u_k) = 0$ for a large number of k-tuples of vectors $(u_1, \dots, u_k)$ in V_n with $u_1 \oplus u_2 \oplus \cdots \oplus u_k = 0$, then F behaves more like an affine mapping. This leads us to introduce a new nonlinearity criterion.

Notation 2 *Let F be an $n \times m$ mapping and k an integer (even or odd) with $1 \leq k \leq 2^n$. Denote by $\mathcal{H}^{(k)}_{F,\beta}(\alpha)$ the collection of ordered k-tuples $(u_1, u_2, \dots, u_k)$ of vectors in V_n satisfying $\bigoplus_{j=1}^{k} u_j = \alpha$ and $\bigoplus_{j=1}^{k} F(u_j) = \beta$ where $\alpha \in V_n$ and $\beta \in V_m$. Set*

$$\tilde{q}^{(k)}_{F,\beta}(\alpha) = \begin{cases} 1 & k = 0 \\ \#\mathcal{H}^{(k)}_{F,\beta}(\alpha) & \text{if } k > 0 \end{cases}$$

where # denote the cardinal number of a set.

In particular, from Notation 2, it is easy to see

$$\tilde{q}^{(1)}_{F,\beta}(\alpha) = \begin{cases} 1 \text{ if } F(\alpha) = \beta \\ 0 \text{ if } F(\alpha) \neq \beta \end{cases} \tag{5}$$

A formal definition for nonhomomorphicity follows.

Definition 6. *Let F be an $n \times m$ mapping, and k be an even number with $k \geq 4$. $\sum_{\beta \neq 0} \tilde{q}^{(k)}_{F,\beta}(0)$ is called* the kth-order nonhomomorphicity *of F, denoted by $\tilde{q}^{(k)}_F$, i.e., $\tilde{q}^{(k)}_F = \sum_{\beta \neq 0} \tilde{q}^{(k)}_{F,\beta}(0)$.*

Note that nonhomomorphicity is defined for an even order k only. This is because the characteristic properties shown in Lemma 2 cannot be extended to the case of an odd k.

The concept of kth-order nonhomomorphicity was first introduced in [9]. The emphasis of [9] was placed on Boolean functions, namely $n \times m$ S-boxes with $m =$

1. The work was carried out further in [11] where the kth nonhomomorphicity of general $n\times m$ S-boxes was studied, albeit for the special case of $k=4$. This leaves an unsolved problem in the case of an arbitrary k with $k\geq 4$. In this paper we solve the problem by presenting a set of results on the kth nonhomomorphicity of general $n\times m$ S-boxes for any even k with $k\geq 4$. Techniques employed in obtaining the results are different from those in [9, 11], and represent a non-trivial extension of the previous works.

From Definition 6, it becomes clear that the following property is true.

Lemma 3. *Let F be an $n\times m$ mapping. For any fixed integer s with $s\geq 2$ and any fixed vector in V_n, the following equation holds:*

$$\sum_{\beta\in V_m}\tilde{q}^{(k)}_{F,\beta}(\alpha)=2^{(k-1)n}$$

Lemma 4. *Let F be an $n\times m$ mapping and s be an integer with $s\geq 2$. Then*

$$\tilde{q}^{(s)}_{F,\beta}(\alpha)=\sum_{\beta'\in V_m}\sum_{\alpha'\in V_n}\tilde{q}^{(s-1)}_{F,\beta'}(\alpha')\tilde{q}^{(1)}_{F,\beta\oplus\beta'}(\alpha\oplus\alpha')$$

Proof.

$$\begin{aligned}
&\tilde{q}^{(s)}_{F,\beta}(\alpha)\\
&=\#\{(u_1,\ldots,u_s)|\textstyle\bigoplus_{j=1}^{s}u_j=\alpha,\ \bigoplus_{j=1}^{s}F(u_j)=\beta\}\\
&=\textstyle\sum_{\alpha'\in V_n}\#\{(u_1,\ldots,u_{s-1})|\bigoplus_{j=1}^{s-1}u_j=\alpha',\ \bigoplus_{j=1}^{s-1}F(u_j)=F(\alpha'\oplus\alpha)\oplus\beta\}\\
&=\textstyle\sum_{\alpha'\in V_n}\tilde{q}^{(s-1)}_{F,F(\alpha')\oplus\beta}(\alpha')\\
&=\textstyle\sum_{\beta'}\sum_{\alpha'\in V_n}\tilde{q}^{(s-1)}_{F,\beta'\oplus\beta}(\alpha')\theta_F(\alpha\oplus\alpha,\beta')\tilde{q}^{(1)}_{F,\beta'}(\alpha\oplus\alpha')\\
&=\textstyle\sum_{\beta'}\sum_{\alpha'\in V_n}\tilde{q}^{(s-1)}_{F,\beta'}(\alpha')\tilde{q}^{(1)}_{F,\beta\oplus\beta'}(\alpha\oplus\alpha')
\end{aligned}$$

Notation 3 *Define a $2^{m+n}\times 2^{m+n}$ real valued $(0,1)$ matrix $\mathbf{Q}$ whose entry on the cross of the γth row and the γ'th column is $\tilde{q}^{(1)}_{F,\beta\oplus\beta'}(\alpha\oplus\alpha')$, where $\gamma=(\alpha,\beta)$ and $\gamma'=(\alpha',\beta')$.*

In addition, define a real-valued $(0,1)$-sequence of length 2^{m+n}, $\Xi=(c_0,c_1,\ldots,c_{2^{m+n}-1})$, as follows

$$c_j=\begin{cases}1 \text{ if } \tilde{q}^{(1)}_{F,\beta}(\alpha)=1\\ 0 \text{ if } \tilde{q}^{(1)}_{F,\beta}(\alpha)=0\end{cases}$$

where (β,α) is the binary representation of an integer j.

Lemma 5. *Let $F=(f_1,\ldots,f_m)$ be an $n\times m$ mapping and β_j be the vector in V_m that is the binary representation of an integer j, $j=0,1,\ldots,2^m-1$. Set $g_j=\langle\beta_j,F\rangle$. Denote the sequence of g_j by η_j. Then $\langle\Xi,L_p\rangle=\langle\eta_t,\ell_s\rangle$ where L_p is the pth row of H_{m+n}, and $p=t\cdot 2^n+s$, $0\leq t\leq 2^m-1$, $0\leq s\leq 2^n-1$.*

Proof. From the construction of a Sylvester Hadamard matrix, L_p can be expressed as $L_p = e_t \bigotimes \ell_s$, where $\bigotimes$ denotes Kronecker product, i.e.,

$$L_p = (d_0\ell_s, d_1\ell_s, \ldots, d_{2^m-1}\ell_s)$$

where $e_t = (d_0, d_1, \ldots, d_{2^m-1})$ and $\ell_s = (c_0, c_1, \ldots, 2^n - 1)$. Hence e_t is the sequence of a linear function ψ on V_m and $\psi(y) = \langle \beta_t, y\rangle$, where β_t is the binary representation of an integer t.

By a straightforward verification, one can get

$$\begin{aligned}\langle \Xi, L_p\rangle &= \sum_{i=0}^{2^n-1}\sum_{j=0}^{2^m-1} \tilde{q}^{(1)}_{F,\beta_j}(\alpha_i)d_j c_i \\ &= \sum_{i=0}^{2^n-1} c_i \sum_{j=0}^{2^m-1} \tilde{q}^{(1)}_{F,\beta_j}(\alpha_i)d_j \\ &= \sum_{i=0}^{2^n-1} c_i \sum_{j=0}^{2^m-1} \tilde{q}^{(1)}_{F,\beta_j}(\alpha_i)(-1)^{\psi(\beta_j)}\end{aligned}$$

Note that for a fixed α_i, from (5), we have $\sum_{j=0}^{2^m-1} \tilde{q}^{(1)}_{F,\beta_j}(\alpha_i)(-1)^{\psi(\beta_j)} = (-1)^{\psi(F(\alpha_i))} = (-1)^{\langle \beta_t, F(\alpha_i)\rangle}$. We also note that $(-1)^{\langle \beta_t, F(\alpha_0)\rangle}, (-1)^{\langle \beta_t, F(\alpha_1)\rangle}, \ldots, (-1)^{\langle \beta_t, F(\alpha_{2^n-1})\rangle}$ is identified with the sequence η_t, defined in Section 5. Hence we have proved $\langle \Xi, L_p\rangle = \langle \eta_t, \ell_s\rangle$.

Lemma 6. *Let F be an $n \times m$ mapping and s be an integer (even or odd) with $s \geq 1$. Then the entry on the cross of the γth row and the γ'th column of $\mathbf{Q}^s$ is precisely identified with $\tilde{q}^{(s)}_{F,\beta}(\alpha)$.*

Proof. By induction on s. From the definition of $\mathbf{Q}$, the lemma holds when $s = 1$. Assume that the lemma holds when $1 \leq s \leq k - 1$.

Consider $\tilde{q}^{(k)}_{F,\beta}(\alpha)$. From Lemma 4, we have

$$\tilde{q}^{(k)}_{F,\beta}(\alpha) = \sum_{\beta' \in V_m}\sum_{\alpha' \in V_n} \tilde{q}^{(s-1)}_{F,\beta'}(\alpha')\tilde{q}^{(s)}_{F,\beta\oplus\beta'}(\alpha \oplus \alpha')$$

Finally recall the assumption that the theorem holds when $2 \leq s \leq k - 1$. By using Lemma 4 we have proved the lemma.

Rewrite ΞH_{m+n} as

$$\Xi H_{m+n} = (\langle \Xi, L_0\rangle, \langle \Xi, L_1\rangle, \ldots, \langle \Xi, L_{2^{m+n}-1}\rangle)$$

where L_i denotes the ith row of H_{m+n} and the binary values 0 and 1 are regarded real numbers.

Hence it is easy to verify

$$QH_{m+n} = H_{m+n} diag(\langle \Xi, L_0\rangle, \langle \Xi, L_1\rangle, \ldots, \langle \Xi, L_{2^{m+n}-1}\rangle)$$

and

$$2^{-m-n} H_{m+n} Q H_{m+n} = diag(\langle \Xi, L_0 \rangle, \langle \Xi, L_1 \rangle, \ldots, \langle \Xi, L_{2^{m+n}-1} \rangle)$$

This causes

$$2^{-m-n} H_{m+n} Q^s H_{m+n} = diag(\langle \Xi, L_0 \rangle^s, \langle \Xi, L_1 \rangle^s, \ldots, \langle \Xi, L_{2^{m+n}-1} \rangle^s)$$

or

$$Q^s H_{m+n} = H_{m+n} diag(\langle \Xi, L_0 \rangle^s, \langle \Xi, L_1 \rangle^s, \ldots, \langle \Xi, L_{2^{m+n}-1} \rangle^s) \tag{6}$$

Comparing the top row on the two sides of the equality (6) and using Lemma 6, we obtain

$$\begin{aligned}&(\tilde{q}^{(s)}_{F,\beta_0}(\alpha_0), \tilde{q}^{(s)}_{F,\beta_1}(\alpha_0), \ldots, \tilde{q}^{(s)}_{F,\beta_{2^m-2}}(\alpha_{2^n-1}), \tilde{q}^{(s)}_{F,\beta_{2^m-1}}(\alpha_{2^n-1}))H_{m+n}\\ &= (\langle \Xi, L_0 \rangle^s, \langle \Xi, L_1 \rangle^s, \ldots, \langle \Xi, L_{2^{m+n}-1} \rangle^s)\end{aligned} \tag{7}$$

where α_i is the binary representation of an integer i with $0 \leq i \leq 2^n - 1$, while β_j is the binary representation of an integer j with $0 \leq j \leq 2^m - 1$.

From (7) and Lemma 5, we conclude

Theorem 1. *Let F be an $n \times m$ mapping and s be an integer (even or odd) with $s \geq 1$. Then*

$$\begin{aligned}&(\tilde{q}^{(s)}_{F,\beta_0}(\alpha_0), \tilde{q}^{(s)}_{F,\beta_1}(\alpha_0), \ldots, \tilde{q}^{(s)}_{F,\beta_{2^m-2}}(\alpha_{2^n-1}), \tilde{q}^{(s)}_{F,\beta_{2^m-1}}(\alpha_{2^n-1}))\\ &= 2^{-m-n}(\langle \eta_0, \ell_0 \rangle^s, \langle \eta_1, \ell_0 \rangle^s, \ldots, \langle \eta_{2^m-2}, \ell_{2^n-1} \rangle^s, \langle \eta_{2^m-1}, \ell_{2^n-1} \rangle^s) H_{m+n}\end{aligned}$$

where η_β is defined in Lemma 5 and ℓ_α is the α row of H_n, β is the binary representation of an integer j with $j = 0, 1, \ldots, 2^m - 1$, and α is the binary representation of an integer i with $i = 0, 1, \ldots, 2^n - 1$.

4 Calculating $\tilde{q}^{(s)}_F$

$\tilde{q}^{(4)}_{F,0}(0)$ has been studied in [11]. In this section we turn our attention to $\tilde{q}^{(k)}_{F,0}(0)$ with $k \geq 0$.

Let $\beta = 0$ and $\alpha = 0$ in Lemma 6. Then each entry on the diagonal of $\mathbf{Q}^s$ is precisely identified with $\tilde{q}^{(s)}_{F,0}(0)$.

Comparing the leftmost entry on the two sides of the equality in Theorem 1, we conclude

Lemma 7. *Let F be an $n \times m$ mapping and s be an integer (even or odd). Then*

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

From Definition 6, we have $\tilde{q}_F^{(s)} = \sum_{\beta\neq 0} \tilde{q}_{F,\beta}^{(s)}(0) = 2^{(k-1)n} - \tilde{q}_{F,0}^{(s)}(0)$. Therefore the following theorem holds:

Theorem 2. *Let F be an $n \times m$ mapping and s be an even number with $s \geq 4$. Then the nonhomomorphicity of F, denoted by $\tilde{q}_F^{(s)}$, satisfies*

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

where $\langle \eta_j, \ell_i \rangle$ is defined in Notation 1.

Since both η_0 and ℓ_0 are identified with the all-one sequence of length 2^n, and ℓ_i is $(1,-1)$-balanced for $i = 1, \ldots, 2^n - 1$, Theorem 2 has another expression:

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

Replacing s in the equality in Theorem 1 by t, where $t \geq 1$ is an integer independent of s, we obtain another equality. Carrying out the inner product between the two equalities, we have proved

$$\sum_{\beta \in V_m} \sum_{\alpha \in V_n} \tilde{q}_{F,\beta}^{(s)}(\alpha) \tilde{q}_{F,\beta}^{(t)}(\alpha) = 2^{-m-n} \sum_{j=0}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^{s+t}$$

By using Lemma 7, we have proved

Corollary 1. *Let F be an $n \times m$ mapping and $s \geq 1$ and $t \geq 1$ be any two integers. Then*

$$\tilde{q}_{F,0}^{(s+t)}(0) = \sum_{\beta \in V_m} \sum_{\alpha \in V_n} \tilde{q}_{F,\beta}^{(s)}(\alpha) \tilde{q}_{F,\beta}^{(t)}(\alpha)$$

5 Bounds on $\tilde{q}_F^{(s)}$

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

Lemma 8. *Let $c_j \geq 0$ and $d_j \geq 0$ be real numbers, where $j = 1, \ldots, t$, and let p and q satisfy $\frac{1}{p} + \frac{1}{q} = 1$ and $p > 1$. Then*

$$(\sum_{j=1}^{t} c_j^p)^{1/p} (\sum_{j=1}^{t} d_j^q)^{1/q} \geq \sum_{j=1}^{t} c_j d_j$$

where the quality holds if and only if $c_j = \nu d_j$, $j = 1, \ldots, t$ for a constant $\nu \geq 0$.

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

$$\sum_{j=1}^{t} c_j^{\frac{s}{2}} \geq t^{1-\frac{s}{2}} (\sum_{j=1}^{t} c_j)^{\frac{s}{2}} \tag{8}$$

where the quality holds if and only if $c_1, \ldots, c_t$ are all identical.

Lemma 9. *Let F be an $n \times m$ mapping and s be even with $s \geq 4$. Then $\tilde{q}_{F,0}^{(s)}(0)$, satisfies*

$$2^{(s-1)n-m} + (2^m - 1)2^{\frac{ns}{2}-m} \leq \tilde{q}_{F,0}^{(s)}(0) \leq 2^{(s-1)n}$$

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

Proof. Consider the first inequality. From Lemma 7, we have

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

By using (8) which is a special case of Lemma 8, we obtain

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

According to Parseval's equation (Page 416 of [4]), 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

$$\tilde{q}_{F,0}^{(s)}(0) \geq 2^{(s-1)n-m} + 2^{-m-n}[((2^m - 1)2^n)^{1-\frac{s}{2}} ((2^m - 1)2^{2n})^{\frac{s}{2}}] \tag{9}$$

This proves the first inequality. Once again by using (8), the equality in (9) 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. Thus we have proved that the equality in (9) holds if and only if each g_j is bent, where $1 \leq j \leq 2^m - 1$.

By the definition of the sth-order nonhomomorphicity of F and Lemma 2, the second inequality is true, and the equality holds if and only if F is affine.

Recalling Definition 6, we conclude

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

$$0 \leq \tilde{h}_F^{(s)} \leq 2^{(s-1)n} - 2^{(s-1)n-m} - (2^m - 1)2^{\frac{ns}{2}-m}$$

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.

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 said to be *perfectly nonlinear*. In this case, we have $m \leq \frac{1}{2}n$ (see [5]).

6 Mean of $\tilde{q}_F^{(k)}$ over all F

Notation 4 *Let O_k (k even) denote the collection of k-tuples $(u_1, \ldots, u_k)$ of vectors in V_n satisfying $u_{j_1} = u_{j_2}, \ldots, u_{j_{k-1}} = u_{j_k}$, where $\{j_1, j_2, \ldots, j_k\} = \{1, 2, \ldots, k\}$. Let D_k denote the collection of k-tuples $(u_1, \ldots, u_k)$ of vectors in V_n satisfying $u_1 \oplus \cdots \oplus u_k = 0$ and $(u_1, \ldots, u_k) \notin O_k$.*

Obviously

$$\#O_k + \#D_k = 2^{(k-1)n} \tag{10}$$

It is easy to verify

Lemma 10. *Let n, m and k be positive integers and $u_1 \oplus \cdots \oplus u_k = 0$, where each u_j is a fixed vector in V_n. Then*

$$F(u_1) \oplus \cdots \oplus F(u_k) = 0$$

holds for every $n \times m$ mapping F if and only if k is even and $(u_1, \ldots, u_k) \in O_k$.

The following lemma can be found in [9]

Lemma 11. *In Notation 4, let k be an even with $2 \leq k \leq 2^n$. Then*

$$\#D_k = \sum_{t=1}^{k/2} \binom{2^n}{t} \sum_{p_1+\cdots+p_t=k/2,\ p_j>0} \frac{(k)!}{(2p_1)! \cdots (2p_t)!}$$

Theorem 4. *Let n, m be positive integers and k be an even with $2 \leq k \leq 2^n$. Then the mean of $\tilde{q}_F^{(k)}$ over all the $n \times m$ mappings, i.e., $2^{-m \cdot 2^n} \sum_F \tilde{q}_F^{(k)}$, satisfies*

$$2^{-m \cdot 2^n} \sum_f \tilde{q}_F^{(k)} = 2^{-m}(2^{(k-1)n} - o_k)$$

Proof. Note that for each $(u_1, \ldots, u_k) \in D_k$, for a random $n \times m$ mapping F, $F(u_1) \oplus \cdots \oplus F(u_k)$ takes every vector in V_m with an equal probability of 2^{-m}. Therefore the mean of $\tilde{q}_{F,\beta}^{(k)}(0)$ over all the $n \times m$ mappings, i.e., $2^{-m \cdot 2^n} \sum_F \tilde{q}_{F,\beta}^{(k)}(0)$ satisfies

$$2^{-m \cdot 2^n} \sum_F \tilde{q}_{F,\beta}^{(k)}(0) = 2^{-m \cdot 2^n} \sum_F \#(\mathcal{H}_{F,\beta}^{(k)}(0)) = 2^{-m} \#D_k \tag{11}$$

From Definition 6, we have

$$2^{-m \cdot 2^n} \sum_F \tilde{q}_F^{(k)} = 2^{-m \cdot 2^n} \sum_{\beta \neq 0} \sum_F \tilde{q}_{F,\beta}^{(k)}(0) = (1 - 2^{-m}) \#D_k \tag{12}$$

Applying (10) to (12), we have proved the theorem.

7 Relative Nonhomomorphicity

The concept of relative nonhomomorphicity introduced in this section is useful for a statistical tool to be introduced later.

Definition 7. Let F be an $n \times m$ mapping and k be an even with $k \geq 4$. Define the *kth-order relative nonhomomorphicity* of F, denoted by $\rho_F^{(k)}$, as $\rho_F^{(k)} = \frac{\tilde{q}_F^{(k)}}{\# D_k}$, i.e., $\rho_F^{(k)} = \frac{\tilde{q}_F^{(k)}}{2^{(k-1)n} - o_k}$.

From Theorem 4, we obtain

Corollary 2. *The mean of* $\rho_F^{(k)}$ *over all the functions on* V_n, *i.e.,* $2^{-m \cdot 2^n} \sum_f \rho_F^{(k)}$, *satisfies*

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

It is interesting to note that $2^{-m \cdot 2^n} \sum_f \rho_F^{(k)} = 1 - 2^{-m}$ is not relevant to k. From Corollary 2, we obtain

$$\rho_F^{(k)} \begin{cases} \geq 1 - 2^{-m} & \text{then } F \text{ is not less nonhomomorphic} \\ & \text{than the mean of nonhomomorphicity} \\ < 1 - 2^{-m} & \text{then } F \text{ is less nonhomomorphic} \\ & \text{than the mean of nonhomomorphicity} \end{cases} \tag{13}$$

If $\rho_F^{(k)}$ is much smaller than $1 - 2^{-m}$, then F should be considered to be cryptographically weak.

8 Estimating Nonhomomorphicity

As shown in Theorem 2, the nonhomomorphicity of an S-boxes can be determined precisely. In this section, however, we introduce a statistical method to estimate nonhomomorphicity. Such a method is useful in the fast analysis of functions.

Denote a real-valued $(0,1)$ function on D_k, $t(u_1, \ldots, u_k)$, as follows

$$t(u_1, \ldots, u_k) = \begin{cases} 1 \text{ if } F(u_1) \oplus \cdots \oplus F(u_k) \neq \beta \\ 0 \text{ otherwise} \end{cases}$$

Hence from the definition of nonhomomorphicity, we have

$$\tilde{q}_F^{(k)} = \sum_{(u_1, \ldots, u_k) \in D_k} t(u_1, \ldots, u_k)$$

Let Ω be a random subset of D_k. Write $\omega = \# \Omega$ and

$$\bar{t} = \frac{1}{\omega} \sum_{(u_1, \ldots, u_k) \in \Omega} t(u_1, \ldots, u_k) \tag{14}$$

Note that this is the "sample mean" [1]. In particular, $\Omega = R_n^{(k)} - O_k$, $\overline{t}$ is identified with the "true mean" or "population mean" [1], namely, $\rho_F^{(k)}$.

Now consider $\sum_{(u_1,\ldots,u_k)\in\Omega}(t(u_1,\ldots,u_k) - \overline{t})^2$. We have

$$\begin{aligned}
&\sum_{(u_1,\ldots,u_k)\in\Omega} (t(u_1,\ldots,u_k) - \overline{t})^2 \\
&= \sum_{(u_1,\ldots,u_k)\in\Omega} t^2(u_1,\ldots,u_k) - 2\overline{t}\cdot \sum_{(u_1,\ldots,u_k)\in\Omega} t(u_1,\ldots,u_k) + \omega\overline{t}^2
\end{aligned}$$

Note that $t^2(u_1,\ldots,u_k) = t(u_1,\ldots,u_k)$. From (14),

$$\begin{aligned}
\sum_{(u_1,\ldots,u_k)\in\Omega} (t(u_1,\ldots,u_k) - \overline{t})^2 &= \omega\overline{t} - 2\omega\overline{t}^2 + \omega\overline{t}^2 \\
&= \omega\overline{t} - 2\omega\overline{t}^2 + \omega\overline{t}^2 \\
&= \omega\overline{t}(1-\overline{t}) \qquad (15)
\end{aligned}$$

Hence the quantity of $\sqrt{\frac{1}{\omega-1}\sum_{(u_1,\ldots,u_k)\in\Omega}(t(u_1,\ldots,u_k) - \overline{t})^2}$, which is called the "sample standard deviation" [1] and is usually denoted by μ, can be expressed as

$$\mu = \sqrt{\frac{1}{\omega-1}\sum_{(u_1,\ldots,u_k)\in\Omega}(t(u_1,\ldots,u_k) - \overline{t})^2} = \sqrt{\frac{\omega\overline{t}(1-\overline{t})}{\omega-1}} \qquad (16)$$

By using (4.4) in Section 4.B of [1], the "true mean" or "population mean", $\rho_{f,1}^{(k)}$, can be bounded by

$$\overline{t} - Z_{e/2}\frac{\mu}{\sqrt{\omega}} < \rho_{f,1}^{(k)} < \overline{t} + Z_{e/2}\frac{\mu}{\sqrt{\omega}} \qquad (17)$$

where $Z_{e/2}$ denotes the value Z of a "standardized normal distribution". Note that (17) holds with a probability of $(1-e)100\%$ (see for example [1]).

For instance,

when $e = 0.2$, $Z_{e/2} = 1.28$, and (17) holds with a probability of 80%,
when $e = 0.1$, $Z_{e/2} = 1.64$, and (17) holds with a probability of 90%,
when $e = 0.05$, $Z_{e/2} = 1.96$, and (17) holds with a probability of 95%,
when $e = 0.02$, $Z_{e/2} = 2.33$, and (17) holds with a probability of 98%,
when $e = 0.01$, $Z_{e/2} = 2.57$, and (17) holds with a probability of 99%,
when $e = 0.001$, $Z_{e/2} = 3.3$, and (17) holds with a probability of 99.9%.

From (14), we have $0 \le \overline{t} < 1$. It is easy to verify that μ in (16) satisfies $0 \le \mu \le \frac{1}{2}\sqrt{\frac{\omega}{\omega-1}}$. This implies that (17) can be replaced simply by

$$\overline{t} - \frac{Z_{e/2}}{2\sqrt{\omega-1}} < \rho_F^{(k)} < \overline{t} + \frac{Z_{e/2}}{2\sqrt{\omega-1}}, \qquad (18)$$

where (18) holds with a probability of $(1-e)100\%$. Hence if ω, i.e., $\#\Omega$, is large, then the lower bound and the upper bound on $\rho_F^{(k)}$ in (17) are closer to each other. On the other hand, if we choose $\omega = \#\Omega$ large enough, then $Z_{e/2}\frac{\mu}{\sqrt{\omega}}$ is sufficiently small, and hence (17) and (18) will provide us with useful information. For instance, viewing (17) and (18) and Corollary 2, set $e = 0.001$ and $Z_{e/2} = 3.3$, we can choose $\omega = \#\Omega$ such that $\frac{Z_{e/2}}{2\sqrt{\omega-1}} < 2^{-(m+2)}$. In this case the estimation of nonhomomorphicity has a reliability of 99.9%. This indicates that $\#\Omega = \omega \geq 5 \cdot 2^{2m+5}$ is sufficiently large.

In summary, we can analyze the nonhomomorphic characteristics of a mapping from V_n to V_m in the following steps:

1. we randomly fix a subset of D_k, say Ω, where $\omega = \#\Omega$ is large enough (say $\omega \geq 5 \cdot 2^{2m+5}$),
2. by using (14), we determine $\bar{t}$, i.e., "the sample mean",
3. by using (17), we determine the range of $\frac{\tilde{q}_F^{(k)}}{\#D_k}$, with a high reliability,

We note that the statistical analysis is efficient due to the following reasons:

(1) the relative nonhomomorphicity, $\frac{\tilde{q}_F^{(k)}}{\#D_k}$ is precisely identified by the use of "population mean" or "true mean", a terminology in statistics,
(2) the method is highly reliable,
(3) ω is dependent only on the size m,but not on n. Hence the method does not require a huge amount of computing.

From *the Law of Large Numbers* [1], as n grows larger and larger, the "sample mean" $\bar{t}$ becomes closer and closer to the "true mean" $\frac{\tilde{q}_F^{(k)}}{\#D_k}$.

Recall Definition 2. To determine the nonlinearity of an individual function f on V_n, we need to calculate $d(f, \varphi_i)$ where $\varphi_0, \varphi_1, \ldots, \varphi_{2^{n+1}-1}$ are all the affine functions on V_n. Let $\varphi_0, \varphi_1, \ldots, \varphi_{2^n-1}$ be all the linear functions on V_n. Then $1 \oplus \varphi_0, 1 \oplus \varphi_1, \ldots, 1 \oplus \varphi_{2^n-1}$ are all the affine, but not linear, functions on V_n. Note that $d(f, 1 \oplus \varphi_i) = 2^n - d(f, \varphi_i)$. Hence we need to calculate each Hamming distance $d(f, \varphi_i)$, for $j = 0, 1, \ldots, 2^n - 1$. On the other hand, to calculate each Hamming distance $d(f, \varphi_i)$, we should compare the value $f(\alpha)$ with the value $\varphi_i(\alpha)$ for each $\alpha \in V_n$.

Now consider Definition 5. To determine the nonlinearity of an $n \times m$ S-box, we need to compare value $g_j(\alpha)$ and the value $\varphi_i(\alpha)$, $(2^m - 1)2^{2n}$ times altogether, where $j = 1, \ldots, 2^m - 1$, $i = 0, 1, \ldots, 2^n - 1$, $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}$.

Compared with the determination of nonlinearity of an $n \times m$ S-box, here we can use the statistical method with a reliability of 99.9%. To achieve this we need to choose Ω with $\#\Omega = \omega \geq 5 \cdot 2^{2m+5}$ which is not relevant to n and much less than $(2^m - 1)2^{2n}$. Hence the statistical method saves time in computing.

As the estimated value of nonhomomorphicity has a high reliability, it can be used to examine other criteria. This will be seen in Section 9.

9 Comparing Nonhomomorphicity with Nonlinearity

Let $F = (f_1, \ldots, f_m)$ be an $n \times m$ mapping and β_j be the vector in V_m that is the binary representation of an integer j, $j = 0, 1, \ldots, 2^m - 1$. Set $g_j = \bigoplus_{u=1}^m b_u f_u$. Denote the sequence of g_j by η_j.

Similarly, let $F^* = (f_1^*, \ldots, f_m^*)$ be an $n \times m$ mapping and β_j be the vector in V_m that is the binary representation of an integer j, $j = 0, 1, \ldots, 2^m - 1$. Set $g_j^* = \bigoplus_{u=1}^m b_u f_u^*$. Denote the sequence of g_j^* by η_j^*.

Since both η_0 and ℓ_0 are the all-one sequence of length 2^n and ℓ_i is $(1, -1)$-balanced,

$$\langle \eta_0, \ell_0 \rangle = 2^n,\ \langle \eta_0, \ell_i \rangle = 0,\ i = 1, \ldots, 2^n - 1$$

Similarly

$$\langle \eta_0^*, \ell_0 \rangle = 2^n,\ \langle \eta_0^*, \ell_i \rangle = 0,\ i = 1, \ldots, 2^n - 1$$

We rewrite each $|\langle \eta_j, \ell_i \rangle|$ as p_s, $j = 1, \ldots, 2^m - 1$, $i = 0, 1, \ldots, 2^n - 1$ and list all the p_s as follows

$$p_1, p_2, \ldots, p_{2^n(2^m-1)}$$

where $p_j \geq p_i$ if $j > i$.

Similarly, rewrite each $|\langle \eta_j^*, \ell_i \rangle|$ as p_s^*, $j = 1, \ldots, 2^m - 1$, $i = 0, 1, \ldots, 2^n - 1$ and list all the p_s^* as follows

$$p_1^*, p_2^*, \ldots, p_{2^n(2^m-1)}^*$$

where $p_j^* \geq p_i^*$ if $j > i$.

We consider the following two cases.

Case 1: $p_j = p_j^*$, $j = 1, \ldots, 2^n(2^m - 1)$. By using Theorem 2, we have $\tilde{q}_F^{(k)} = \tilde{q}_{F^*}^{(k)}$, where k is any even number with $k \geq 4$.

Case 2: there exists some j_0 such that $p_j = p_j^*$, $j = 1, \ldots, j_0$ and $p_{j_0+1} > P_{j_0+1}^*$. Then there exists an even number k_0 such that $p_{j_0}^k / p_{j_0}^{*k} > 2^n - j_0$ for every even k with $k \geq k_0$. This implies that $\sum_{j=1}^{2^n(2^m-1)} p_j^k > \sum_{j=1}^{2^n(2^m-1)} p_j^{*k}$. Hence

$$\sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^k > \sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j^*, \ell_i \rangle^k$$

where k is any even number with $k \geq k_0$. By using Theorem 2, we have proved $\tilde{q}_F^{(k)} > \tilde{q}_{F^*}^{(k)}$.

In summary, we conclude

Theorem 5. *Let F and F^* be two $n \times m$ mappings. Then $\tilde{q}_F^{(k)} = \tilde{q}_{F^*}^{(k)}$ where k is any even number with $k \geq 4$. Otherwise there exists some even number k_0 such that $\tilde{q}_F^{(k)} > \tilde{q}_{F^*}^{(k)}$ or $\tilde{q}_F^{(k)} < \tilde{q}_{F^*}^{(k)}$, where k is any even number with $k \geq k_0$.*

By the same reasoning, we can prove

Theorem 6. *Let F and F^* be two $n \times m$ mappings. If $N_f > (<) N_{f^*}$ then there exists some even number k_0 such that $\tilde{q}_F^{(k)} > (<) \tilde{q}_{F^*}^{(k)}$ where k is any even number with $k \geq k_0$.*

We can give Theorem 6 an equivalent statement as follows.

Theorem 7. *Let F and F^* be two $n \times m$ mappings. If there exists some even number k_0 such that $\tilde{q}_F^{(k)} \geq \tilde{q}_{F^*}^{(k)}$ where k is any even number with $k \geq k_0$ then $N_f \geq N_{f^*}$.*

Examining Theorem 7, we can see that when k is large, $\tilde{q}_F^{(k)}$ guarantees a high nonlinearity. As $\tilde{q}_F^{(k)}$ can be statistically estimated, this result can be useful in facilitating the analysis of nonlinear properties of S-boxes.

Lemma 12. *There exists some even number k_0 with $k_0 \leq 2^n$, satisfies the properties in Theorems 6 and 7.*

Proof. Recall the proof of Theorem 6. We have $p_j = p_j^*$, $j = 1, \ldots, j_0$ and $p_{j_0+1} > P_{j_0+1}^*$. Since each p_j is an even number, we have $p_{j_0+1} \geq 2 + P_{j_0+1}^*$. Hence $p_{j_0}^k / p_{j_0}^{*k} > 2^n - j_0$ for every even k with $k \geq k_0$.

10 Nonhomomorphicity in Special Cases

The nonhomomorphicity is more useful in two special cases: the nonhomomorphicity of Boolean functions and the 4th-order nonhomomorphicity of S-boxes.

10.1 The Nonhomomorphicity of Boolean functions

In fact, a Boolean function f on V_n is a degenerated case of $n \times 1$ S-box. In this case (13) is specialized as

$$\rho_f^{(k)} \begin{cases} \geq \frac{1}{2} \text{ then } f \text{ is not less nonhomomorphic} \\ \quad\ \text{than the mean of nonhomomorphicity} \\ < \frac{1}{2} \text{ then } f \text{ is less nonhomomorphic} \\ \quad\ \text{than the mean of nonhomomorphicity} \end{cases} \tag{19}$$

Obviously (19) is simpler than (13) and hence is easer to use in practice. More details about the nonhomomorphicity of Boolean functions can be found in [9].

Since a function on V_n is an $n \times 1$ S-box, Theorem 4 can be specialized as follows:

Corollary 3. *Let n, m be positive integers and k be an even with $2 \leq k \leq 2^n$. Then the mean of $\tilde{q}_F^{(k)}$ over all the $n \times m$ mappings, i.e., $2^{-m \cdot 2^n} \sum_F \tilde{q}_F^{(k)}$, satisfies*

$$2^{-m \cdot 2^n} \sum_f \tilde{q}_F^{(k)} = 2^{-m}(2^{(k-1)n} - o_k)$$

10.2 The 4th-order nonhomomorphicity of S-boxes

From Lemma 2, we can focus on $\tilde{q}_F^{(4)}$ rather than high order nonhomomorphicity. Furthermore it turns out that $\tilde{q}_F^{(4)}$ is related to other criteria.

Theorem 8. *Let F be an $n \times m$ S-box. Then*

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

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

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

where $k_\beta(\alpha)$, $\langle \eta_j, \ell_i \rangle$ and $\Delta_j^2(\alpha_i)$ have been defined in Notation 1,

Proof. (i) is specialized from Theorem 1 by setting $s = 4$.

(ii) A useful formula can be found in [10]: $P = H_n K H_m$ where P and K are defined in Notation 1. Hence $P^T P = H_n K^T H_m H_m K H_n = 2^m H_n K^T K H_n = 2^{m+n}(2^{-n} H_n K^T K H_n)$. Note that $2^{-n} H_n$ is the inverse of H_n. From linear algebra, similar matrices have the same sum of the elements on the diagonals. Hence $\sum_{j=0}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^4 = \sum_{\alpha \in V_n} \sum_{\beta \in V_m} k_\beta^2(\alpha)$.

Due to (4), $\sum_{\alpha \in V_n} \sum_{\beta \in V_m} k_\beta^2(\alpha) = 2^{-m-n}[2^{4n} + \sum_{j=1}^{2^m-1} \sum_{i=0}^{2^n-1} \langle \eta_j, \ell_i \rangle^4]$. We have proved (ii).

By using (1) and (i), we obtain (iii).

Example 1. The Data Encryption Algorithm or DES employs eight 6×4 mappings or S-boxes. Consider the first mapping F. From Definition 6, 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 8

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

From the property of the difference distribution table K, we have $k_0(0) = 2^n$ 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

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

Once again recalling the property of K, we have $\sum_{\beta \in V_m} k_\beta(\alpha) = 2^n$, 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 $\max\{|\langle \eta_j, \ell_i \rangle| | 1 \leq j \leq 2^4 - 1, 0 \leq i \leq 2^6 - 1\} = p_M$. Due to Theorem 8, we have

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

By using Parseval's equation, Page 416 of [4], we have $\sum_{i=0}^{2^6-1} \langle \eta_j, \ell_i \rangle^2 = 2^{2\cdot 6}$ for each fixed j, $j = 1, \ldots, 2^4 - 1$. Hence $p_M^2 \geq 2^{12} - \frac{231264}{60} > 241$. As p_M^2 is square and hence a multiple of 4, we have $p_M^2 \geq 256$. By using Definition (5), we conclude that $N_F \leq 2^{6-1} - \frac{1}{2}p_M \leq 24$. Recall that the maximum nonlinearity of functions on V_6 is $2^{6-1} - 2^{3-1} = 28$ and it can be achieved only by bent functions.

Write $\max\{|\Delta_j(\alpha_i)| | 1 \leq j \leq 2^4 - 1, 1 \leq i \leq 2^6 - 1\} = \Delta_M$. Once again, due to Theorem 8,

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

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

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

This proves that

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

As Δ_M^2 is square, it must be a multiple of 4. Hence we have $\Delta_M^2 \geq 196$ and $\Delta_M \geq 14$.

11 Conclusions

We have proposed the nonhomomorphicity of S-boxes as a new nonlinearity criteria. We have explicitly expressed the nonhomomorphicity by other nonlinear characteristics, identified tight upper and lower bounds on nonhomomorphicity as well as the mean of nonhomomorphicity over all the S-boxes with the same size, and proposed a statistical method to estimate the nonhomomorphicity of S-boxes. We have also demonstrated applications of nonhomomorphicity in the analysis of S-boxes. It is our belief that more applications of the new criterion will be identified in the future.

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. Rudoff Lidl and Harald Niederreiter. *Finite Fields, Encyclopedia of Mathematics and Its Applications.* Cambridge University Press, 1983.
4. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, New York, Oxford, 1978.
5. K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology - EUROCRYPT'91*, volume 547 of *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 of *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 *Selected Areas in Cryptography, 5th Annual International Workshop, SAC'98*, volume 1556 of *Lecture Notes in Computer Science*, pages 280–295. Springer-Verlag, Berlin, Heidelberg, New York, 1999.
10. X. M. Zhang, Y. Zheng, and Hideki Imai. Relating differential distribution tables to other properties of substitution boxes. *Designs, Codes and Cryptography*, 19:45–63, 2000.
11. Y. Zheng and X. M. Zhang. The nonhomomorphicity of S-boxes. In *Proceedings of the 1-st International Conference on Information Security and Cryptography*, pages 131–145. Korea Institute of Information & Cryptology, 1998.