Research Article

Zhenyu Liu and Zepeng Zhuo*

Further research results on confusion coefficient of Boolean functions

https://doi.org/10.1515/jmc-2021-0039
received September 23, 2021; accepted April 06, 2023

Abstract: The notion of confusion coefficient (CC) is a property that attempts to characterize the confusion property of cryptographic algorithms against differential power analysis. In this article, we establish a relationship between CC and the transparency order (TO) for any Boolean function and deduce some relationships between the sum-of-squares of CC, signal-to-noise ratio, and TO. We also give a tight upper bound and a tight lower bound on the sum-of-squares of CC for balanced s-plateaued functions. Finally, the results generalized a lower bound on the sum-of-squares of CC of Boolean functions with the Hamming weight k.

Keywords: transparency order, Boolean function, confusion coefficient, nonlinearity, signal-to-noise ratio

MSC 2020: 94-D10

1 Introduction

Side-channel analysis (SCA) is a very powerful technique for block ciphers [1]. Differential power analysis (DPA) is one of the effective methods of SCA. To improve the resistance of a block cipher to DPA, the substitution boxes ((n, m)-functions or S-boxes), as the most important nonlinear part of block ciphers, should have some features reducing the information leakage. Currently, there are three important indicators regarding the resistance of S-boxes against DPA-like attacks.

(1) Signal-to-noise ratio (SNR) following [2] was proposed by Guilley at CARDIS conference in 2004. First, they built a complete model of information leakage based on the framework of traditional cryptographic analysis, so that the attacker could obtain the autocorrelation value of Hamming weight of the guessed key value.

(2) In 2005, transparency order (TO) was introduced for (n, m)-functions based on single-bit DPA and the Hamming distance model in the study by Prouff [3]. With the in-depth research of scholars' cryptology, Chakraborty et al. [4] refined TO with the cross-correlation function, and they found that the refined TO has impact on the resistance of the implementation against DPA attacks.

(3) In 2012, confusion coefficient (CC) was presented when they studied the confusion property of cryptographic algorithms in the study by Fei et al. [5]. Based on the results of the study by Fei et al. [5], Picek et al. [6] calculated the nonlinearity of S-boxes of different sizes in 2014 and obtained the variance of CC. In the same year, Qiu et al. [7] revised the original CC and gave a new definition of CC in order to reduce the dimension and the number of CC.

The organization of this article is as follows. In Section 2, the basic concepts and notions are presented. In Section 3, we deduce the relationship between TO and CC. In Section 4, we derive the lower bound on the sum of squares of CC from TO and sum of squares of Boolean functions and give the relationships between CC, SNR and TO. We also investigate the upper bound and lower bound on the sum-of-squares of CC for a s-plateaued function and discuss the lower bound on the sum-of-squares of CC of Boolean function with the Hamming weight k. We end in Section 5 with conclusions.

*** Corresponding author: Zepeng Zhuo,** School of Mathematical Science, Huaibei Normal University, Huaibei, Anhui 235000, China; School of Cyber Science, University of Science and Technology of China, Hefei 230027, China, e-mail: 342647200@qq.com
Zhenyu Liu: School of Mathematical Science, Huaibei Normal University, Huaibei, Anhui 235000, China

2 Preliminaries

Let n be a positive integer, F_2 be the binary finite field, F_2^n be the n-dimensional vector space on F_2 and B_n be the set of all n-dimensional Boolean functions. The support of a Boolean function $f \in B_n$ is defined as $\mathrm{Supp}(f) = \{(x_1, x_2, \ldots, x_n) \in F_2^n | f(x_1, x_2, \ldots, x_n) = 1\}$. The Hamming weight of f is denoted by $wt(f)$, that is, $wt(f) = |\mathrm{Supp}(f)|$.

For any function $f \in B_n$, the Walsh transform of f (also known as the Walsh spectrum) is defined as:

$$F(f + \varphi_a) = \sum_{x \in F_2^n} (-1)^{f(x)+\varphi_a(x)},$$

where $\varphi_a(x) = a \cdot x = x_1a_1 + x_2a_2 + \cdots + x_na_n$. We denote by + the additions in F_2, in F_2^n and in B_n.

The Hamming distance between two functions f and g, denoted $d(f, g) = wt(f + g)$. We say that an n-variable Boolean function f is balanced if $wt(f) = 2^{n-1}$. Let $f \in B_n$, the nonlinearity of f is $N_f = \min_{g \in A_n} d(f, g)$, and it can be determined by:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} |F(f + \varphi_a)|.$$

Any $f \in B_n$ can be expressed in algebraic normal form (ANF) as:

$$f(x) = \bigoplus_{I \in P_N} a_I \left(\prod_{i \in I} \right) = \bigoplus_{I \in P_N} a_I x^I,$$

where P_N denotes the power set of $N = 1, \ldots, n$ in ref. [14]. 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 $\deg(f)$ and is called the algebraic degree of the function: $\deg(f) = \max\{|I| : a_I \neq 0\}$, where $|I|$ denotes the size of I. A Boolean function is an affine function if its algebraic degree satisfies $\deg(f) < 2$, and the set of all affine functions is denoted by A_n.

The nonlinearity of an n-variable Boolean function is less than or equal to $2^{n-1} - 2^{\frac{n}{2}-1}$, and a function is called bent if it attains this bound.

Let $f, g \in B_n$. The cross-correlation function of f and g is defined as:

$$\Delta_{f,g}(a) = \sum_{x \in F_2^n} (-1)^{f(x)+g(x+a)}, a \in F_2^n.$$

If $f = g$, then the autocorrelation function of f at $a \in F_2^n$ is defined as:

$$\Delta_f(a) = \sum_{x \in F_2^n} (-1)^{f(x)+f(x+a)}.$$

The two indicators (σ_f, Δ_f) are called the global avalanche characteristics of a Boolean function $f \in B_n$:

$$\sigma_f = \sum_{x \in F_2^n} [\Delta_f(a)]^2, \Delta_f = \max_{a \in F_2^n, a \neq 0} |\Delta_f(a)|.$$

Let n and m be two positive integers. The functions $F = (f_1, \ldots, f_m), f_i \in B_n$, be a vectorial function from F_2^n to F_2^m, and the Boolean functions $f_1, f_2, \ldots, f_m$ are called the coordinate functions of F.

TO of F is defined by:

$$\mathrm{TO}(F) = \max_{\beta \in F_2^m} \left(m - \frac{1}{2^{2n} - 2^n} \sum_{y \in F_2^{n^*}} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{\beta_i + \beta_j} \Delta_{f_i, f_j}(y) \right| \right),$$

where

$$\Delta_{f_i, f_j}(y) = \sum_{x \in F_2^n} (-1)^{f_i(x)+f_j(x+y)}$$

is the cross-correlation between f_i, f_j (if $f_i = f_j$, we shall use the notation Δ_{f_i} and call it the autocorrelation of f_i). If $m = 1$, then $F = f$ is a Boolean function, and

$$\mathrm{TO}(f) = 1 - \frac{1}{2^n(2^n-1)} \sum_{y \in F_2^{n^*}} \left| \sum_{x \in F_2^n} (-1)^{f(x)+f(x+y)} \right|.$$

This article only focus on the case when $m = 1$.

The next definition gives the distribution of the Walsh spectra for a three-valued Boolean function.

Let $f \in B_n$. Then, for any $a \in F_2^n$,

$$\sum_{y \in F_2^n} \sum_{x \in F_2^n} (-1)^{f(x)+f(x+y)+a \cdot y} = F^2(f + \varphi_a).$$

The SNR of f is defined by:

$$\mathrm{SNR}(f) = \frac{2^{2n}}{\sqrt{\sum_{a \in F_2^n} F^4(f + \varphi_a)}}.$$

Let k_i and $k_j \in F_2^n$ be two keys. The CC κ over (k_i, k_j) is defined as:

$$\kappa = \kappa(k_i, k_j) = \Pr[(\psi|k_i) \neq (\psi|k_j)] = \frac{N_{(\psi|k_i) \neq (\psi|k_j)}}{N_t},$$

where N_t is the total number of values for the relevant ciphertext bits, and $N_{(\psi|k_i) \neq (\psi|k_j)}$ is the number of occurrences for which different key hypotheses k_i and k_j result in different ψ values.

Carlet et al. [8] studied the intrinsic resiliency of S-boxes against SCA and further gave the concrete form of CC for a Boolean function $f \in B_n$:

$$\kappa(k, k^*) = \frac{1}{2^{n+2}} \sum_{t \in F_2^n} [f(t + k^*) - f(t + k)]^2,$$

where $t \in F_2^n$ is one known plaintext, $k^* \in F_2^n$ is the correct key and $k \in F_2^n$ is the key.

3 Relationship between TO and CC

We first discuss the relationship between TO and CC.

Lemma 1. [9] *Let $f \in B_n$. $k^*, k \in F_2^n$, and $k + k^* \neq 0$. Then,*

$$\kappa(k, k^*) \geq \frac{1}{4} - \frac{(2^n - 2N_f)^2}{2^{n+3}}.$$

Lemma 2. [10] *Let $f \in B_n$. Then,*

$$\mathrm{TO}(f) = 1 - \frac{(2^n - 2N_f)^2}{2^n(2^n-1)} + \frac{1}{2^n - 1}.$$

According to Lemmas 1 and 2, we obtain Theorem 1.

Corollary 1. *Let $f \in B_n.k^*, k \in F_2^n$, and $k + k^* \neq 0$. Then,*

$$\mathrm{TO}(f) \leq 1 - \frac{1 - 8\kappa(k, k^*)}{2^n - 1}.$$

Proof. By Lemma 1, we have

$$(2^n - 2N_f)^2 \geq \left[\frac{1}{4} - \kappa(k, k^*)\right] 2^{n+3},$$

and from Lemma 2, we have

$$\begin{aligned}\mathrm{TO}(f) &\le 1 - \frac{2^{n+3}\left[\frac{1}{4} - \kappa(k,k^*)\right]}{2^n(2^n-1)} + \frac{1}{2^n-1}\\ &= 1 - \frac{2 - 8\kappa(k,k^*)}{2^n-1} + \frac{1}{2^n-1}\\ &= 1 - \frac{1 - 8\kappa(k,k^*)}{2^n-1}.\end{aligned}$$

□

According to Corollary 1, we can find that the smaller CC of a Boolean function is, the smaller the upper bound of TO is.

4 Some research results of sum-of-squares of CC

4.1 Bounds on the sum-of-squares of CC of one Boolean function

For the convenience, for a given $k^* \in F_2^n$, we denoted the sum-of-squares of CC for a Boolean function by:

$$K_f(k^*) = \sum_{k\in F_2^n} \kappa^2(k,k^*).$$

Lemma 3. [12] *Let $f \in B_n$. For a given $k^* \in F_2^n$, we have*

$$K_f(k^*) = 2^{n-6} - \frac{[2^n - 2wt(f)]^2}{2^{n+5}} + \frac{\sigma_f}{2^{2n+6}}.$$

Theorem 1. *Let $f \in B_n$. For a given $k^* \in F_2^n$, we have*

$$K_f(k^*) \ge 2^{n-6} - \frac{(2^n-1)\mathrm{TO}(f) - 2^n}{32} + \frac{\sigma_f}{2^{2n+6}}.$$

Proof. We know the Walsh spectrum of $f(x)$ at $a = 0$ is

$$F(f+\varphi_0) = \sum_{x\in F_2^n} (-1)^{f(x)} = 2^n - 2wt(f),$$

$$\sum_{y\in F_2^{n^*}} \left| \sum_{x\in F_2^n} (-1)^{f(x)+f(x+y)} \right| \ge \max_{a\in F_2^n} F^2(f+\varphi_a) - 2^n.$$

$$\sum_{y\in F_2^{n^*}} \left| \sum_{x\in F_2^n} (-1)^{f(x)+f(x+y)} \right| \ge F^2(f+\varphi_0) - 2^n = [2^n - 2wt(f)]^2 - 2^n.$$

From the definition of TO

$$\begin{aligned}\mathrm{TO}(f) &= 1 - \frac{1}{2^n(2^n-1)} \sum_{y\in F_2^{n^*}} \left| \sum_{x\in F_2^n} (-1)^{f(x)+f(x+y)} \right|\\ &\le 1 - \frac{[2^n - 2wt(f)]^2 - 2^n}{2^n(2^n-1)}.\end{aligned}$$

Based on Lemma 3,

$$[2^n - 2wt(f)]^2 = 2^{n+5}\left[2^{n-6} + \frac{\sigma_f}{2^{2n+6}} - K_f(k^*)\right].$$

Thus,

$$\mathrm{TO}(f) \le 1 - \frac{2^{3n} + \sigma_f - 2^{2n+6}K_f(k^*) - 2^{2n+1}}{2^{2n+1}(2^n - 1)}.$$

$$K_f(k^*) \ge 2^{n-6} + \frac{(2^n - 1)\mathrm{TO}(f) - 2^n}{32} + \frac{\sigma_f}{2^{2n+6}}.$$ □

According to Theorem 1, we can find that the bigger the TO and the σ_f of a Boolean function is, the bigger the lower bound of the $K_f(k^*)$ is.

4.2 Relationships between $K_f(k^*)$, SNR, and TO

In this section, we give the relationships between the $K_f(k^*)$, the SNR, and the TO.

Lemma 4. [12] *Let $f \in B_n$. For a given $k^* \in F_2^n$, we have*

$$K_f(k^*) = 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right] - \frac{[2^n - 2wt(f)]^2}{2^{n+5}}.$$

Theorem 2. *Let $f \in B_n$. For a given $k^* \in F_2^n$, we have*

$$K_f(k^*) \ge 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right] + \frac{(2^n - 1)\mathrm{TO}(f)}{2^5} - 2^{n-5}.$$

Proof. By Lemma 4,

$$K_f(k^*) = 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right] - \frac{[2^n - 2wt(f)]^2}{2^{n+5}}.$$

Clearly,

$$\sum_{y \in F_2^{n^*}} \left| \sum_{x \in F_2^n} (-1)^{f(x)+f(x+y)} \right| \ge [2^n - 2wt(f)]^2 - 2^n,$$

Therefore,

$$\mathrm{TO}(f) \le 1 - \frac{[2^n - 2wt(f)]^2 - 2^n}{2^n(2^n - 1)},$$

$$[2^n - 2wt(f)]^2 \le 2^n + 2^n(2^n - 1)[1 - \mathrm{TO}(f)].$$

Hence,

$$\begin{aligned} K_f(k^*) &\ge 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right] - \frac{2^n + 2^n(2^n - 1)[1 - \mathrm{TO}(f)]}{2^{n+5}} \\ &= 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right] - \frac{2^n + (2^n - 1)[2^n - 2^n\mathrm{TO}(f)]}{2^{n+5}} \\ &= 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right] + \frac{(2^n - 1)\mathrm{TO}(f)}{2^5} - 2^{n-5}. \end{aligned}$$ □

Based on Theorem 2, we know that the lower bound of sum-of-squares of CC is directly proportional to TO and inversely proportional to SNR for a Boolean function; thus, these indicators cannot be the best at the same time.

4.3 Bounds on the sum-of-squares of CC of s-plateaued function

Further, recall that $f \in B_n$ is called plateaued if $|F(f+\varphi_u)| \in \{0, 2^{\frac{n+s}{2}}\}$ for all $u \in F_2^n$ for a fixed integer s depending on f (we also then call f is s-plateaued).

Lemma 5. [13] *Let $f \in B_n$, then*

$$\mathrm{SNR}(f) \geq \frac{2^n}{2^n - 2N_f}.$$

Lemma 6. [12] *Let $f \in B_n$ be a balanced Boolean function. For a given $k \in F_2^n$, we have*

$$K_f(k^*) \geq 2^{n-6} + \frac{[2^n - (2^n-1)\mathrm{TO}(f)]^2}{2^{n+6}}.$$

Theorem 3. *Let $f \in B_n$ be a balanced s-plateaued function, we have*

$$2^{n-6}(1 + 2^{2s-2n}) \leq K_f(k^*) \leq 2^{n-6}(1 + 2^{s-n}).$$

Proof. By Lemma 4, we know that $f \in B_n$ be a balanced Boolean function. For a given $k \in F_2^n$, we have

$$K_f(k^*) = 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right].$$

According to the condition and Lemma 5, we know that $f \in B_n$ be a balanced s-plateaued function, then

$$\begin{aligned} N_f &= 2^{n-1} - 2^{\frac{n+s}{2}-1}, \\ K_f(k^*) &= 2^{n-6}\left[1 + \frac{1}{\mathrm{SNR}^2(f)}\right] \\ &\leq 2^{n-6}\left[1 + \frac{(2^n - 2N_f)^2}{2^{2n}}\right] \\ &\leq 2^{n-6}(1 + 2^{s-n}). \end{aligned}$$

Based on Lemma 2, Lemma 6, and the condition, we have

$$\begin{aligned} K_f(k^*) &\geq 2^{n-6} + \frac{[2^n - (2^n-1)\mathrm{TO}(f)]^2}{2^{n+6}} \\ &\geq 2^{n-6} + \frac{\left[2^n - (2^n-1)\left(1 - \frac{(2^n-2N_f)^2}{2^n(2^n-1)} + \frac{1}{2^n-1}\right)\right]^2}{2^{n+6}} \\ &= 2^{n-6} + 2^{2s-n-6} \\ &= 2^{n-6}(1 + 2^{2s-2n}). \end{aligned}$$

Thus, this result is proved. □

Example 1. If $s = 1$(n must then be odd), or $s = 2$(n must then be even), we call *fsemi − bent*. We can make Tables 1 and 2.

Table 1: $s = 1$: the bounds on $K_f(k^*)$ for balanced s-plateaued function

n	Lower bound on $K_f(k^*)$	Upper bound on $K_f(k^*)$
1	0.0625	0.0625
3	0.1328	0.1563
5	0.5020	0.5313

Table 2: $s = 2$: the bounds on $K_f(k^*)$ for balanced s-plateaued function

n	Lower bound on $K_f(k^*)$	Upper bound on $K_f(k^*)$
2	0.125	0.125
4	0.2656	0.3125
6	1.0039	1.0625

4.4 Bounds on the sum-of-squares of CC of Boolean function with the Hamming weight k

Finally, we discuss some properties of CC of Boolean function with the hamming weight k.

Lemma 7. [11] *Let* $f \in B_n$, $wt(f) = k$, *and* $\left\lfloor \frac{k(k-1)}{2(2^n-1)} \right\rfloor = t$. *Then,*

$$\sigma_f \geq 2^{3n} + 3 \cdot 2^{n+3}k^2 - 2^{2n+3}k - 32 \cdot k^3 + 16 \cdot k^2 + 2^5[(2t+1)(k^2-k) - (2^{n+1}-2)(t^2+t)].$$

Theorem 4. *Let* $f \in B_n$. $wt(f) = k$ *and* $\left\lfloor \frac{k(k-1)}{2(2^n-1)} \right\rfloor = t$, *then*

$$K_f(k^*) \geq 2^{n-5} - \frac{(2^n-2k)^2}{2^{n+5}} + \frac{3k^2}{2^{n+3}} - \frac{k}{8} - \frac{k^3}{2^{2n+1}} + \frac{k^2}{2^{2n+2}} + \frac{(2t+1)(k^2-k)}{2^{2n+1}} - \frac{(2^{n+1}-2)(t^2+t)}{2^{2n+1}}.$$

Proof. By Lemma 7, we know that:

$$\begin{aligned} K_f(k^*) &= 2^{n-6} - \frac{[2^n - 2wt(f)]^2}{2^{n+5}} + \frac{\sigma_f}{2^{2n+6}} \\ &\geq 2^{n-6} - \frac{(2^n-2k)^2}{2^{n+5}} + \frac{2^{3n} + 3 \cdot 2^{n+3}k^2 - 2^{2n+3}k - 32k^3 + 16k^2}{2^{2n+6}} \\ &\quad + \frac{2^5[(2t+1)(k^2-k) - (2^{n+1}-2)(t^2+t)]}{2^{2n+6}} \\ &= 2^{n-5} - \frac{(2^n-2k)^2}{2^{n+5}} + \frac{3k^2}{2^{n+3}} - \frac{k}{8} - \frac{k^3}{2^{2n+1}} + \frac{k^2}{2^{2n+2}} \\ &\quad + \frac{(2t+1)(k^2-k)}{2^{2n+1}} - \frac{(2^{n+1}-2)(t^2+t)}{2^{2n+1}}. \end{aligned}$$

□

Table 3: Lower bound on $K_f(k^*)$ for balanced Boolean functions

n	Lower bound on $K_f(k^*)$
3	0.1563
4	0.2734
5	0.5196
6	1.0176
7	2.0167

Example 2. We can deduce that $K_f(k^*) \geq 2^{n-6} - 2^{-n-3} - 2^{-6}$, $(n \geq 3)$ if f is the balanced Boolean function. Table 3 can be drawn.

5 Conclusion

In this article, we give the relationship between CC and TO. And we also give the relationships between sum-of-squares of CC, TO, and SNR of Boolean function. Furthermore, we give the upper and lower bound on the sum-of-squares of CC of s-plateaued function and the lower bound on sum-of-squares of CC of Boolean function with the Hamming weight k. But CC and other cryptographic indicators cannot reach the best; at the same time, we hope that these results of Boolean functions will help us to construct good S-box in the future.

Funding information: This study was supported by the Natural Science Foundation of Anhui Higher Education institutions of China (No. KJ2020ZD008) and Graduate Innovation Fund of Huaibei Normal University (No. yc2021022).

Conflict of interest: Authors state no conflict of interest.

References

[1] Kocher P, Jaffe J, Jun B. Differential power analysis. Advances in Cryptology-CRYPTOa99. LNCS 1666. Berlin: Springer; 1999. p. 388–397.
[2] Guilley S, Hoogvorst P, Pacalet R. Differential power analysis model and some results. In Smart Card Research and Advanced Applications VI, IFIP 18th World Computer Congress, TC8/WG8.8 and TC11/WG11.2 Sixth International Conference on Smart Card Research and Advanced Applications(CARDIS), Toulouse, France, 2004. p. 127–142.
[3] Prouff E. DPA attacks and s-boxes. Fast Software Encryption-FSE 2005. LNCS 3557. Berlin, Heidelberg: Springer; 2005. p. 424–441.
[4] Chakraborty K, Sarkar S, Maitra S, Mazumdar B, Mukhopadhyay D, Prouff E. Redefining the transparency order. Designs Codes Cryptography. 2017;82(1):95–115.
[5] Fei Y, Luo Q, Ding AA. A statistical model for DPA with novel algorithmic confusion analysis. International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer; 2012. p. 233–250.
[6] Picek S, Papagiannopoulos K, Ege B, Batina L, Jakobovic D. Confused by confusion: systematic evaluation of DPA resistance of various s-boxes. In: Meier W, Mukhopadhyay D. (eds). Progress in Cryptology-INDOCRYPT 2014, LNCS 8885. 2014. p. 374–390.
[7] Qiu S, Bai GQ, Chen HY. One-dimensional confusion coefficient for block cipher. J Cryptol Res. 2014;1(2):124–133.
[8] Carlet C, de Chérisey É, Gulley S, Kavut S, Tang D. Intrinsic resiliency of S-boxes against Side-channel Attacks-best and Worst Scenarios. IEEE Trans Informa Forensic Secur. 2021;16:203–218.
[9] Zhang XM, Zheng YL. Auto-correlations and new bounds on the nonlinearity of Boolean functions. EUROCRYPT'96 Proceedings, LNCS. Vol. 1070. Berlin, Heidelberg: Springer-Verlag; 1996. p. 294–306.
[10] Wang QC, Stanica P. Transparency order for Boolean functions: analysis and construction. Designs Codes Cryptography. 2019;87(9):2043–2059.
[11] Zhou Y, Wang WQ, Xiao GZ. Global avalanche characteristics and nonlinearity of Boolean function with the Hamming weight k. J Electron Inform Technol. 2009;31(2):435–438.
[12] Zhou Y, Hu JY, Miao XD, Han Y, Zhang F. On the confusion coefficient of Boolean functions. J Math Cryptol. 2022;16:1–13.
[13] Zhou Y, Zhao W, Chen ZX, et al. On the signal-to-noise ratio for Boolean functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020;E103.A(12).
[14] Crama E, Hammer PL. Boolean models and methods in mathematics, computer science, and engineering. Cambridge, UK: Cambridge University Press; 2010.