A NOTE ON THE SIGNAL-TO-NOISE RATIO OF \((n,m)\)-FUNCTIONS

**Yu Zhou**

Science and Technology on Communication Security Laboratory
Chengdu 610041, China

**Xinfeng Dong\(^1,2\)**

\(^1\) Center for Cyber Security, School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu 611731, China

\(^2\) Science and Technology on Communication Security Laboratory
Chengdu 610041, China

**Yongzhuang Wei**

Guilin University of Electronic Technology
Guilin 541004, China

**Fengrong Zhang**

School of Computer Science and Technology
China University of Mining and Technology
Xuzhou 221116, China

(Communicated by Claude Carlet)

**Abstract.** The concept of the signal-to-noise ratio (SNR) as a useful measure indicator of the robustness of \((n,m)\)-functions \(F = (f_1, \ldots, f_m)\) (cryptographic S-boxes) against differential power analysis (DPA), has received extensive attention during the previous decade. In this paper, we give an upper bound on the SNR of balanced \((n,m)\)-functions, and a clear upper bound regarding unbalanced \((n,m)\)-functions. Moreover, we derive some deep relationships between the SNR of \((n,m)\)-functions and three other cryptographic parameters (the maximum value of the absolute value of the Walsh transform, the sum-of-squares indicator, and the nonlinearity of its coordinates), respectively. In particular, we give a trade-off between the SNR and the refined transparency order of \((n,m)\)-functions. Finally, we prove that the SNR of \((n,m)\)-functions is not affine invariant, and data experiments verify this result.

2020 Mathematics Subject Classification: 06E30, 94C10.

**Key words and phrases:** Signal-to-noise ratio, \((n,m)\)-functions, the sum-of-squares indicator, transparency order, affine equivalent.

Yu Zhou and Xinfeng Dong are supported in part by the National Key R&D Program of China (No. 2017YFB0802000, No. 2017YFB0802004), and in part by Sichuan Science and Technology Program (No. 2020JDJQ0076). Yongzhuang Wei is supported in part by the National Natural Science Foundation of China (No. 6137203), and in part by the Guangxi Science and Technology Foundation (Guilin AB18281019, 2019GXNSFGA245004). Fengrong Zhang is supported in part by the Natural Science Foundation of China (61972400) and in part by the Jiangsu Natural Science Foundation (BK20181352).

* Corresponding author: Yu Zhou.
1. Introduction

Differential power analysis (DPA) is one of the most effective methods of side-channel attacks [13], where the leakage information regarding the user’s secret key is extracted by using the obtained power traces, while the encryption algorithm is being physically executed on some specific platforms. In order to resist this attack, the substitution boxes ((n,m)-functions or S-boxes), as the only nonlinear parts of block ciphers, should have acceptable resistance to reduce the information leakage under DPA-like attacks. Currently, there are three important indicators regarding the resistance of S-boxes against DPA-like attacks, i.e., signal-to-noise ratio (SNR), transparency order (TO) and confusion coefficient (CC). More specially, in 2004, the concept of SNR was introduced by Guilley et al. in [11]. In 2005, the transparency order (TO) with the auto-correlation function which measures the resistance of (n,m)-functions to DPA attacks was proposed by Prouff et al. in [16]. Later, some flaws have been found in the original definition of the transparency order, and a new refined transparency order (RTO, see Definition 6) with the cross-correlation function was presented in [8]. The refined transparency order has important influence on the resistance against DPA attacks. A tight upper bound on transparency order for an (n,1)-function was established in [21], and the lower bound directly depending on the nonlinearity was also obtained. In 2012, the definition of confusion coefficient (CC) was proposed by Fei et al. in [9]. On the other hand, in 2006, an efficient DPA attack on Grain and Trivium ciphers was proposed by Fischer et al. in [10], where the side-channel characteristic of the physical implementation can be seen as the SNR as defined in [11] indeed. In 2014, two theoretical distinguishers based on the Kolmogorov-Smirnov (KS) distance were presented in [12]. In this case, the relationship between SNR and CC on the distinguishers performance was discussed.

Notice that the notion of SNR was defined in terms of Walsh transform of (n,m)-functions in [11]. In particular, an upper bound on the SNR of balanced (n,m)-functions and a lower bound on the SNR of unbalanced (n,m)-functions were respectively investigated in [11]. It can be seen from the SNR of (n,m)-functions that the SNR is closely related to the Walsh transforms of its coordinates.

So far, few attempts have been made to check whether the balanced (n,m)-functions can really achieve the upper bound on the SNR or not. And whether the SNR of (n,m)-functions is affine invariant or not. But further investigating the in-depth relationships between the SNR and other cryptography indicators still appears to be an important issue.

In this paper, we consider the unsolved problems regarding SNR in [11]. Specially, in this reference it is shown that \( \sum_{\alpha \in \mathbb{F}_2^n} Y_\alpha = m \cdot 2^{2n} \) if \( F = (f_1, f_2, \cdots, f_m) \) is a balanced (n,m)-function, but \( \sum_{\alpha \in \mathbb{F}_2^n} Y_\alpha \in [0, m^2 2^{2n}] \) for the rest of the cases. Actually, the condition of our result (see Theorem 2) is weaker than that in [11]. A comprehensive description is given, i.e. \( \sum_{\alpha \in \mathbb{F}_2^n} Y_\alpha = m \cdot 2^{2n} \) if \( f_i \oplus f_j \) \( (1 \leq i < j \leq m) \) is a balanced function, but \( \sum_{\alpha \in \mathbb{F}_2^n} Y_\alpha \in [0, m^2 2^{2n}] \) for the rest of the cases. By this observation, we prove that the SNR of any balanced (n,m)-function cannot achieve the upper bound \( 2^n/2 \). On the other hand, the tight upper bound on the SNR of unbalanced (n,m)-functions \( F = (f_1, f_2, \cdots, f_m) \) is described. In particular, the upper bound on the SNR of bent (n,m)-functions is determined exactly. The concept of the sum of Walsh transform-product indicator (SWTPI) is introduced, and a relationship between SWTPI and the sum-of-squares indicator is derived as
A note on the Signal-to-noise ratio of \((n, m)\)-functions

well. Based on SWTPI, some relationships between the SNR of \((n, m)\)-functions and other important cryptographic indicators (including the maximum value of the absolute value of the Walsh transform, the sum-of-squares indicator and the nonlinearity of its coordinates) are established. Some bounds on the SNR of \((n, m)\)-functions are given in Table 2. Furthermore, the equality between the SNR of \(F\) and \(F \circ A\) is verified for any affine permutation \(A\), while \(F\) and \(A \circ F\) can have different SNR. It directly means that SNR does not have the affine invariant property. For instance, we calculate SNR for all optimal \((4, 4)\) S-boxes and many S-boxes used in some well-known encryption algorithms. These S-boxes all miss the affine invariant property.

The paper is organized as follows. In Section 2, the basic concepts are introduced. In Section 3, some results regarding SWTPI are given. In Section 4, the upper bounds on the SNR of balanced and unbalanced \((n, m)\)-functions are derived. Moreover, some relationships between the SNR and three cryptographic indicators are investigated. The simulations results are discussed in Section 5. Some concluding remarks are given in Section 6.

2. Preliminaries

A Boolean function on \(n\) variables may be viewed as a mapping from \(\{0, 1\}^n\) into \(\{0, 1\}\). Throughout this paper the binary field \(GF(2)\) is denoted by \(\mathbb{F}_2\) and the set of all Boolean functions mapping from \(\mathbb{F}_2^n\) to \(\mathbb{F}_2\) is denoted by \(\mathcal{B}_F\). Let \(\oplus\) be the addition operation. A Boolean function \(f\) is commonly represented as a multivariate polynomial over \(\mathbb{F}_2\) called the algebraic normal form (ANF) of \(f\). More precisely, \(f(x_1, x_2, \ldots, x_n)\) can be written as

\[
f(x) = \bigoplus_{I \in \mathcal{P}(N)} a_I (\prod_{i \in I} x_i),
\]

where \(\mathcal{P}(N)\) denotes the power set of \(N = \{1, \ldots, n\}\) in [6]. Every coordinate \(x_i (x = (x_1, x_2, \ldots, x_n))\) appears in this polynomial with exponents at most 1. The degree of the ANF is denoted by \(\text{deg}(f)\) and is called the algebraic degree of the function (this makes sense thanks to the existence and uniqueness of the ANF):

\[
\text{deg}(f) = \max\{|I| : a_I \neq 0\}, \text{ where } |I| \text{ denotes the size of } I.
\]

The Hamming weight \(w_H(x)\) of a binary vector \(x \in \mathbb{F}_2^n\) is the number of its nonzero coordinates, i.e. the size of \(\{i \in N : x_i \neq 0\}\), where \(N\) denotes the set \(\{1, 2, \ldots, n\}\), called the support of the binary vector. The Hamming weight \(w_H(f)\) of a Boolean function \(f\) on \(\mathbb{F}_2^n\) is the size of the support of the function, i.e. the set \(\{x \in \mathbb{F}_2^n : f(x) \neq 0\}\). We say that a Boolean function \(f\) is balanced if its Hamming weight equals \(2^{n-1}\). A Boolean function is an affine function if its algebraic degree satisfies \(\text{deg}(f) < 2\), and the set of all affine functions is denoted by \(\mathcal{A}_n\). If the constant term of an affine function is equal to zero, then this Boolean function is also called a linear function.

**Definition 1.** Let \(f \in \mathcal{B}_F\). The Walsh transform of \(f\) is defined by

\[
\mathcal{F}(f \oplus \varphi_\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \varphi_\alpha(x)},
\]

where \(\varphi_\alpha(x) = \alpha \cdot x = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \cdots \oplus \alpha_n x_n, \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n\).

The nonlinearity of \(f \in \mathcal{B}_F\) is defined as the minimum Hamming distance to the set of all \(n\)-variable affine function. From Definition 1, we know that the
nonlinearity of $f$ can be computed by
\[ nl(f) = 2^n - 1 - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |\mathcal{F}(f \oplus \varphi_{\alpha})|. \]

**Definition 2.** Let $f \in \mathcal{BF}_n$. The auto-correlation function of $f$ is defined by
\[ \mathcal{F}(D_b f) = \sum_{x \in \mathbb{F}_2^n} (-1)^{D_b f(x)}, \]
where $D_b f(x) = f(x) \oplus f(x \oplus b)$ is called the derivative of $f$ in the direction of $b \in \mathbb{F}_2^n$. And the cross-correlation function of two Boolean functions $f, g \in \mathcal{BF}_n$ is defined by
\[ \mathcal{F}(D_b (f, g)) = \sum_{x \in \mathbb{F}_2^n} (-1)^{D_b (f, g)(x)}, \]
where $D_b (f, g)(x) = f(x) \oplus g(x \oplus b)$ is called the derivative of $f$ and $g$ in the direction of $b \in \mathbb{F}_2^n$.

Two $n$-variable Boolean functions $f$ and $g$ are perfectly uncorrelated if $\mathcal{F}(D_{\alpha} (f, g)) = 0$ for all $\alpha \in \mathbb{F}_2^n$, and they are uncorrelated of degree $k$ if $\mathcal{F}(D_{\alpha} (f, g)) = 0$ for all $\alpha \in \mathbb{F}_2^n$ such that $0 \leq w_H(\alpha) \leq k$. From the results in [17, Corollary 3.4], we have $\mathcal{F}(f \oplus \varphi_{\alpha}) \mathcal{F}(g \oplus \varphi_{\alpha}) = 0$ for any $\alpha \in \mathbb{F}_2^n$ if $f$ and $g$ are perfectly uncorrelated. This property is equivalent to the fact that $f$ and $g$ have disjoint Walsh supports (see [15]).

Let $n$ and $m$ be two positive integers. The functions $F = (f_1, f_2, \ldots, f_m)$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called $(n, m)$-functions (we call also vectorial Boolean functions [7]), the Boolean functions $f_1, f_2, \ldots, f_m$ are called the coordinate functions of $F$. An $(n, m)$-function $F$ is balanced if and only if its component functions are balanced, that is, for every nonzero $v \in \mathbb{F}_2^m$, the Boolean function $v \cdot F$ is balanced.

**Definition 3.** ([11]) Let $F = (f_1, \ldots, f_m)$ be an $(n, m)$-function. The signal-to-noise ratio (SNR) of $F$ is defined by
\[ \text{SNR}(DPA)(F) = \frac{m \cdot 2^{2n}}{\sum_{\alpha \in \mathbb{F}_2^n} [\sum_{i=1}^m \mathcal{F}(f_i \oplus \varphi_{\alpha})]^4}. \]

For convenience, we introduce the following symbol:
\[ \Gamma_F = \sum_{\alpha \in \mathbb{F}_2^n} [\sum_{i=1}^m \mathcal{F}(f_i \oplus \varphi_{\alpha})]^4, \]
which will be used in the sequel.

**Definition 4.** ([26]) Let $f, g \in \mathcal{BF}_n$. The sum-of-squares indicator of the cross-correlation between $f$ and $g$ is defined by
\[ \mathcal{V}(f, g) = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}^2(D_{\alpha} (f, g)). \]

If $f = g$, then we have (also see $GAC$ in [23]):
\[ \mathcal{V}(f) = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}^2(D_{\alpha} f). \]
Notice that, for any \( f, g \in \mathcal{B}_n \) we have, as shown in [17]:

\[
(2) \quad \mathcal{V}(f) = \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}^i(f \oplus \varphi_\alpha), \quad \mathcal{V}(f, g) = \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}^2(f \oplus \varphi_\alpha) \mathcal{F}^2(g \oplus \varphi_\alpha).
\]

In particular, (2) implies that the sum-of-squares indicator can be expressed in terms of Walsh transform. In order to further characterize the product of the Walsh transforms of these functions, we introduce a new definition to generalize \( \mathcal{V}(f, g) \) by (2).

**Definition 5.** Let \( f, g, s, t \in \mathcal{B}_n \). The sum of Walsh transform-product indicator (SWTP) of four Boolean functions \( f, g, s, t \) is defined by

\[
(3) \quad \sigma_{f,g,s,t}^{(i,j,k,l)} = \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}^i(f \oplus \varphi_\alpha) \mathcal{F}^j(g \oplus \varphi_\alpha) \mathcal{F}^k(s \oplus \varphi_\alpha) \mathcal{F}^l(t \oplus \varphi_\alpha),
\]

where \( i + j + k + l = 4, i, j, k, l \in \{0, 1, 2, 3, 4\} \).

For convenience, we denote \( \sigma_{f,g,s,t}^{(0,0,0,0)} \) by \( \sigma_{f,g,s,t}^{(0,0,0,0)} \) if \( i = 0 \). Based on (3), we have

1) If \( i = j = k = l = 0 \), then \( \sigma_{f,g,s,t}^{(0,0,0,0)} = \sigma_f^{(4)} = \mathcal{V}(f) \).

2) If \( i = j = 2, k = l = 0 \), then \( \sigma_{f,g,s,t}^{(2,2,0,0)} = \sigma^g_{f,g} = \mathcal{V}(f, g) \).

3) If \( i = j = 3, k = l = 0 \), then \( \sigma_{f,g,s,t}^{(3,3,0,0)} = \sigma_{f,g}^{(1,3)} \).

4) If \( i = j = k = l = 1 \), then \( \sigma_{f,g,s,t}^{(1,1,1,1)} = \sigma_{f,g,s,t} \).

Definition 5 gives some relations \( \sigma_{f,g,s,t}^{(i,j,k,l)} \) for four Boolean functions \( f, g, s, t \).

Generally, we focus on \( \mathcal{V}(f) (= \sigma_{f,g,s,t}^{(0,0,0,0)}) \) and \( \mathcal{V}(f, g) (= \sigma_{f,g,s,t}^{(2,2,0,0)}) \). Especially, (3) will be transformed into (2), if \( i = 4 \) and \( i = 2, j = 2, k = l = 0 \), respectively.

In order to describe the relationship between the SNR and the RTO, we consider Definition 6.

**Definition 6.** ([8]) Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n, m)\)-function. The refined transparency order \((\text{RTO})\) of \( F \) is defined by:

\[
(4) \quad \text{RTO}(F) = \max_{\beta \in \mathbb{F}_2^n} \left\{ m - \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^n} \sum_{j=1}^m | \sum_{i=1}^m (-1)^{\beta_i \oplus \beta_j} \mathcal{F}(D_\alpha(f_i, f_j)) | \right\},
\]

where \( \mathbb{F}_2^* = \mathbb{F}_2 \setminus \{0^n\} \), and \( 0^n = (0, 0, \ldots, 0) \in \mathbb{F}_2^n \) is an \( n \)-dimensional zero vector.

### 3. The relationships between SWTP and the sum-of-squares indicator

In this section, some relationships between SWTP and the sum-of-squares indicator are discussed. We give some equations on \( \sigma_{f,g,s,t}^{(i,j,k,l)} \).

**Lemma 7.** Let \( f, g, s, t \in \mathcal{B}_n \). Then

1) \( \sigma_{f,g,s,t}^{(1,1,1,1)} = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}(D_\alpha(f, g)) \mathcal{F}(D_\alpha(s, t)) \);

2) \( \sigma_{f,g,s,t}^{(2,1,1,0)} = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}(D_\alpha f) \mathcal{F}(D_\alpha g) \);

3) \( \sigma_{f,g,s,t}^{(3,1,0,0)} = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}(D_\alpha f) \mathcal{F}(D_\alpha g) \);

4) \( \sigma_{f,g,s,t}^{(2,2,0,0)} = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}(D_\alpha f) \mathcal{F}(D_\alpha g) = \mathcal{V}(f, g) \);

5) \( \sigma_{f,g,s,t}^{(4,0,0,0)} = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}^2(D_\alpha f) = \mathcal{V}(f) \).
Proof. For any \( u \in \mathbb{F}_2^n \), we know
\[
\mathcal{F}(D_\alpha(f,g)) = \frac{1}{2^n} \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega_u} \mathcal{F}(f \oplus \varphi_\omega) \mathcal{F}(g \oplus \varphi_\omega).
\]
\[1)\] Let \( \Lambda = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}(D_\alpha(f,g)) \mathcal{F}(D_\alpha(s,t)) \), we have
\[
\Lambda = \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}(D_\alpha(f,g)) \mathcal{F}(D_\alpha(s,t))
= \frac{1}{2^{2n}} \sum_{\alpha \in \mathbb{F}_2^n} \left\{ \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega_\alpha} \mathcal{F}(f \oplus \varphi_\omega) \mathcal{F}(g \oplus \varphi_\omega) \right\} \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega_\alpha} \mathcal{F}(s \oplus \varphi_\omega) \mathcal{F}(t \oplus \varphi_\omega)
= \frac{1}{2^{2n}} \sum_{\alpha \in \mathbb{F}_2^n} \left\{ \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega_\alpha} \mathcal{F}(f \oplus \varphi_\omega) \mathcal{F}(g \oplus \varphi_\omega) \right\} \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega_\alpha} \mathcal{F}(s \oplus \varphi_\omega) \mathcal{F}(t \oplus \varphi_\omega)
= \frac{1}{2^{2n}} \sum_{\alpha \in \mathbb{F}_2^n} A_\alpha B_\alpha,
\]
where
\[
A_\alpha = \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega_\alpha} \mathcal{F}(f \oplus \varphi_\omega) \mathcal{F}(g \oplus \varphi_\omega),
B_\alpha = \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega_\alpha} \mathcal{F}(s \oplus \varphi_\omega) \mathcal{F}(t \oplus \varphi_\omega).
\]
Let \( Q(\omega, \alpha) = (-1)^{\omega_\alpha} (\alpha, \omega, \omega \in \mathbb{F}_2^n) \), and the matrix \( H \) be generated in the following way:
\[
H = \begin{pmatrix}
Q(0,0) & Q(1,0) & \cdots & Q(2^n - 1,0) \\
Q(0,1) & Q(1,1) & \cdots & Q(2^n - 1,1) \\
\cdots & \cdots & \cdots & \cdots \\
Q(0,2^n - 1) & Q(1,2^n - 1) & \cdots & Q(2^n - 1,2^n - 1)
\end{pmatrix}
\]
where \( i \) (\( 0 \leq i \leq 2^n - 1 \)) is the integer corresponding to vector \( \alpha \in \mathbb{F}_2^n \), and \( H_i \) denotes the \( i \)-th row of \( H \).

Thus, we know that \( H \) is a Hadamard matrix with rank \( 2^n \). Meanwhile, let \( c_{f,g}, c_{s,t} \) be two column vectors defined by:
\[
c_{f,g} = [\mathcal{F}(f \oplus \varphi_0) \mathcal{F}(g \oplus \varphi_0), \mathcal{F}(f \oplus \varphi_1) \mathcal{F}(g \oplus \varphi_1), \cdots, \mathcal{F}(f \oplus \varphi_{2^n - 1}) \mathcal{F}(g \oplus \varphi_{2^n - 1})]^T, 
\]
\[
c_{s,t} = [\mathcal{F}(s \oplus \varphi_0) \mathcal{F}(t \oplus \varphi_0), \mathcal{F}(s \oplus \varphi_1) \mathcal{F}(t \oplus \varphi_1), \cdots, \mathcal{F}(s \oplus \varphi_{2^n - 1}) \mathcal{F}(t \oplus \varphi_{2^n - 1})]^T.
\]
And let \( A_\alpha \) be the product between \( H_i \) and \( c_{f,g} \), \( B_\alpha \) be the product between \( H_i \) and \( c_{s,t} \). According to the property of the Hadamard matrix: \( HH^T = 2^n I \) (\( I \) is the identity matrix), we have
\[
\Lambda = \frac{1}{2^{2n}} \sum_{\alpha \in \mathbb{F}_2^n} A_\alpha B_\alpha
= \frac{1}{2^{2n}} H \times c_{f,g} \times H \times c_{s,t}^T
= \frac{1}{2^{2n}} c_{f,g}^T \times H^T \times H \times c_{s,t}
= \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}(f \oplus \varphi_\alpha) \mathcal{F}(g \oplus \varphi_\alpha) \mathcal{F}(s \oplus \varphi_\alpha) \mathcal{F}(t \oplus \varphi_\alpha)
= \sigma_{f,g,s,t}^{(1,1,1,1)}.
\]
Similarly, \( 2), 3), 4) \) and \( 5) \) can be proved as well. \( \square \)

Based on Lemma 7, the upper bounds on SWTPI are presented.
Theorem 8. Let \( f, g, s, t \in B\mathbb{F}_n \).

1) \( \sigma_{f,g,s,t}^{(1,1,1,1)} \leq \sqrt{\mathbb{V}(f,g)\mathbb{V}(s,t)} \), where the equation takes the equal if and only if \( F(f \oplus \varphi_\alpha)F(g \oplus \varphi_\alpha) = F(s \oplus \varphi_\alpha)F(t \oplus \varphi_\alpha) \) for any \( \alpha \in \mathbb{F}_2^n \);

2) \( \sigma_{f,g,s,t}^{(3,1,0,0)} = \sigma_{f,g}^{(3,1)} \leq \sqrt{\mathbb{V}(f)\mathbb{V}(g)} \), where the equation takes the equal if and only if \( F^2(f \oplus \varphi_\alpha)F(g \oplus \varphi_\alpha) = F^2(g \oplus \varphi_\alpha)F(f \oplus \varphi_\alpha) \) for any \( \alpha \in \mathbb{F}_2^n \);

3) \( \sigma_{f,g,s,t}^{(2,2,0,0)} = \sigma_{f,g}^{(2,2)} = \mathbb{V}(f,g) \leq \sqrt{\mathbb{V}(f)\mathbb{V}(g)} \), where the equation takes the equal if and only if \( F^2(f \oplus \varphi_\alpha) = F^2(g \oplus \varphi_\alpha) \) for any \( \alpha \in \mathbb{F}_2^n \);

4) \( \sigma_{f,g,s,t}^{(2,1,1,0)} = \sigma_{f,g,s}^{(2,1,1)} \leq \sqrt{\mathbb{V}(f)\mathbb{V}(s,g)} \), where the equation takes the equal if and only if \( F^2(f \oplus \varphi_\alpha) = F(g \oplus \varphi_\alpha)F(s \oplus \varphi_\alpha) \) for any \( \alpha \in \mathbb{F}_2^n \).

Proof. According to Definition 5 and Cauchy inequality, we have

\[
\sigma_{f,g,s,t}^{(i,j,k,l)} = \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} F^i(f \oplus \varphi_\alpha)F^j(g \oplus \varphi_\alpha)F^k(s \oplus \varphi_\alpha)F^l(t \oplus \varphi_\alpha)
\]

\[
= \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^i(f \oplus \varphi_\alpha)F^j(g \oplus \varphi_\alpha)] [F^k(s \oplus \varphi_\alpha)F^l(t \oplus \varphi_\alpha)]
\]

\[
\leq \frac{1}{2^n} \sqrt{\sum_{\alpha \in \mathbb{F}_2^n} [F^i(f \oplus \varphi_\alpha)F^j(g \oplus \varphi_\alpha)]^2} \sqrt{\sum_{\alpha \in \mathbb{F}_2^n} [F^k(s \oplus \varphi_\alpha)F^l(t \oplus \varphi_\alpha)]^2}
\]

\[
= \sqrt{\frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^i(f \oplus \varphi_\alpha)F^j(g \oplus \varphi_\alpha)]^2} \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^k(s \oplus \varphi_\alpha)F^l(t \oplus \varphi_\alpha)]^2.
\]

There are four cases:

1) If \( i = j = k = l = 1 \), then we have

\[
\sigma_{f,g,s,t}^{(1,1,1,1)} \leq \sqrt{\frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^1(f \oplus \varphi_\alpha)F^1(g \oplus \varphi_\alpha)]^2} \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^1(s \oplus \varphi_\alpha)F^1(t \oplus \varphi_\alpha)]^2
\]

\[
= \sqrt{\mathbb{V}(f,g)\mathbb{V}(s,t)}.
\]

2) If \( i = 3, j = 1 \) and \( k = l = 0 \), then we have

\[
\sigma_{f,g,s,t}^{(3,1,0,0)} = \sigma_{f,g}^{(3,1)} = \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} F^3(f \oplus \varphi_\alpha)F^1(g \oplus \varphi_\alpha)
\]

\[
= \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} F^2(f \oplus \varphi_\alpha)F^1(f \oplus \varphi_\alpha)F^1(g \oplus \varphi_\alpha)
\]

\[
\leq \sqrt{\frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^2(f \oplus \varphi_\alpha)]^2} \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^1(f \oplus \varphi_\alpha)F^1(g \oplus \varphi_\alpha)]^2
\]

\[
= \sqrt{\mathbb{V}(f)\mathbb{V}(f,g)}.
\]

3) If \( i = 2, j = 2 \) and \( k = l = 0 \), then we have

\[
\sigma_{f,g,s,t}^{(2,2,0,0)} = \sigma_{f,g}^{(2,2)} \leq \sqrt{\frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^2(f \oplus \varphi_\alpha)]^2} \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [F^2(g \oplus \varphi_\alpha)]^2
\]

\[
= \sqrt{\mathbb{V}(f)\mathbb{V}(g)}.
\]
4) If \( i = 2, j = 1, k = 1 \) and \( l = 0 \), then we have

\[
\sigma_{f,g,s,t}^{(2,1,1,0)} \leq \sqrt{\frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [\mathcal{F}(f \oplus \varphi_\alpha)]^2} \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} [\mathcal{F}(g \oplus \varphi_\alpha)\mathcal{F}(s \oplus \varphi_\alpha)]^2
\]

\[
= \sqrt{\mathcal{V}(f)\mathcal{V}(g,s)}.
\]

The sufficient and necessary conditions of 1), 2), 3) and 4) are easy to be proved. □

These results are closely related to the lower bound on the SNR of any \((n,m)\)-function in Section 4.3.

4. The new upper bound on the SNR of \((n,m)\)-functions

In this section, let \( F = (f_1, \ldots, f_m) \) be an \((n,m)\)-function, and \( Y_\omega = [\sum_{i=1}^{m} \mathcal{F}(f_i \oplus \varphi_\omega)]^2 \) for any \( \omega \in \mathbb{F}_2^n \) [11], we have

\[
\text{SNR}(\text{DPA})(F) = \frac{m \cdot 2^{2n}}{\sqrt{\sum_{\omega \in \mathbb{F}_2^n} Y_\omega}}.
\]

In order to attain the exact upper bounds on the SNR of balanced or unbalanced \((n,m)\)-functions, we first give Lemma 9.

Lemma 9. ([20, 25]) For \( x_i \in \mathbb{Z} \), let \( \sum_{i=1}^{t} x_i = X \). Then

\[
\sum_{i=1}^{t} x_i^2 \geq 2X\left\lfloor \frac{X}{t} \right\rfloor - t\left\lfloor \frac{X}{t} \right\rfloor^2 + X - t\left\lfloor \frac{X}{t} \right\rfloor,
\]

where the equality (5) is achieved if and only if one of the following conditions holds:

1. Let \( \left\lfloor \frac{X}{t} \right\rfloor = M \in \mathbb{Z}, a + b = t, |A| = a \geq 1, |B| = b \geq 1, A \cap B = \Phi, A \cup B = \{1, \ldots, t\} \). If \( i \in B \), then \( x_i = M; \) if \( i \in A \), then \( x_i = M + 1 \).

2. \( x_i = M \) for all \( i = 1, \ldots, t \).

Lemma 10. ([26]) Let \( f, g \in \mathcal{B}F_n \). Then

\[
\sum_{\omega \in \mathbb{F}_2^n} \mathcal{F}(f \oplus \varphi_\omega)\mathcal{F}(g \oplus \varphi_\omega) = 2^n \mathcal{F}(D_{0^n}(f,g)).
\]

Lemma 11. Let \( f \in \mathcal{B}F_n \). Then

\[
\sum_{\omega \in \mathbb{F}_2^n} \mathcal{F}(f \oplus \varphi_\omega) = 2^n(-1)^{f(0^n)}.
\]

Lemma 12. ([11]) Let \( F = (f_1, \ldots, f_m) \) be an \((n,m)\)-function.

1. If \( F \) is a balanced \((n,m)\)-function, then

\[
\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m \cdot 2^{2n}.
\]

2. Otherwise, \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega \in [0, m^22^{2n}] \).

Lemma 12 implies that \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m \cdot 2^{2n} \) if \( F(x) \) is a balanced \((n,m)\)-function.
Theorem 13. Let $F = (f_1, \ldots, f_m)$ be an $(n,m)$-function.

(1) If $f_i \oplus f_j$ is a balanced Boolean function for $1 \leq i < j \leq m$, then we have

$$\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m \cdot 2^{2n}.$$  

(2) Otherwise, $\sum_{\omega \in \mathbb{F}_2^n} Y_\omega \in [0, m^2 2^{2n}]$.

Proof. According to the expression of $Y_\omega$, we have

$$\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = \sum_{\omega \in \mathbb{F}_2^n} [\sum_{i=1}^{m} F(f_i \oplus \varphi_\omega)]^2$$

$$= \sum_{\omega \in \mathbb{F}_2^n} [\sum_{i=1}^{m} F^2(f_i \oplus \varphi_\omega) + 2 \sum_{i<j} F(f_i \oplus \varphi_\omega) F(f_j \oplus \varphi_\omega)]$$

$$= \sum_{i=1}^{m} \sum_{\omega \in \mathbb{F}_2^n} F^2(f_i \oplus \varphi_\omega) + 2 \sum_{i<j} \sum_{\omega \in \mathbb{F}_2^n} F(f_i \oplus \varphi_\omega) F(f_j \oplus \varphi_\omega)$$

$$= m \cdot 2^{2n} + 2 \cdot 2^n \sum_{i<j} [D_0(f_i, f_j)]$$

$$= m \cdot 2^{2n} + 2 \cdot 2^n \sum_{i<j} [2^n - 2w_H(f_i \oplus f_j)].$$

(1) If $f_i \oplus f_j$ is a balanced Boolean function for $1 \leq i < j \leq m$, then $w_H(f_i \oplus f_j) = 2^{n-1}$, that is $\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m \cdot 2^{2n}$.

(2) If $f_i \oplus f_j$ is not a balanced Boolean function for $1 \leq i < j \leq m$, it is easy to verify $\sum_{\omega \in \mathbb{F}_2^n} Y_\omega \in [0, m^2 2^{2n}]$. \qed

Example 1. Let $F = (f_1, \ldots, f_m)$ be an $(n,m)$-function.

1) If $m = 1$, $F = f_1$, then

$$\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = \sum_{\omega \in \mathbb{F}_2^n} [F(f_1 \oplus \varphi_\omega)]^2 = 2^{2n}.$$  

It also means, $\sum_{\omega \in \mathbb{F}_2^n} Y_\omega$ can achieve the upper bound $m \cdot 2^{2n}$ ($m = 1$). Furthermore, \[ SNR(DPA) \left( F \right) = \sqrt{\frac{2^{2n}}{m!}}. \]

2) If $F = (f_1, \cdots, f_m)$, then

$$\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = \sum_{\omega \in \mathbb{F}_2^n} [\sum_{i=1}^{m} F(f_i \oplus \varphi_\omega)]^2$$

$$\leq \sum_{\omega \in \mathbb{F}_2^n} [\sum_{i=1}^{m} F^2(f_i \oplus \varphi_\omega)]^2$$

$$= m \cdot \sum_{\omega \in \mathbb{F}_2^n} \left[ \sum_{i=1}^{m} F^2(f_i \oplus \varphi_\omega) \right]$$

$$= m \cdot 2^{2n}, \tag{6}$$

where the equality (6) takes the equal if and only if $F(f_i \oplus \varphi_\omega) = F(f_j \oplus \varphi_\omega)$ with given $\omega \in \mathbb{F}_2^n$ for any $1 \leq i \neq j \leq m$. That is $f_1 = f_2 = \cdots = f_m$. It implies that $\sum_{\omega \in \mathbb{F}_2^n} Y_\omega$ reaches the upper bound $m^2 2^{2n}$.
3) If \( F = (f_1, \ldots, f_m) \) satisfies \( \sum_{\omega \in \mathbb{F}_2^n} f_i \ominus \varphi_\omega = 0 \) for any \( \omega \in \mathbb{F}_2^n \), then \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega = 0 \). For example, \( F = (f, f + 1) \), then \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega = 0 \).

4) If \( m = 4 \). The coordinate functions are defined as:

\[
\begin{align*}
    f_1(x, y_1, y_2) &= g(x) \oplus y_1 \oplus y_2, \\
    f_2(x, y_1, y_2) &= g(x) \oplus y_1, \\
    f_3(x, y_1, y_2) &= g(x) \oplus y_2, \\
    f_4(x, y_1, y_2) &= g(x),
\end{align*}
\]

where \( g \) is a bent \((n - 2)\)-function and \( n (n \geq 4) \) is even. Then we have the Walsh transform in Table 1, where \( \gamma \in \mathbb{F}_2^{n-2} \) and \( \gamma_1, \gamma_2 \in \mathbb{F}_2 \).

| \( \alpha = (\gamma, \gamma_1, \gamma_2) \) | \( (\gamma, 0, 0) \) | \( (\gamma, 0, 1) \) | \( (\gamma, 1, 0) \) | \( (\gamma, 1, 1) \) |
|---|---|---|---|---|
| \( \mathcal{F}(f_1 \oplus \varphi_\omega) \) | 0 | 0 | 0 | \( 2^2 \cdot \mathcal{F}(g \oplus \varphi_\gamma) \) |
| \( \mathcal{F}(f_2 \oplus \varphi_\omega) \) | 0 | 0 | 2\( 2^2 \cdot \mathcal{F}(g \oplus \varphi_\gamma) \) | 0 |
| \( \mathcal{F}(f_3 \oplus \varphi_\omega) \) | 0 | \( 2^2 \cdot \mathcal{F}(g \oplus \varphi_\gamma) \) | 0 | 0 |
| \( \mathcal{F}(f_4 \oplus \varphi_\omega) \) | \( 2^2 \cdot \mathcal{F}(g \oplus \varphi_\gamma) \) | 0 | 0 | 0 |

Table 1. Walsh transform of \( f_i \)

Note that \( g \) is a bent \((n - 2)\)-function, then (1) \( \mathcal{F}^2(g \oplus \varphi_\gamma) = 2^{n-2} \) for any \( \gamma \in \mathbb{F}_2^{n-2} \); (2) \( F \) is not a balanced function, and \( f_1 \oplus f_2, f_1 \oplus f_3, f_1 \oplus f_4, f_2 \oplus f_3, f_2 \oplus f_4, f_3 \oplus f_4 \) are balanced functions.

By Table 1, we have

\[
\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = \sum_{\omega \in \mathbb{F}_2^n} \left( \sum_{i=1}^m \mathcal{F}(f_i \oplus \varphi_\omega) \right)^2
\]

\[
= \sum_{\omega \in \mathbb{F}_2^n} \left[ 2^4 \cdot 2^{n-2} \right]
\]

\[
= 4 \cdot 2^{2n},
\]

i.e. \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega \) belongs to \([0, m^22^{2n}]\).

Moreover, we can calculate SNR(DPA)(\( F \)) = \( 2^{n/2} \).

From 4), we also find that \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m \cdot 2^{2n} \), if \( f_i \) and \( f_j \) are perfectly uncorrelated (or disjoint spectra functions) for any \( 1 \leq i \neq j \leq m \), where \( F = (f_1, \ldots, f_m) \).

\( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m2^{2n} \) plays an important role in obtaining the upper bound on the SNR of unbalanced \((n, m)\)-functions (see [11]). For \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega \) to reach \( m2^{2n} \), Theorem 13 is more detailed than Lemma 12. By Example 1, there are unbalanced \((n, m)\)-functions such that \( f_i \oplus f_j \ (1 \leq i < j \leq m) \) are balanced functions. Thus, compared with Lemma 12, Theorem 13 enables us to find more \((n, m)\)-functions satisfying: \( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m2^{2n} \).

Therefore, we have an upper bound on SNR(DPA)(\( F \)) for \( F = (f_1, \ldots, f_m) \) if \( f_i \oplus f_j \ (1 \leq i < j \leq m) \) are balanced functions.

**Theorem 14.** Let \( F = (f_1, \ldots, f_m) \) be an \((n, m)\)-function. If \( f_i \oplus f_j \ (1 \leq i < j \leq m) \) are balanced functions, then \( \text{SNR(DPA)}(F) \leq 2^{n/2} \).

4.1. The new upper bound on the SNR of balanced \((n, m)\)-functions.

Based on Lemma 12, it has been shown in [11] that the SNR of balanced \((n, m)\)-functions is bounded above by \( 2^{n/2} \). In this section, we verify that this upper bound cannot be tight at all.
Theorem 15. Let $F = (f_1, \ldots, f_m)$ ($f_i \in \mathcal{BF}_{n}, 1 \leq i \leq m$) be any balanced $(n, m)$-function. Then $\text{SNR}(DPA)(F) < 2^{n/2}$.

Proof. Assume $\text{SNR}(DPA)(F) = 2^{n/2}$, we have

$$\text{SNR}(DPA)(F) = \frac{m \cdot 2^{2n}}{\sqrt{\sum_{\omega \in \mathbb{F}_2^n} Y_\omega^2}} = 2^{n/2}.$$ 

By Cauchy’s inequality and $\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = m \cdot 2^{2n}$, we have

$$m^2 \cdot 2^{3n} = \sum_{\omega \in \mathbb{F}_2^n} Y_\omega^2 \geq \left( \sum_{\omega \in \mathbb{F}_2^n} Y_\omega \right)^2 = \left( \frac{m \cdot 2^{2n}}{2n} \right)^2 = m^2 \cdot 2^{3n}.$$ 

That is, $Y_\omega = \left( \sum_{i=1}^{m} F(f_i \oplus \phi_\omega) \right)^2 = m \cdot 2^n$ for any $\omega \in \mathbb{F}_2^n$. Moreover,

$$(7) \quad \sum_{i=1}^{m} F(f_i \oplus \phi_\omega) = \pm \sqrt{m \cdot 2^n}.$$ 

If $\omega = 0^n$ in (7), then (7) is equivalent to $\sum_{i=1}^{m} F(f_i \oplus \phi_{0^n}) = \pm \sqrt{m \cdot 2^n}$. Note that $F$ is a balanced $(n, m)$-function, then $f_i$ is a balanced function for $1 \leq i \leq m$. Thus, $F(f_i \oplus \phi_{0^n}) = 0$ for $1 \leq i \leq m$. That is, $0 = \pm \sqrt{m \cdot 2^n}$, this contradicts to $m \geq 1$ and $n \geq 1$. Therefore, we have $\text{SNR}(DPA)(F) < 2^{n/2}$. \hfill $\Box$

4.2. New upper bounds on the SNR of unbalanced $(n, m)$-functions.

In this section, the upper bound on the SNR of unbalanced $(n, m)$-functions is discussed by Hamming weight of the coordinate functions. Moreover, the upper bound on the SNR of bent $(n, m)$-functions is presented.

Theorem 16. Let $F = (f_1, \ldots, f_m)$ be an unbalanced $(n, m)$-function and $H_F = \sum_{i<j} [2^n - 2w_H(f_i \oplus f_j)]$. Then

$$(8) \quad \text{SNR}(DPA)(F) \leq \frac{m \sqrt{2^{3n}}}{m2^n + 2H_F},$$

where (8) takes the equal if and only if $Y_\omega = m \cdot 2^n + 2H_F$ for all $\omega \in \mathbb{F}_2^n$. 

Proof. According to the expression of $Y_\omega$, we have

\[
\sum_{\omega \in \mathbb{F}_2^n} Y_\omega = \sum_{\omega \in \mathbb{F}_2^n} \left( \sum_{i=1}^{m} \mathcal{F}(f_i \oplus \varphi_\omega) \right)^2
\]

\[
= \sum_{\omega \in \mathbb{F}_2^n} \left( \sum_{i=1}^{m} \mathcal{F}(f_i \oplus \varphi_\omega)^2 + 2 \sum_{i<j} \mathcal{F}(f_i \oplus \varphi_\omega) \mathcal{F}(f_j \oplus \varphi_\omega) \right)
\]

\[
= \sum_{i=1}^{m} \sum_{\omega \in \mathbb{F}_2^n} \mathcal{F}(f_i \oplus \varphi_\omega)^2 + 2 \sum_{i<j} \sum_{\omega \in \mathbb{F}_2^n} \mathcal{F}(f_i \oplus \varphi_\omega) \mathcal{F}(f_j \oplus \varphi_\omega)
\]

\[
= m \cdot 2^{2n} + 2 \sum_{i<j} 2^n \mathcal{F}(D_0^\omega(f_i, f_j))
\]

\[
= m \cdot 2^{2n} + 2^{n+1} \sum_{i<j} [2^n - 2w_H(f_i \oplus f_j)]
\]

\[
= m \cdot 2^{2n} + 2^{n+1} H_F.
\]

Let $X = m \cdot 2^{2n} + 2^{n+1} H_F$, $t = 2^n$ and $\lfloor \frac{X^2}{t} \rfloor = m \cdot 2^n + 2H_F$ in Lemma 9, we have

\[
\sum_{\omega \in \mathbb{F}_2^n} Y_\omega^2 \geq 2(m \cdot 2^{2n} + 2^{n+1} H_F)(m \cdot 2^n + 2H_F) - 2[m \cdot 2^n + 2H_F]^2
\]

\[
+ (m \cdot 2^{2n} + 2^{n+1} H_F) - 2^n(m \cdot 2^n + 2H_F)
\]

\[
= m^2 2^{3n} + 4m \cdot 2^{2n} H_F + 4 \cdot 2^n H_F^2
\]

\[
= 2^n(m \cdot 2^n + 2H_F)^2.
\]

Moreover, we have

\[
\text{SNR}(DPA)(F) = \frac{m \cdot 2^{2n}}{\sqrt{\sum_{\omega \in \mathbb{F}_2^n} Y_\omega^2}} \leq \frac{m \cdot 2^{2n}}{\sqrt[2]{2^n(m \cdot 2^n + 2H_F)^2}}
\]

\[
= \frac{m \sqrt{2^{3n}}}{m 2^{2n} + 2H_F}.
\]

By Lemma 9, we consider two cases.

1) If $Y_\omega$ satisfies the first condition in Lemma 9, then we have $M = \lfloor \frac{X}{t} \rfloor = m \cdot 2^n + 2H_F \in \mathbb{Z}$, where $a + b = 2^n, |A| = a \geq 1, |B| = b \geq 1, A \cap B = \Phi, A \cup B = \mathbb{F}_2^n$. (If $\omega \in B$, then $Y_\omega = M$, and if $\omega \in A$, then $Y_\omega = M + 1$). Actually, $\mathcal{F}(f \oplus \varphi_\omega) \equiv 0 \mod 4$ for any balanced Boolean function $f(x) \in BF_n (\omega \in \mathbb{F}_2^n)$, then we have $Y_\omega \equiv 0 \mod 16$ for $\omega \in \mathbb{F}_2^n$, i.e. $Y_\omega \neq M + 1$. This is impossible.

2) If $Y_\omega$ satisfies the second condition in Lemma 9, then $Y_\omega = M = m \cdot 2^n + 2H_F$ for all $\omega \in \mathbb{F}_2^n$. \hfill \Box

Remark 1. Theorem 16 also implies two facts:

1) This new upper bound on the SNR of an unbalanced $(n,m)$-function is presented for the first time, which is determined by the Hamming weight of the sum functions. In other word, if we know the Hamming weight of the sum functions, the exact upper bound on the SNR of unbalanced $(n,m)$-functions can be attained easily.
2) If $f_i \oplus f_j$ ($1 \leq i < j \leq m$) are balanced functions, then we have $H_F = 0$, i.e. $SNR(DPA)(F) \leq 2^{n/2}$. This upper bound is the same as the bound in Theorem 14.

**Example 2.** Let $F = (f, 1 \oplus f)$ be an $(n,2)$-function, where $f$ is a bent function. Then we have $Y_\omega = 2 \cdot 2^n - 2 \cdot 2^0$ for all $\omega \in \mathbb{F}_2^n$, and $SNR(DPA)(F) = \frac{2\sqrt{2^n}}{2^{n/2}} = 2^{n/2}$.

The lower bound on the SNR of bent $(n,m)$-functions was obtained in [11], but the upper bound on the SNR was not provided. Theorem 16 gives the upper bound on the SNR of a bent $(n,m)$-function since any bent function is unbalanced. Generally, for a bent $(n,m)$-function we have Corollary 1.

**Corollary 1.** Let $F = (f_1, \ldots, f_m)$ be a bent $(n,m)$-function ($m \leq n/2$). Then

$$SNR(DPA)(F) \leq \frac{2^n}{2^{n/2} - m + 1}.$$  

**Proof.** Since $F = (f_1, \ldots, f_m)$ is a bent $(n,m)$-function, $f_i \oplus f_j$ are also bent function for any $1 \leq i \neq j \leq m$, that is, $w_H(f_i \oplus f_j) = 2^{n-1} \pm 2^{n/2-1}$. Thus

$$H_F = \sum_{i<j} [2^n - 2w_H(f_i \oplus f_j)]$$

$$\geq \sum_{i=1}^m \sum_{1<i<j} [2^n - 2(2^{n-1} + 2^{n/2-1})]$$

$$= -m(m-1)2^{n/2-1}.$$  

Thus, we have

$$SNR(DPA)(F) \leq \frac{m\sqrt{2^{3n}}}{m \cdot 2^n + 2H_F} = \frac{2^n}{2^{n/2} - m + 1}.$$  

In Corollary 1, we find $SNR(DPA)(F) < 2^{n/2}$ for $m \geq 2$. In particular, if $m = 1$, we have $SNR(DPA)(F) \leq 2^{n/2}$.

### 4.3. The relationships between the SNR and other cryptographic properties.

In this section, the relationships between the SNR and other cryptographic properties are discussed.

**Theorem 17.** Let $F = (f_1, \ldots, f_m)$ be an $(n,m)$-function. Then

$$SNR(DPA)(F) = \frac{m\sqrt{2^{3n}}}{\sqrt{\Gamma_F}},$$

where

$$\Gamma_F^2 = \sum_{i=1}^m V(f_i) + 4 \sum_{i=1}^m \sum_{j \neq i} \sigma_{f_i,f_j}^{(3,1)} + 6 \sum_{i=1}^m \sum_{i<j} \sigma_{f_i,f_j}^{(2,2)} + 12 \sum_{i=1}^m \sum_{i<j<k} \sigma_{f_i,f_j,f_k}^{(2,1,1)} + 24 \sum_{i=1}^m \sum_{i<j<k<l} \sigma_{f_i,f_j,f_k,f_l}^{(1,1,1,1)}.$$
Proof. According to Definition 3, we have

\[
\Gamma_F = \sum_{\alpha \in \mathbb{F}_2^n} \left[ \sum_{i=1}^{m} \mathcal{F}(f_i \oplus \varphi_\alpha) \right]^4
\]

\[
= \sum_{\alpha \in \mathbb{F}_2^n} \sum_{i=1}^{m} \mathcal{F}^4(f_i \oplus \varphi_\alpha) + 4 \sum_{i=1}^{m} \sum_{j \neq i} \mathcal{F}^3(f_i \oplus \varphi_\alpha)(f_j \oplus \varphi_\alpha)
\]

\[
+ 6 \sum_{i=1}^{m} \sum_{j \neq i} \mathcal{F}^2(f_i \oplus \varphi_\alpha)\mathcal{F}^2(f_j \oplus \varphi_\alpha)
\]

\[
+ 12 \sum_{i=1}^{m} \sum_{i<j<k} \mathcal{F}(f_i \oplus \varphi_\alpha)\mathcal{F}(f_j \oplus \varphi_\alpha)\mathcal{F}(f_k \oplus \varphi_\alpha)
\]

\[
+ 24 \sum_{i=1}^{m} \sum_{i<j<k<l} \mathcal{F}(f_i \oplus \varphi_\alpha)\mathcal{F}(f_j \oplus \varphi_\alpha)\mathcal{F}(f_k \oplus \varphi_\alpha)\mathcal{F}(f_l \oplus \varphi_\alpha).
\]

By Definition 5, we have

\[
\Gamma_F = 2^n \sum_{i=1}^{m} \mathcal{V}(f_i) + 4 \sum_{i=1}^{m} \sum_{j \neq i} \sigma_{f_i,f_j}^{(3,1)} + 6 \sum_{i=1}^{m} \sum_{i<j} \sigma_{f_i,f_j}^{(2,2)}
\]

\[
+ 12 \sum_{i=1}^{m} \sum_{i<j<k} \sigma_{f_i,f_j,f_k}^{(2,1,1)} + 24 \sum_{i=1}^{m} \sum_{i<j<k<l} \sigma_{f_i,f_j,f_k,f_l}^{(1,1,1,1)}.
\]

Moreover, we have Corollary 2.

**Corollary 2.** Let \( F = (f_1, \ldots, f_m) \) be an \((n,m)\)-function. If \( f_i \) and \( f_j \) are perfectly uncorrelated for any \( 1 \leq i < j \leq m \), then we have

\[
SNR(DPA)(F) = \frac{m\sqrt{2^{3n}}}{\sqrt{\sum_{i=1}^{m} \mathcal{V}(f_i)}}.
\]

**Proof.** Since \( f_i \) and \( f_j \) are perfectly uncorrelated for any \( 1 \leq i < j \leq m \), that is, \( \mathcal{F}(f_i \oplus \varphi_\omega)\mathcal{F}(f_j \oplus \varphi_\omega) = 0 \) for \( \omega \in \mathbb{F}_2^n \) and \( 1 \leq i < j \leq m \) [17]. By Theorem 17, we easily attain this result. \( \square \)

**Remark 2.**

1) Let \( F = (f_1, \ldots, f_m) \) be a \( r \)-order plateaued \((n,m)\)-function [24]. If \( f_i \) and \( f_j \) are perfectly uncorrelated for \( 1 \leq i < j \leq m \), then we have \( SNR(DPA)(F) = \sqrt{m \cdot 2^r} \).

2) Let \( F = (f_1, \ldots, f_m) \) be a bent \((n,m)\)-function. If \( f_i \) and \( f_j \) are perfectly uncorrelated for \( 1 \leq i < j \leq m \), then we have \( SNR(DPA)(F) = \sqrt{m \cdot 2^n} \).

**Theorem 18.** Let \( F = (f_1, \ldots, f_m) \) be an \((n,m)\)-function. Then

\[
SNR(DPA)(F) \geq \frac{m\sqrt{2^{3n}}}{\sqrt{\Gamma_F^*(\sigma)}}.
\]
where
\[
\Gamma_P^*(\sigma) = \sum_{i=1}^{m} V(f_i) + 4 \sum_{i=1}^{m} \sum_{i<j} (V(f_i))^\frac{1}{2} (V(f_j))^\frac{1}{2} + 6 \sum_{i=1}^{m} \sum_{i<j} (V(f_i))^\frac{1}{2} (V(f_j))^\frac{1}{2} + 12 \sum_{i=1}^{m} \sum_{i<j<k} (V(f_i))^\frac{1}{2} (V(f_j))^\frac{1}{2} (V(f_k))^\frac{1}{2} + 24 \sum_{i=1}^{m} \sum_{i<j<k<l} (V(f_i))^\frac{1}{2} (V(f_j))^\frac{1}{2} (V(f_k))^\frac{1}{2} (V(f_l))^\frac{1}{2}.
\]

**Proof.** By Theorem 8 and \(V(f, g) \leq V(f)^\frac{1}{2} V(g)^\frac{1}{2}\) for any \(f(x), g(x) \in \mathcal{B} \mathcal{F}_n\) [27], we easily attain this result.

Actually, Theorem 18 gives the relationship between \(SNR(DPA)(F)\) and \(V(f_i)\) \((1 \leq i \leq m)\), and implies that \(SNR(DPA)(F)\) becomes smaller, if \(V(f_i)\) \((1 \leq i \leq m)\) becomes larger. Based on Theorem 18 for any \(f \in \mathcal{B} \mathcal{F}_n\), we have \(V(f) \leq 2^n |\mathcal{L}_f| \) [24], where \(\mathcal{L}_f = \max_{\alpha \in \mathbb{F}_2^m} |\mathcal{F}(f) \oplus \varphi_\alpha|\), and then we easily deduce Corollary 3.

**Corollary 3.** Let \(F = (f_1, \ldots, f_m)\) be an \((n, m)\)-function. Then
\[
SNR(DPA)(F) \geq \frac{m^{2^n}}{\Gamma_P^*(\mathcal{L})},
\]
where
\[
\Gamma_P^{**}(\mathcal{L}) = \sum_{i=1}^{m} \mathcal{L}_i^2 + 4 \sum_{i=1}^{m} \sum_{i<j} \mathcal{L}_i^2 \mathcal{L}_j^2 + 6 \sum_{i=1}^{m} \sum_{i<j} \mathcal{L}_i \mathcal{L}_j + 12 \sum_{i=1}^{m} \sum_{i<j<k} \mathcal{L}_i \mathcal{L}_j \mathcal{L}_k + 24 \sum_{i=1}^{m} \sum_{i<j<k<l} \mathcal{L}_i \mathcal{L}_j \mathcal{L}_k \mathcal{L}_l.
\]

**Remark 3.** Corollary 3 gives the relationship between \(SNR(DPA)(F)\) and \(\mathcal{L}_f\) \((1 \leq i \leq m)\), and implies that \(SNR(DPA)(F)\) becomes smaller, if \(\mathcal{L}_f\) \((1 \leq i \leq m)\) becomes larger. Based on Theorem 18 and Corollary 3, we can also derive the relationship between \(SNR(DPA)(F)\) and the nonlinearity of the coordinate functions \(nl(f_i)\) \((1 \leq i \leq m)\).

The relationship between \(SNR(DPA)(F)\) and \(nl(f_i)\) \((1 \leq i \leq m)\).
\[
SNR(DPA)(F) \geq \frac{m^{2^n}}{\Gamma_P^{**}(\mathcal{N})},
\]
where
\[
\Gamma_P^{**}(\mathcal{N}) = \sum_{i=1}^{m} (2^n - 2nl(f_i))^2 + 4 \sum_{i=1}^{m} \sum_{i<j} (2^n - 2nl(f_i))^\frac{1}{2} (2^n - 2nl(f_j))^\frac{1}{2} + 6 \sum_{i=1}^{m} \sum_{i<j} (2^n - 2nl(f_i))^\frac{1}{2} (2^n - 2nl(f_j))^\frac{1}{2} + 12 \sum_{i=1}^{m} \sum_{i<j<k} (2^n - 2nl(f_i))^\frac{1}{2} (2^n - 2nl(f_j))^\frac{1}{2} (2^n - 2nl(f_k))^\frac{1}{2} + 24 \sum_{i=1}^{m} \sum_{i<j<k<l} [(2^n - 2nl(f_i))(2^n - 2nl(f_j))(2^n - 2nl(f_k))(2^n - 2nl(f_l))^\frac{1}{2}].
\]
At the end of this section, we summarize some bounds on the SNR of \((n, m)\)-functions in Table 2.

**Table 2.** The signal-to-noise ratio bounds on S-boxes \(F = (f_1, \ldots, f_m)\)

| Ref. | \(SNR\) | S-Box type                      |
|------|----------|---------------------------------|
| [11] | \(1 \leq SNR \leq 2^{n/2}\) | Balanced S-Boxes                |
| Theorem 15 | \(SNR < 2^{n/2}\) | Balanced S-Boxes                |
| [11] | \(1/m \leq SNR\) | Unbalanced S-Boxes              |
| Theorem 16 | \(SNR \leq m \cdot \frac{2^{n/2}}{m^{2^n} + 2H_F}\) | Unbalanced S-Boxes              |
| [11] | \(2^{n/2}/q \approx SNR\) | Bent S-Boxes                    |

**Corollary 1**

\(SNR \leq 2^{n/2}\)

\(f_i\) and \(f_j\) are perfectly uncorrelated \((1 \leq i < j \leq m)\)

**Corollary 2**

\(SNR = m \sqrt{\frac{2^m}{\sum_{i=1}^{m} V(f_i)}}\)

4.4. **The signal-to-noise ratio of affine equivalence S-boxes.**

Some of the SNR of \((8, 8)\) S-boxes (included \((8, 8)\)-linear S-boxes, DES S-box, AES S-box, Bent S-box, etc) were proposed in [11], however the SNR of \((4, 4)\) S-boxes are not investigated. Notice that some \((4, 4)\) S-boxes are extensively used in many encryption algorithms, which are used in resource constrained environments. The number of bijective mappings (affine equivalence) \(F : F_2^n \to F_2^m\), was determined in [5], where the number of affine equivalence S-boxes is 302.

In what follows, the affine invariant property of \(SNR(DPA)(F)\) will be discussed. Notice that some cryptographic properties remain invariant under affine equivalence, e.g. nonlinearity, algebraic degree, etc. More specifically, let \(S_1\) and \(S_2\) be two balanced \((n, n)\)-functions, if there exists a pair of invertible affine mappings \(A\) and \(B\) such that \(B^{-1} \circ S_2 \circ A = S_1\), then we call \(S_1\) and \(S_2\) are affine equivalent. Each of these affine mappings can be expressed as a linear transform followed by an addition, which leads to an affine equivalence relation:

\[S_1(x) = B^{-1} \cdot S_2(A \cdot x \oplus a) \oplus b, x \in F_2^n,\]

where \(A\) is an invertible \(n \times n\)-bit linear mapping, \(B\) is an invertible \(m \times m\)-bit linear mapping, \(a\) is an \(n\)-bit constant and \(b\) is an \(m\)-bit constant.

**Theorem 19.** Let \(F = (f_1, \ldots, f_m)\) be a balanced \((n, m)\)-function. Then

\[SNR(DPA)(F(A \cdot x \oplus c)) = SNR(DPA)(F(x)),\]

where \(A\) is an invertible \(n \times n\)-bit linear mapping and \(c \in F_2\).

**Proof.** For convenience, let \(h_i(x) = f_i(A \cdot x \oplus c)\) for \(1 \leq i \leq n\), we need to prove \(SNR(DPA)(F) = SNR(DPA)(H)\) for \(H = (h_1, \ldots, h_m)\).

By Definition 3, we have

\[\Gamma_H = \sum_{\alpha \in F_2^n} \left| \sum_{i=1}^{m} F(h_i \oplus \varphi_{\alpha}) \right|^4\]

\[= \sum_{\alpha \in F_2^n} \left( \sum_{i=1}^{m} \sum_{x \in F_2^n} (-1)^{h_i(x) \oplus \varphi_{\alpha} x} \right)^4\]
Let $\alpha \in \mathbb{F}_2^n$. Then
\[
\sum_{i=1}^{m} \sum_{x \in \mathbb{F}_2^n} (-1)^{f_i(x) \cdot \Theta \cdot \alpha \cdot x} = \sum_{\alpha \in \mathbb{F}_2^n} \sum_{i=1}^{m} \sum_{x \in \mathbb{F}_2^n} (-1)^{f_i(y) \cdot \Theta \cdot \alpha \cdot A^{-1}(y \cdot c)}
\]
\[
= \sum_{\alpha \in \mathbb{F}_2^n} \sum_{i=1}^{m} (-1)^{A^{-1} \cdot c} \sum_{y=A \cdot x \oplus c \cdot x \in \mathbb{F}_2^n} (-1)^{f_i(y) \cdot \Theta \cdot \alpha \cdot A^{-1} \cdot y}
\]
\[
= \sum_{\alpha \in \mathbb{F}_2^n} [(-1)^{A^{-1} \cdot c}]^4 \sum_{i=1}^{m} \mathcal{F}(f_i \oplus \varphi_{A\cdot i})
\]
\[
= \sum_{\beta=\alpha \cdot A^{-1}, \alpha \in \mathbb{F}_2^n} \left[ \sum_{i=1}^{m} \mathcal{F}(f_i \oplus \varphi_{\beta}) \right]^4
\]
\[
= \Gamma_{F}.
\]
Therefore, we have $SNR(DPA)(F(A \cdot x \oplus c)) = SNR(DPA)(F(x))$. □

On the other hand, we consider $SNR(DPA)(F(A \cdot x \oplus c) \oplus d) = SNR(DPA)(F(x))$ for any affine permutation $A \in \mathbb{F}_n$ and $c, d \in \mathbb{F}_2^n$. For affine equivalent, we have Theorem 20.

**Theorem 20.** Let $F = (f_1, \ldots, f_m)$ be a balanced $(n, m)$-function. Then $SNR(DPA)(F) \neq SNR(DPA)(B \circ F)$ for some affine permutation $B \in \mathbb{F}_n$.

**Proof.** Let $F(x, y) = (f_1(x, y), \ldots, f_m(x, y))$ and $G(x, y) = (g_1(x, y), \ldots, g_m(x, y))$ be two balanced $(n + m, m)$-functions, and define $f_i, g_i$ as
\[
f_i(x, y) = g(x) \oplus y, \ i = 1, 2, \ldots, m;
\]
\[
g_j(x, y) = y_j \oplus y_j, \ g_j(x, y) = f_j(x, y), \ j = 2, \ldots, m,
\]
where $n$ is even, $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $y = (y_1, \ldots, y_m) \in \mathbb{F}_2^m$, $g \in \mathcal{B}_n$ is a bent function.

Then $F$ and $G$ are affine equivalent S-boxes under affine transformation $B$, i.e., $G = B \circ F$:
\[
B = \begin{pmatrix}
1 & 1 & 0 & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & 1
\end{pmatrix}_{m \times m}
\]

It can be verified that $f_i$ and $f_j$ $(1 \leq i \neq j \leq m)$ are perfectly uncorrelated, but $g_i$ and $g_j$ $(1 \leq i \neq j \leq m)$ are perfectly uncorrelated. By Corollary 2, we can easily calculate the distribution of Walsh transform with coordinate functions of $F$ and $G$.

For any $\gamma = (\alpha, \beta)$ and $\alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^m$, we have
\[
\mathcal{F}(f_i \oplus \varphi_{\gamma}) = \left\{ \begin{array}{ll}
2^m \mathcal{F}(g \oplus \varphi_{\alpha}), & \gamma = (0^n, 1^m), \\
0, & \gamma \neq (0^n, 1^m), \ i = 1, 2, \ldots, m,
\end{array} \right.
\]
where $1^m$ means that the $i$-th position is 1, and the remaining positions are 0. And
\[
\mathcal{F}(g_1 \oplus \varphi_{\gamma}) = \left\{ \begin{array}{ll}
2^{n+1}, & \gamma = (0^n, 1, 1, 0, \cdots, 0), \\
0, & \gamma \neq (0^n, 1, 1, 0, \cdots, 0).
\end{array} \right.
\]
Note that \( g \) is a bent function such that \(| \mathcal{F}(g \oplus \varphi_\alpha) | = 2^{n/2}\) for any \( \alpha \in \mathbb{F}_2^n \).

Moreover, we have
\[
\text{SNR}(DPA)(F) = \frac{m \sqrt{2^{3(n+m)}}}{\sqrt{\frac{1}{2^{m+n}} (2^m \cdot 2^{n/2})^4 \times 4}} = \sqrt{m} 2^n.
\]
\[
\text{SNR}(DPA)(G) = \frac{m \sqrt{2^{3(n+m)}}}{\sqrt{\frac{1}{2^{m+n}} (2^m \cdot 2^{n/2})^4 \times (m-1) + \frac{1}{2^{m+n}} (2^{n+1})^4}} = \frac{m 2^n}{\sqrt{m-1 + 2^{2n}}}.
\]

We have \( \text{SNR}(DPA)(F) \neq \text{SNR}(DPA)(G) \).

From Theorem 20, we know that \( \text{SNR}(DPA)(F) \) is not affine invariant. In Section 5, some simulations that support Theorems 19 and 20 are made for \((4,4)\)-functions.

4.5. THE RELATIONSHIP BETWEEN THE SNR AND THE RTO.

In this section, the relationship between the SNR and the RTO for any \((n,m)\)-function is established.

In 2005, the notion of transparency order (TO) was proposed by Prouff et al. in [16], and this notion was also defined in terms of the auto-correlation coefficients of S-boxes. However, in 2017 Chakraborty et al. [8] identified certain limitations of the original definition in [16], and they presented the definition of transparency order (RTO) based on the cross-correlation coefficients of \((n,m)\)-functions.

Lemma 21. ([8]) Let \( F = (f_1, \ldots, f_m) \) be an \((n,m)\)-function. \( \text{RTO}(F) \) has the following lower bound
\[
m - \frac{\sqrt{2^n - 1}}{2^{2n} - 2^n} \sum_{j=1}^{m} \left( \sum_{i=1}^{m} \sum_{a \in \mathbb{F}_2^n} \mathcal{F}^2(f_i \oplus \varphi_\alpha) \mathcal{F}^2(f_j \oplus \varphi_\alpha) \right) + 2 \sum_{1 \leq i < k \leq m} \sum_{a \in \mathbb{F}_2^n} \mathcal{F}(f_i \oplus \varphi_\alpha) \mathcal{F}^2(f_j \oplus \varphi_\alpha) \mathcal{F}(f_k \oplus \varphi_\alpha) \right)^{1/2}.
\]

The expression of \( \left[ \sum_{i=1}^{m} f_i^\alpha \right]^4 \) in Definition 3 is given in Lemma 22.

Lemma 22. Let \( F = (f_1, \ldots, f_m) \) be an \((n,m)\)-function. Then
\[
\left[ \sum_{i=1}^{m} f_i^\alpha \right]^4 = \sum_{i=1}^{m} (f_i^\alpha)^4 + 4 \sum_{1 \leq i < j \leq m} (f_j^\alpha)^3 (f_i^\alpha) + 6 \sum_{1 \leq i < j \leq m} (f_j^\alpha)^2 (f_i^\alpha)^2
\]
\[
+ 12 \sum_{j=1}^{m} \sum_{i,j < k < \ell} (f_j^\alpha)^2 (f_i^\alpha) (f_k^\alpha) + 24 \sum_{1 \leq i < j < k < \ell \leq m} (f_i^\alpha) (f_j^\alpha) (f_k^\alpha) (f_\ell^\alpha),
\]
where \( f_i^\alpha = \mathcal{F}(f_i \oplus \varphi_\alpha) \) for \( 1 \leq i \leq m \) and \( \alpha \in \mathbb{F}_2^n \).

Moreover, we also give another form of Lemma 22.
Lemma 23. Let $F = (f_1, \ldots, f_m)$ be an $(n, m)$-function. Then
\[
\sum_{j=1}^{m} \sum_{i=1}^{m} (f_i^*)^2(f_j^*)^2 = \sum_{j=1}^{m} (f_i^*)^4 + 2 \sum_{1 \leq i < j \leq m} (f_i^*)^2(f_j^*)^2 + 4 \sum_{1 \leq i < j \leq m} (f_i^*)^3(f_j^*)^2
\]
\[+ 2 \sum_{j=1}^{m} \sum_{i,j,k,\ell \neq j} (f_i^*)^2(f_j^*)^2(f_k^*)^2(f_{\ell}^*)^2,\]
where $f_i^* = F(f_i \oplus \varphi_\alpha)$ for $1 \leq i \leq m$ and $\alpha \in \mathbb{F}_2^n$.

Based on Lemma 22 and Lemma 23, we have Theorem 24.

Theorem 24. Let $F = (f_1, \ldots, f_m)$ be a balanced $(n, m)$-function. Then
\[
\text{RTO}(F) \geq m - \sqrt{m(2^n - 1)} \left( \frac{m \cdot 2^{2n}}{\text{SNR}(DPA)(F)} \right)^{1/2} - \sum_{\alpha \in \mathbb{F}_2^n} \left( 4 \sum_{1 \leq i < j \leq m} (f_i^*)^2(f_j^*)^2 \right)
\]
\[+ 10 \sum_{j=1}^{m} \sum_{i,j,k,\ell \neq j} (f_i^*)^2(f_j^*)^2(f_k^*)^2(f_{\ell}^*)^2,\]
where $f_i^* = F(f_i \oplus \varphi_\alpha)$ for $1 \leq i \leq m$ and $\alpha \in \mathbb{F}_2^n$.

Remark 4. Although this relationship is rather rough, it can also reflect the relationship between the SNR and the RTO. Moreover, the definition of the SNR in [11] can be expressed by
\[
\text{SNR}(DPA)(F) = \frac{m \cdot 2^{2n}}{\left( \sum_{\alpha \in \mathbb{F}_2^n} (\sum_{i=1}^{m} F(f_i \oplus \varphi_\alpha))^4 \right)^{1/2}},
\]
\[
\sum_{\alpha \in \mathbb{F}_2^n} (\sum_{i=1}^{m} F(f_i \oplus \varphi_\alpha))^4 = \left( \frac{m \cdot 2^{2n}}{\text{SNR}(DPA)(F)} \right)^2 \geq 0,
\]
i.e.
\[
\left( \frac{m \cdot 2^{2n}}{\text{SNR}(DPA)(F)} \right)^2 \geq \sum_{\alpha \in \mathbb{F}_2^n} \left( 4 \sum_{1 \leq i < j \leq m} (f_i^*)^2(f_j^*)^2 \right)
\]
\[+ 10 \sum_{j=1}^{m} \sum_{i,j,k,\ell \neq j} (f_i^*)^2(f_j^*)^2(f_k^*)^2(f_{\ell}^*)^2 \geq 0.
\]

Combining the relation (5) and Theorem 24, we have
\[
\text{RTO}(F) \geq m - \sqrt{m(2^n - 1)} \left( \frac{m \cdot 2^{2n}}{\text{SNR}(DPA)(F)} \right)^{1/2}.
\]
It implies that the $\text{SNR}(DPA)(F)$ becomes larger, if $\text{RTO}(F)$ becomes larger.
5. Experimental data

By Theorem 19 and Theorem 20, we know that the SNR is not affine invariant. In the following we analyse SNR of (4,4) S-boxes. We know that a balanced (4,4) S-box corresponds to a 16-bit permutation, and the number of 16-bit permutations is 16! (= 2092278988800), which is about $2^{44.25}$. Moreover, according to the definition of the SNR, the Walsh transform of four component functions have to be calculated, and the number of the addition ($\sum$) in the Walsh transform for four component functions is at least $4 \times 2^4 \times 2^4 = 2^{10}$. If we ignore the scale of logical operations (for example vector inner product $\omega \cdot x$, addition $f(x) \oplus \omega \cdot x$, $(-1)^{f(x) \oplus \omega \cdot x}$, $x, \omega \in F_{2^2}$), this will take at least $2^{54.25}$ operations to calculate the SNR of all permutations.

It is almost infeasible for ordinary platform to finish simulations of the SNR of all balanced (4,4) S-boxes in some months. In this case, we only focus on calculating the SNR of (4,4) S-boxes in two aspects (see Section 5.1 and Section 5.2).

5.1. 302 affine equivalent S-boxes of all balanced (4,4) S-boxes.
Firstly, we give the SNR of 302 (4,4) S-boxes (affine equivalent [5]) in Table 3. And then we give the SNR of S-boxes in some well known encryption algorithms (such as Lblock [22], PRESENT [4], Piccolo [18], SKINNY [3], MANTIS [3], Marvin [19], Midori [1] and Gift [2]) in Table 4.

| Class | SNR(DPA)(F)_{(4,4)} | Number | Per(%) |
|-------|---------------------|--------|--------|
| 0     | 1.612137            | 1      | 0.33   |
| 1     | 1.663601            | 2      | 0.66   |
| 2     | 1.691253            | 9      | 2.98   |
| 3     | 1.705606            | 1      | 0.33   |
| 4     | 1.783290            | 1      | 0.33   |
| 5     | 1.976967            | 1      | 0.33   |
| 6     | 2.000000            | 1      | 0.33   |
| 7     | 2.023858            | 57     | 18.87  |
| 8     | 2.074252            | 14     | 4.64   |
| 9     | 2.128608            | 10     | 3.31   |
| 10    | 2.187475            | 43     | 14.24  |
| 11    | 2.218801            | 6      | 1.99   |
| 12    | 2.251512            | 4      | 1.32   |
| 13    | 2.398501            | 42     | 13.91  |
| 14    | 2.483682            | 29     | 9.60   |
| 15    | 2.529822            | 11     | 3.64   |
| 16    | 2.578633            | 16     | 5.30   |
| 17    | 2.685380            | 39     | 12.91  |
| 18    | 2.806586            | 6      | 1.99   |
| 19    | 2.945383            | 7      | 2.32   |
| 20    | 3.023716            | 1      | 0.33   |
| 21    | 3.108115            | 1      | 0.33   |
A note on the Signal-to-noise ratio of \((n,m)\)-functions

Table 4. The SNR of well known S-boxes

| Name of algorithm | S-box | SNR(DPA)(S-box)_{(4,4)} |
|-------------------|-------|-------------------------|
| Lblock [22]       | E9F0D4AB128376C5 | 2.945839 |
|                   | 4BE9FD0A7C562813 | 2.806586 |
|                   | 1E7CFD06B593248A | 2.806586 |
|                   | 768B0F3E9ACD5241 | 2.945839 |
|                   | E5F072CD1849BA63 | 2.945839 |
|                   | 2DBCFE097A631845 | 2.806586 |
|                   | B94E0FAD6C573812 | 2.945839 |
|                   | DAF0E49B218375C6 | 2.945839 |
|                   | 87E5FD06BC9A2413 | 2.806586 |
|                   | B5F0729D481CEA36 | 2.945839 |
| PRESENT [4]       | C56B90AD3EF84712 | 2.128608 |
| Piccolo [18]      | E4B238091A7F6C5D | 3.108115 |
| SKINNY [3]        | C6901A2B385D4E7F | 2.685380 |
| MANTIS [3]        | CAD3EBF789150246 | 1.663601 |
| Marvin [19]       | 021B83ED46F5C79A | 3.023716 |
| Midori [1]        | CAD3EBF789150246 | 1.663601 |
|                   | 1053E2F7DA9BC846 | 2.128608 |
| Gift [2]          | 1A4C6F392DB7508E | 2.398501 |

Remark 5. From Tables 3 and 4, we find three facts.

1) Table 3 gives the SNR of all 302 S-boxes of size \(4 \times 4\), which obtains a somewhat better insight in the behavior of this parameter. Our simulations also show that the SNR is confined within the range \(1.612137 \leq SNR(DPA)(F) \leq 3.108115\), which is consistent with the theoretical bound \(1 \leq SNR(DPA)(F) < 4\) for \((4,4)\) S-boxes (see Theorem 15).

2) In Table 3, the number of the SNR in the range \(SNR(DPA)(F)_{(4,4)} = [2.023858, 2.945839]\) equals to 284 = 57 + 14 + 11 + 42 + 6 + 10 + 43 + 6 + 39 + 6 + 7, which corresponds to about 94.04% of their total number. If we randomly select a \((4,4)\) S-box, the probability of the SNR for all \((4,4)\) S-boxes falling into the range \([2.023858, 2.945839]\) is 94.04%, which is quite high.

3) In Table 4, the SNR of 14 S-boxes (in 18 S-boxes with the well known encryption algorithms) is located in the range \([2.023858, 2.945839]\), and the SNR reaches the maximum value 3.108115 for only one S-box. It directly means the SNR of the \((4,4)\) S-boxes used in these algorithm is highly consistent to the SNR of 302 affine equivalent classes S-box.

5.2. The SNR of 16 classes of optimal \((4,4)\) S-boxes.

In 2007, Leander et al. gave 16 classes optimal \((4,4)\) S-boxes in [14]. These S-boxes satisfy three cryptographic properties: 1) the linearity is 8; 2) the difference is 8; 3) the algebraic degree is 3. The representatives of the truth table are put in Table 5.

By Theorem 19 and Theorem 20, for each type of S-box \(G = (g_1, g_2, g_3, g_4)\) \((g_i \in BF_4, i = 1, 2, 3, 4)\), we can calculate the SNR of its affine equivalent S-box \(A \circ G\) \((A\) is an invertible \(4\times4\) matrix in \(F_2\)). Here we do not consider the case of \(G(x \circ A \oplus b)\) \((A\) is an invertible \(4\times4\) matrix in \(F_2\), \(b \in F_2^4\)) because of \(SNR(DPA)(G(x \circ A \oplus b)) = SNR(DPA)(G(x))\) for \(A\) and \(b\) (see Theorem 19).
Table 5. Representatives for all 16 classes of optimal (4, 4) S-boxes [14]

| Class | (4, 4) S-boxes |
|-------|----------------|
| $G_0$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 11, 12, 9, 3, 14, 10, 5 |
| $G_1$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 11, 14, 3, 5, 9, 10, 12 |
| $G_2$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 11, 14, 3, 10, 12, 5, 9 |
| $G_3$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 12, 15, 3, 10, 14, 11, 9 |
| $G_4$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 12, 15, 3, 10, 14, 5, 3 |
| $G_5$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 3, 5 |
| $G_6$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 5, 3 |
| $G_7$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 12, 14, 11, 10, 9, 3, 5 |
| $G_8$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 9, 5, 10, 11, 3, 12 |
| $G_9$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 9, 5, 10, 11, 3, 12 |
| $G_{10}$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 11, 5, 10, 9, 3, 12 |
| $G_{11}$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 11, 10, 5, 9, 12, 3 |
| $G_{12}$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 11, 10, 9, 3, 12, 5 |
| $G_{13}$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 12, 9, 5, 11, 10, 3 |
| $G_{14}$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 12, 11, 3, 9, 5, 10 |
| $G_{15}$ | 0, 1, 2, 3, 4, 7, 15, 6, 8, 14, 12, 11, 9, 3, 10, 5 |

Moreover, we know that the number of the invertible $n \times n$ matrix in $\mathbb{F}_q$ is

$$q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1).$$

Thus, the number (denoted by $N_{(4 \times 4)}$) of the invertible 4×4 matrix in $\mathbb{F}_2$ is $N_{(4 \times 4)} = 20160$, i.e. the number of the affine S-boxes ($A \circ G$) of one S-boxes ($G$) is 20160, where $G$ is a 4-bit S-box and $A$ is an invertible 4×4 matrix. In what follows, we calculate the SNR of 322560 ($=16 \times 20160$) S-boxes. The specific simulations data are given in Tables 6, 7.

In order to describe these data, we give the following marks.

1) $A \circ G_i$: the affine equivalent S-boxes of $G_i$, where $A$ is an invertible 4×4 matrix in $\mathbb{F}_2$;
2) $RV$: the range of the SNR of $A \circ G_i$;
3) $DN$: the number of the different values of the SNR of $A \circ G_i$;
4) Mean, Variance: the mean value and the variance of the SNR of $A \circ G_i$, respectively.

Based on these marks, we obtain SNR(DPA)($G_i$) of each optimal representative class S-box $G_i$ ($i = 0, 1, 2, ..., 15$) in Table 6. Especially, for $G_0$, we give the distribution of the SNR of affine equivalent S-boxes $A \circ G_0$ in Table 7.

**Remark 6.** By Table 6 and Table 7, we find four facts.

1) $RV$ of the SNR of affine equivalent S-box $A \circ G_i$ is [1.600000, 3.108115], where $A$ is an invertible 4×4 matrix in $\mathbb{F}_2$, $i = 0, 1, 2, ..., 15$. For a certain class of $G_i$, the SNR of $A \circ G_i$ are different to the SNR of $G_i$.

2) There are 20160 affine equivalent S-boxes $A \circ G_i$ in each optimal S-boxes $G_i$ ($i = 0, 1, 2, ..., 15$), but the value distributions ($DN$) of the SNR of $A \circ G_i$ are only 15 cases, 17 cases, 21 cases and 22 cases, respectively. For example, there are 22
A note on the Signal-to-noise ratio of \((n, m)\)-functions

Table 6. The SNR of affine equivalent S-boxes of 16 optimal \((4, 4)\) S-boxes

| Class | SNR(DPA)(\(G_i\)) | \(RV\) | \(DN\) | Mean   | Variance |
|--------|-------------------|--------|--------|--------|----------|
| \(G_0\) | 2.945839 | [1.600000, 3.108115] | 22 | 2.457354 | 0.110006 |
| \(G_1\) | 2.685380 | [1.600000, 3.108115] | 22 | 2.456126 | 0.108045 |
| \(G_2\) | 2.685380 | [1.600000, 3.108115] | 22 | 2.456967 | 0.108855 |
| \(G_3\) | 2.685380 | [1.612137, 3.108115] | 15 | 2.466327 | 0.102287 |
| \(G_4\) | 3.108115 | [1.612137, 3.108115] | 17 | 2.466608 | 0.102820 |
| \(G_5\) | 3.108115 | [1.612137, 3.108115] | 17 | 2.466729 | 0.104456 |
| \(G_6\) | 3.108115 | [1.612137, 3.108115] | 17 | 2.465285 | 0.102820 |
| \(G_7\) | 2.806586 | [1.612137, 3.108115] | 16 | 2.47125 | 0.092405 |
| \(G_8\) | 2.945839 | [1.612137, 3.108115] | 22 | 2.45613 | 0.108452 |
| \(G_9\) | 2.685380 | [1.612137, 3.108115] | 22 | 2.453230 | 0.110267 |
| \(G_{10}\) | 2.685380 | [1.612137, 3.108115] | 22 | 2.452648 | 0.109412 |
| \(G_{11}\) | 2.685380 | [1.612137, 3.108115] | 17 | 2.464596 | 0.101206 |
| \(G_{12}\) | 2.685380 | [1.612137, 3.108115] | 17 | 2.448995 | 0.106486 |
| \(G_{13}\) | 2.945839 | [1.612137, 3.108115] | 17 | 2.481046 | 0.096809 |
| \(G_{14}\) | 2.945839 | [1.612137, 3.108115] | 21 | 2.465087 | 0.099087 |
| \(G_{15}\) | 2.945839 | [1.600000, 3.108115] | 21 | 2.466658 | 0.10133 |

Table 7. Distribution of the SNR of affine equivalent S-boxes of \(G_0\)

| Class | SNR(DPA)(\(A \circ G_0\)) | Number | Per(%) |
|--------|-----------------------------|--------|--------|
| 0      | 1.600000                    | 48     | 0.238095 |
| 1      | 1.612137                    | 120    | 0.595238 |
| 2      | 1.663601                    | 192    | 0.952381 |
| 3      | 1.691253                    | 312    | 1.547619 |
| 4      | 1.705606                    | 336    | 1.666667 |
| 5      | 1.720331                    | 144    | 0.714286 |
| 6      | 1.783290                    | 72     | 0.357143 |
| 7      | 2.023858                    | 792    | 3.928571 |
| 8      | 2.074252                    | 696    | 3.452381 |
| 9      | 2.128608                    | 624    | 3.095238 |
| 10     | 2.187475                    | 1968   | 9.761905 |
| 11     | 2.218801                    | 480    | 2.380902 |
| 12     | 2.251512                    | 432    | 2.142857 |
| 13     | 2.398501                    | 2328   | 11.547619 |
| 14     | 2.43682                     | 912    | 4.523810 |
| 15     | 2.529822                    | 2928   | 14.523810 |
| 16     | 2.578633                    | 1368   | 6.785714 |
| 17     | 2.685380                    | 3768   | 18.690476 |
| 18     | 2.806586                    | 672    | 3.333333 |
| 19     | 2.945839                    | 792    | 3.928571 |
| 20     | 3.023716                    | 240    | 1.190476 |
| 21     | 3.108115                    | 936    | 4.642857 |
cases of the SNR of $A \circ G_0$ in Table 7. This implies that the distribution of values is relatively concentrated.

3) The range of the mean value for the SNR of affine equivalent S-boxes $A \circ G_i$ belongs to the range of [2.448995, 2.481046], and the variance belongs to range of [0.092405, 0.110267]. The distribution of its value is concentrated in a relatively small interval.

4) Especially, we get the detailed distribution of the SNR of $A \circ G_0$ in Table 7. The calculation results of other $G_i$ ($i = 1, 2, 3, ..., 15$) are similar to Table 7, which is ignored due to the limited length of this paper.

6. Conclusions

In this paper, some exact bounds on the SNR of $(n, m)$-functions are investigated. In particular, we prove that the SNR of balanced $(n, m)$-functions should be less than $2^n/2$. Moreover, some relationships between the SNR of $(n, m)$-functions and three other cryptographic parameters are provided. Furthermore, the SNR of many $(4, 4)$ S-boxes are described via practical simulations.

ACKNOWLEDGMENTS

The authors are grateful to Dr. Li Luyang for computing all data in Table 3 and Table 4, and authors also are grateful to Dr. Tang Chunming and Dr. Tang Deng for their valuable suggestions. We would also like to thank the anonymous referees and editors very much for their valuable suggestions and comments that improved the quality of this paper.

REFERENCES

[1] S. Banik, A. Bogdanov and T. Isobe, et al., Midori: A block cipher for low energy, in Advances in Cryptology - ASIACRYPT 2015. Part II, Lecture Notes in Comput. Sci., 9453, Springer, Heidelberg, 2015, 411–436.

[2] S. Banik, S. K. Pandey and T. Peyrin, et al., GIFT: A small present - Towards reaching the limit of lightweight encryption, in Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, 10529, Springer, Cham, 2017, 321–345.

[3] C. Beierle, J. Jean and S. Kölbl, et al., The SKINNY family of block ciphers and its low-latency variant MANTIS, in Advances in Cryptology - CRYPTO 2016. Part II, Lecture Notes in Comput. Sci., 9815, Springer, Berlin, 2016, 123–153.

[4] A. Bogdanov, L. R. Knudsen and G. Leander, et al., PRESENT: An ultra-lightweight block cipher, in Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Comput. Sci., 4727, Springer, 2007, 450–466.

[5] C. D. Cannaïère, Analysis and Design of Symmetric Encryption Algorithms, Ph.D thesis, Katholieke Universiteit Leuven, 2007.

[6] C. Carlet, Boolean functions for cryptography and error-correcting codes, in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, 2010, 257–397.

[7] C. Carlet, Vectorial Boolean functions for cryptography, in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, 2010, 398–470.

[8] K. Chakraborty, S. Sarkar and S. Maitra, et al., Redefining the transparency order, Des. Codes Cryptogr., 82 (2017), 95–115.

[9] Y. Fei, Q. Luo and A. A. Ding, A statistical model for DPA with novel algorithmic confusion analysis, in Cryptographic Hardware and Embedded Systems - CHES 2012, Lecture Notes in Computer Science, 7428, Springer, 2012, 233–250.
A note on the Signal-to-noise ratio of \((n, m)\)-functions

[10] W. Fischer, B. M. Gammel, O. Kniffler and J. Velten, Differential power analysis of stream ciphers, in *Topics in Cryptology - CT-RSA 2007*, Lecture Notes in Comput. Sci., 4377, Springer, Berlin, 2006, 257–270.

[11] S. Guilley, P. Hoogvorst and R. Pacalet, Differential power analysis model and some results, in *Smart Card Research and Advanced Applications VI*, IFIP International Federation for Information Processing, 153, Springer, Boston, MA, 2004, 127–142.

[12] A. Heuser, O. Rioul and S. Guilley, A theoretical study of Kolmogorov-Smirnov distinguishers - Side-channel analysis vs. differential cryptanalysis, in *Constructive Side-Channel Analysis and Secure Design*, Lecture Notes in Comput. Sci., 8622, Springer, 2014, 9–28.

[13] P. Kocher, J. Jaffe and B. Jun, Differential power analysis, in *Advances in Cryptology - CRYPTO’99*, Lecture Notes in Comput. Sci., 1666, Springer, 1999, 388–397.

[14] G. Leander and A. Poschmann, On the classification of 4 bit S-boxes, in *Arithmetic of Finite Fields*, Lecture Notes in Comput. Sci., 4547, Springer, Berlin, 2007, 159–176.

[15] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar, New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity, in *International Workshop on Coding and Cryptography*, Electron. Notes Discrete Math., 6, Elsevier Sci. B. V., Amsterdam, 2001, 10pp.

[16] E. Prouff, DPA attacks and S-Boxes, in *Fast Software Encryption*, Lecture Notes in Comput. Sci., 3557, Springer, 2005, 424–441.

[17] P. Sarkar and S. Maitra, Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes, *Theory Comput. Syst.*, 35 (2002), 39–57.

[18] K. Shibutani, T. Isobe and H. Hiwatari, et al., Piccolo: An ultra-lightweight blockcipher, in *Cryptographic Hardware and Embedded Systems - CHES 2011*, Lecture Notes in Comput. Sci., 6917, Springer, 2011, 342–357.

[19] M. A. Simplicio Jr., P. D. F. F. S. Barbuda and P. S. L. M. Barreto, et al., The MARVIN message authentication code and the LETTERTSOUP authenticated encryption scheme, *Security Comm. Networks*, 2 (2009), 165–180.

[20] J. J. Son, J. I. Lim, S. Chee and S. H. Sung, Global avalanche characteristics and nonlinearity of balanced Boolean function, *Inform. Process. Lett.*, 65 (1998), 139–144.

[21] Q. Wang and P. Stănică, Transparency order for Boolean functions: Analysis and construction, *Des. Codes Cryptogr.*, 87 (2019), 2043–2059.

[22] W. Wu and L. Zhang, LBlock: A lightweight block cipher, in *Applied Cryptography and Network Security*, Lecture Notes in Comput. Sci., 6715, Springer, 2011, 327–344.

[23] X.-M. Zhang and Y. Zheng, GAC–The criterion for global avalanche characteristics of cryptographic functions, *J. UCS*, 1 (1995), 320–337.

[24] Y. Zheng and X.-M. Zhang, On plateaued functions, *IEEE Trans. Inform. Theory*, 47 (2001), 1215–1223.

[25] Y. Zhou, L. Wang, W. Wang, X. Dong and X. Du, One sufficient and necessary condition on balanced Boolean functions with \(\sigma_f = 2^{2n} + 2^{n+3} (m \geq 3)\), *Internat. J. Found. Comput. Sci.*, 25 (2014), 343–353.

[26] Y. Zhou, M. Xie and G. Xiao, On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, *Inform. Sci.*, 180 (2010), 256–265.

[27] Y. Zhou, W. Zhang, S. Zhu and G. Xiao, The global avalanche characteristics of two Boolean functions and algebraic immunity, *Int. J. Comput. Math.*, 89 (2012), 2165–2179.

Received June 2019; 1st revision October 2019; final revision March 2020.

E-mail address: zhouyu.zhy@tom.com
E-mail address: xinfengdong@163.com
E-mail address: walker_wyz@guet.edu.cn
E-mail address: zhfl203@cumt.edu.cn