Hindawi
Security and Communication Networks
Volume 2019, Article ID 1348639, 15 pages
https://doi.org/10.1155/2019/1348639

Research Article

Measuring the Sum-of-Squares Indicator of Boolean Functions in Encryption Algorithm for Internet of Things

Yu Zhou,[1] **Yongzhuang Wei**,[2] **and Fengrong Zhang**[3]

[1] *Science and Technology on Communication Security Laboratory, Chengdu 610041, China*
[2] *Department of Communication and Information Engineering, Guilin University of Electronic Technology, Guilin 541004, China*
[3] *China University of Mining Technology School of Computer Science and Technology, Xuzhou 221116, China*

Correspondence should be addressed to Yu Zhou; zhouyu.zhy@tom.com

Received 24 January 2019; Accepted 27 February 2019; Published 27 March 2019

Guest Editor: Fagen Li

Encryption algorithm has an important application in ensuring the security of the Internet of Things. Boolean function is the basic component of symmetric encryption algorithm, and its many cryptographic properties are important indicators to measure the security of cryptographic algorithm. This paper focuses on the sum-of-squares indicator of Boolean function; an upper bound and a lower bound of the sum-of-squares on Boolean functions are obtained by the decomposition Boolean functions; some properties and a search algorithm of Boolean functions with the same autocorrelation (or cross-correlation) distribution are given. Finally, a construction method to obtain a balanced Boolean function with small sum-of-squares indicator is derived by decomposition Boolean functions. Compared with the known balanced Boolean functions, the constructed functions have the higher nonlinearity and the better global avalanche characteristics property.

1. Introduction

The Internet of Things is an important part of the new generation of information technology and also an important stage of information development. But the Internet of Things is being threatened and attacked by more and more potential threats and attacks [1, 2]. As Internet of Things evolves, these networks, and many others, will be connected with security and management capabilities and so forth.

The current-time wireless sensor network is attacked by hackers from time to time, and it has put up a new challenge for information security. With wireless communication, low cost, resource constraints, and so forth, current threats include differential power analysis, kinds of keys decryption, Trojan attacks, virus damage, and physical method.

Because of the special use of wireless sensor, the design of key storage, distribution, and encryption or decryption algorithm is inconvenient. Therefore, we need to be practical and convenient for the cryptographic algorithm in resource-constrained environment, the most basic of which is to clarify the cryptographic properties of cryptographic components.

The scenarios used in the Internet of Things are mostly resource-constrained, so its cryptographic algorithm requires some hardware and software requirements, low power consumption, moderate security intensity, and limited resource area, which makes the design of such cryptographic algorithm more difficult. Therefore, the research of cryptographic components in cryptographic algorithm is very important.

Symmetric cryptographic algorithm is the most widely used in cooperative networks. Its advantage is to ensure the confidentiality of communication data. If the algorithm is authenticated, it can ensure the integrity of communication data. Block cipher and stream cipher are two main design directions. Boolean function, as the most basic and widely used cryptographic component, has been highly studied by scholars, for example, linear feedback shift registers (LFSR), S-box, and MDS.

Boolean functions have many cryptographical indicators, including balance, high nonlinearity, high algebraic degree, resilience, propagation characteristic [3], global avalanche characteristic (GAC) [4], algebraic immunity [5], and transparency order [6]. Among these properties, GAC can link with other cryptographic indicators. In 1995, Zhang and Zheng introduced the global avalanche characteristic (GAC [4]: the sum-of-squares indicator (σ_f), the absolute indicator ($\triangle_f$)) for an n-variable Boolean function $f(x)$, and they gave the lower and the upper bounds on the two indicators. Reference [4] implied that the smaller σ_f and $\triangle_f$, the better the GAC of a Boolean function. In 1998, Son et al. [7] gave a lower bound on these indicators for a balanced Boolean function: $\sigma_f \geq 2^{2n} + 2^{n+3}$ and $\triangle_f \geq 8(n \geq 3)$. Sung et al. [8] improved these results and provided a bound on the sum-of-squares indicator of balanced functions satisfying the propagation criterion with respect to t vectors. In 2010, [9] generalized the GAC and put up a new criterion based on the cross-correlation functions: the sum-of-squares indicator ($\sigma_{f,g}$) and the absolute indicator ($\triangle_{f,g}$) for two n-variable Boolean functions $f(x), g(x)$; they gave the lower and the upper bounds on the two indicators. Reference [10] derived a new bound on the sum-of-squares indicator and gave a method to construct balanced Boolean functions with $n(n \geq 6)$ variables by the disjoint spectra functions, where n is an even integer, satisfying strict avalanche criterion, high nonlinearity, and lower GAC.

Meanwhile, some authors gave lots of constructions of Boolean functions with good GAC, Tang [11] gave a method to construct balanced Boolean functions of n variables, the constructed functions possess the highest nonlinearity and the better global avalanche characteristics (GAC) property, but they only obtained an upper bound of GAC. Reference [12] gave a method to construct high nonlinearity Boolean function. These constructions had not considered Boolean functions with the same autocorrelation distributions or the same cross-correlation distributions. If these functions have the same autocorrelation distributions or the same cross-correlation distributions, then these Boolean functions have the same GAC [4], the same transparency order [6], the same nonlinearity, the same absolute value of Walsh spectrum, the same correlation immunity, the same propagation criterion, and so forth. Thus, this paper will construct a Boolean function with small GAC, and we give some relationships of the sum-of-squares indicator between an n-variable Boolean function and four $(n-2)$–variable decomposition Boolean functions; the relationships are based on construction on Boolean functions with good global avalanche characteristics.

Based on the above consideration, we study the following questions:

(1) What is a clear characterization of four $(n-2)$-variable decomposition functions, if the sum-of-squares indicator of an n-variable Boolean function is lower? This study provides theoretical support for the security of lightweight dynamic cryptographic algorithms in the Internet of Things.

(2) What are the cross-correlation properties of any two Boolean functions, if Boolean functions have the same autocorrelation distribution? This research lays a foundation for lightweight dynamic cryptographic algorithms in the Internet of Things.

(3) How to construct a Boolean function with good global avalanche characteristics. This study provides some algorithm component for the lightweight dynamic cryptographic algorithms in the Internet of Things.

The rest of this paper is organized as follows: Section 2 introduces some basic definitions. In Section 3, an upper bound on the sum-of-squares indicator of n-variable Boolean function by using four decomposition $(n-2)$-variable Boolean functions is given. Section 4 gives some properties of a Boolean function with the upper bound on the sum-of-squares indicator. In Section 5, we give a construction of one Boolean function with small sum-of-squares indicator by the disjoint spectrum method. Finally, Section 6 concludes this paper.

2. Preliminaries

Let $\mathbb{B}_n$ denote the set of n variables Boolean functions. We denote by $\oplus$ the additions in $\mathbb{F}_2$, in $\mathbb{F}_2^n$, and in $\mathbb{B}_n$. Every Boolean function $f(x) \in \mathbb{B}_n$ admits a unique representation called its algebraic normal form (ANF) as a polynomial over $\mathbb{F}_2$:

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{1\leq i\leq n} a_i x_i \oplus \bigoplus_{1\leq i<j\leq n} a_{i,j} x_i x_j \oplus \cdots \oplus a_{1,\ldots,n} x_1 x_2 \cdots x_n \quad (1)$$

where the coefficients $a_0, a_i, a_{i,j}, \ldots, a_{1,\ldots,n} \in \mathbb{F}_2$. The algebraic degree, $\deg(f)$, is the number of variables in the highest-order term with nonzero coefficient. The support of a Boolean function $f(x) \in \mathbb{B}_n$ is defined as $\mathrm{Supp}(f) = \{(x_1, \ldots, x_n) \mid f(x_1, \ldots, x_n) = 1\}$. We say that a Boolean function $f(x)$ is balanced if its truth table contains an equal number of ones and zeros, that is, if its Hamming weight equals 2^{n-1}. A Boolean function is affine if there exists no term of degree > 1 in the ANF and the set of all affine functions is denoted by $\mathbb{A}_n$. An affine function with constant term equal to zero is called a linear function.

Definition 1. The Walsh spectrum of $f(x) \in \mathbb{B}_n$ is defined as

$$\mathcal{F}(f \oplus \varphi_\alpha) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\alpha x}, \quad (2)$$

where $\varphi_\alpha = \alpha x = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \cdots \oplus \alpha_n x_n$.

Definition 2. The cross-correlation function between $f(x), g(x) \in \mathbb{B}_n$ is defined as

$$\triangle_{f,g}(\alpha) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus g(x\oplus\alpha)}, \quad \alpha \in \mathbb{F}_2^n. \quad (3)$$

If $f(x) = g(x)$, then $\triangle_f(\alpha) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus\alpha)}$.

Two n-variable Boolean functions $f(x), g(x)$ are called to be perfectly uncorrelated if $\triangle_{f,g}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$ and are called to be uncorrelated of degree k if $\triangle_{f,g}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$ such that $0 \leq wt(\alpha) \leq k$.

Definition 3 (see [9]). Let $f(x), g(x) \in \mathbb{B}_n$; the sum-of-squares indicator of the cross-correlation between $f(x)$ and $g(x)$ is defined as

$$\sigma_{f,g} = \sum_{\alpha\in\mathbb{F}_2^n} \triangle_{f,g}^2(\alpha); \tag{4}$$

the absolute indicator of the cross-correlation between $f(x)$ and $g(x)$ is defined as

$$\triangle_{f,g} = \max_{\alpha\in\mathbb{F}_2^n} \left|\triangle_{f,g}(\alpha)\right|. \tag{5}$$

The above indicators are called the global avalanche characteristics between two Boolean functions. If $f(x) = g(x)$, then

$$\begin{aligned}\sigma_f &= \sum_{\alpha\in\mathbb{F}_2^n} \triangle_f^2(\alpha),\\ \triangle_f &= \max_{\alpha\in\mathbb{F}_2^n, wt(\alpha)\neq\mathbf{0}^n} \left|\triangle_f(\alpha)\right|,\end{aligned} \tag{6}$$

and the two indicators are the global avalanche characteristics of Boolean functions (*GAC* [4]).

In order to study cross-correlation distributions between any two Boolean functions, we need the following definition.

Definition 4 (see [13]). Let $f(x), g(x) \in \mathbb{B}_n$. If $D_a(f,g) : x \longmapsto f(x) \oplus g(x \oplus a)$ is constant, a is said to be a *linear structure* of f and g. For convenience, let

$$\begin{aligned}U_{f,g}^0 &= \left\{a \in \mathbb{F}_2^n \mid f(x) \oplus g(x \oplus a) = 0,\ \forall x \in \mathbb{F}_2^n\right\};\\ U_{f,g}^1 &= \left\{a \in \mathbb{F}_2^n \mid f(x) \oplus g(x \oplus a) = 1,\ \forall x \in \mathbb{F}_2^n\right\};\end{aligned} \tag{7}$$

if $\mathbf{0}^n \in U_{f,g}$, it is easy to know that $U_{f,g}^0$ and $U_{f,g} = U_{f,g}^0 \cup U_{f,g}^1$ are linear subspaces of $\mathbb{F}_2^n$.

In Definition 4, if $f(x) = g(x)$, then $U_f^0 = \{a \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus a) = 0,\ \forall x \in \mathbb{F}_2^n\}$; $U_f^1 = \{a \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus a) = 1,\ \forall x \in \mathbb{F}_2^n\}$. U_f^0 and $U_f = U_f^0 \cup U_f^1$ are linear subspaces of $\mathbb{F}_2^n$.

In [13], the authors obtained some properties of any two Boolean functions with the same autocorrelation distribution; let $T_n(f)$ and $T_{n\times n}(f,g)$ be functions set with the same autocorrelation distribution and the cross-correlation distribution of given $f(x), g(x) \in \mathbb{B}_n$, respectively:

$$\begin{aligned}T_n(f) = \Big\{&g(x) \in \mathbb{B}_n \mid \triangle_g(\alpha_i) = \triangle_f(\alpha_i),\ \forall\alpha_i\\ &\in \mathbb{F}_2^n\ \left(0 \le i \le 2^n - 1\right),\ f(x) \in \mathbb{B}_n\Big\}.\end{aligned} \tag{8}$$

And

$$\begin{aligned}T_{n\times n}(f,g) = \Big\{&(r(x), t(x)) \in \mathbb{B}_n \times \mathbb{B}_n \mid (\triangle_{r,t}(\alpha)\\ &= \triangle_{f,g}(\alpha),\ \forall\alpha_i\\ &\in \mathbb{F}_2^n\ \left(0 \le i \le 2^n - 1\right),\ f(x), g(x) \in \mathbb{B}_n\Big\}.\end{aligned} \tag{9}$$

We denote a Boolean function $f(x) \in \mathbb{B}_n$ by $\overline{f} = f_0 \times 2^0 + f_1 \times 2^1 + \cdots + f_{2^n-1} \times (2^{2^n-1})$. For example, taking $n = 3$, the Boolean function with truth table $(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7) = (1,0,0,0,1,1,0,1)$ is written as $\overline{f} = 177$.

Denote $\mathbf{0}^n = (0,0,\ldots,0) \in \mathbb{F}_2^n$ in this paper.

3. The Upper Bound on the Sum-of-Squares between an *n*-Variables Boolean Function and (*n*−2)-Variable Decomposition Functions

In this section, we give an expression for the sum-of-squares indicator of an n-variable Boolean function. This result is important to the following sections.

In order to give the relationship of the sum-of-squares indicator between one Boolean function and four decomposition Boolean functions, we need the following Lemma 5.

Lemma 5 (see [13]). *Let $h(x), g(x) \in \mathbb{B}_n$. Then*

$$\sum_{\alpha\in\mathbb{F}_2^n} \triangle_h(\alpha)\triangle_g(\alpha) = \sum_{e\in\mathbb{F}_2^n} \triangle_{h,g}^2(e) = \sigma_{h,g}. \tag{10}$$

Lemma 5 gave a relationship between autocorrelation functions and cross-correlation functions. Reference [14] gives the relationship between the sum-of-squares indicator on an n-variable Boolean function and four decomposition $(n-2)$-variable Boolean functions in the following.

Lemma 6 (see [14]). *Let $f(x_n, x_{n-1}, x) = (x_n \oplus 1)(x_{n-1} \oplus 1)f_1(x) \oplus (x_n \oplus 1)x_{n-1}f_2(x) \oplus x_n(x_{n-1} \oplus 1)f_3(x) \oplus x_n x_{n-1} f_4(x)$; $x_n, x_{n-1} \in \mathbb{F}_2,\ x \in \mathbb{F}_2^{n-2}$. Then*

$$\begin{aligned}&\sigma_f\\ &= \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + \sigma_{f_4}\\ &\quad + 6\left[\sigma_{f_1,f_2} + \sigma_{f_3,f_4} + \sigma_{f_1,f_3} + \sigma_{f_2,f_4} + \sigma_{f_1,f_4} + \sigma_{f_2,f_3}\right]\\ &\quad + 8\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_2}(\alpha)\triangle_{f_3,f_4}(\alpha)\\ &\quad + 8\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_3}(\alpha)\triangle_{f_2,f_4}(\alpha)\\ &\quad + 8\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_4}(\alpha)\triangle_{f_2,f_3}(\alpha).\end{aligned} \tag{11}$$

Based on Lemmas 5 and 6, we have the upper bound on σ_f for any n-variable Boolean function $f(x) \in \mathbb{B}_n$.

Theorem 7. *Let $f(x_n, x_{n-1}, x) = (x_n \oplus 1)(x_{n-1} \oplus 1)f_1(x) \oplus (x_n \oplus 1)x_{n-1}f_2(x) \oplus x_n(x_{n-1} \oplus 1)f_3(x) \oplus x_n x_{n-1} f_4(x)$; $x_n, x_{n-1} \in \mathbb{F}_2,\ x \in \mathbb{F}_2^{n-2}$. Then*

$$\begin{aligned}&\sigma_f\\ &\le \sum_{1\le i\le 4} \sigma_{f_i} + 6\sum_{1\le i<j\le 4} \sigma_{f_i,f_j}\end{aligned}$$

$$+\,8\left[\sqrt{\sigma_{f_1,f_2}\sigma_{f_3,f_4}}+\sqrt{\sigma_{f_1,f_3}\sigma_{f_2,f_4}}+\sqrt{\sigma_{f_1,f_4}\sigma_{f_2,f_3}}\right], \tag{12}$$

with the equality holding if and only if $\triangle_{f_1,f_2}(\alpha)=\triangle_{f_3,f_4}(\alpha)$, $\triangle_{f_1,f_3}(\alpha)=\triangle_{f_2,f_4}(\alpha)$, *and* $\triangle_{f_1,f_4}(\alpha)=\triangle_{f_2,f_3}(\alpha)$ *for any* $\alpha\in\mathbb{F}_2^{n-2}$.

Proof. Note that, for any a_i, b_i, Cauchy inequality holds:

$$\sum_{i=1}^{n} a_i b_i \leq \left(\sum_{i=1}^{n} a_i^2\right)^{1/2}\left(\sum_{i=1}^{n} b_i^2\right)^{1/2}, \tag{13}$$

with equality holding if and only if $a_i = b_i$ for any i $(1 \leq i \leq n)$.

Thus, based on Definition 3, we have

$$\begin{aligned}
&\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_2}(\alpha)\,\triangle_{f_3,f_4}(\alpha)\\
&\quad\leq\left(\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_2}^2(\alpha)\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_3,f_4}^2(\alpha)\right)^{1/2}\\
&\quad=\sqrt{\sigma_{f_1,f_2}\sigma_{f_3,f_4}},\\
&\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_3}(\alpha)\,\triangle_{f_2,f_4}(\alpha)\\
&\quad\leq\left(\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_3}^2(\alpha)\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_2,f_4}^2(\alpha)\right)^{1/2}\\
&\quad=\sqrt{\sigma_{f_1,f_3}\sigma_{f_2,f_4}},\\
&\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_4}(\alpha)\,\triangle_{f_2,f_3}(\alpha)\\
&\quad\leq\left(\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_4}^2(\alpha)\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_2,f_3}^2(\alpha)\right)^{1/2}\\
&\quad=\sqrt{\sigma_{f_1,f_4}\sigma_{f_2,f_3}}.
\end{aligned} \tag{14}$$

This result is proven. □

Reference [15] gave the relationship between $\sigma_{f,g}$ and σ_f, σ_g for any Boolean function $f, g \in \mathbb{B}_n$.

Lemma 8 (see [15]). *Let* $f(x), g(x)\in\mathbb{B}_n$. *Then* $\sigma_{f,g}\leq\sqrt{\sigma_f\sigma_g}$; *the equality holds if and only if* $|\mathcal{F}(f\oplus\varphi_\alpha)| = |\mathcal{F}(g\oplus\varphi_\alpha)|$ *for all* $\alpha\in\mathbb{F}_2^n$ *or if and only if* $\triangle_f(\alpha)=\triangle_g(\alpha)$ *for all* $\alpha\in\mathbb{F}_2^n$.

Furthermore, according to Lemma 8 and Theorem 7, we have the following theorem.

Theorem 9. *Let* $f(x_n, x_{n-1}, x) = (x_n\oplus 1)(x_{n-1}\oplus 1)f_1(x)\oplus(x_n\oplus 1)x_{n-1}f_2(x)\oplus x_n(x_{n-1}\oplus 1)f_3(x)\oplus x_n x_{n-1}f_4(x)$; $x_n, x_{n-1}\in\mathbb{F}_2$, $x\in\mathbb{F}_2^{n-2}$. *Then*

$$\begin{aligned}
2^{2n} &\leq \sigma_f\\
&\leq \sum_{1\leq i\leq 4}\sigma_{f_i} + 6\sum_{1\leq i<j\leq 4}\sqrt{\sigma_{f_i}\sigma_{f_j}}\\
&\quad + 24\left(\sigma_{f_1}\sigma_{f_2}\sigma_{f_3}\sigma_{f_4}\right)^{1/4},
\end{aligned} \tag{15}$$

and, furthermore, we have the following:

(1) The right equality holds if and only if the two following conditions are satisfied:

(⋆) $\triangle_{f_1}(\alpha)=\triangle_{f_2}(\alpha)=\triangle_{f_3}(\alpha)=\triangle_{f_4}(\alpha)$ *for all* $\alpha\in\mathbb{F}_2^{n-2}$;

(⋆⋆) $\triangle_{f_1,f_2}(\alpha)=\triangle_{f_3,f_4}(\alpha)$, $\triangle_{f_1,f_3}(\alpha)=\triangle_{f_2,f_4}(\alpha)$, *and* $\triangle_{f_1,f_4}(\alpha)=\triangle_{f_2,f_3}(\alpha)$ *for any* $\alpha\in\mathbb{F}_2^{n-2}$.

(2) The left equality holds if and only if f is a bent function.

Remark 10. By Theorem 9, we know that $\sigma_f = \sigma_{f_1}+\sigma_{f_2}+\sigma_{f_3}+\sigma_{f_4}$ if and only if f_i and f_j $(1\leq i\neq j\leq 4)$ are perfectly uncorrelated functions. The lower bound is easy reached; it is because we can find that f_i and f_j $(1\leq i\neq j\leq 4)$ are perfectly uncorrelated functions. For example, let $f(x) = f(x_1, x_2, x_3, x_4)\in\mathbb{B}_4$ be a bent function and

$$\begin{aligned}
f_1(x, x_5, x_6, x_7, x_8) &= f(x)\oplus x_5,\\
f_2(x, x_5, x_6, x_7, x_8) &= f(x)\oplus x_6,\\
f_3(x, x_5, x_6, x_7, x_8) &= f(x)\oplus x_7,\\
f_4(x, x_5, x_6, x_7, x_8) &= f(x)\oplus x_8,
\end{aligned} \tag{16}$$

and then any two Boolean functions among f_1, f_2, f_3, f_4 are perfectly uncorrelated functions, and for every function $f_i(x)$ $(i = 1, 2, 3, 4)$ we have

$$\mathcal{F}(f_i\oplus\varphi_\alpha)=\begin{cases}0, & 240 \textit{ times};\\ \pm 2^6, & 16 \textit{ times}.\end{cases} \tag{17}$$

Thus, $\sigma_{f_i} = 2^{20}$. If $F(x, x_5, x_6, x_7, x_8, x_9, x_{10}) = (x_9\oplus 1)(x_{10}\oplus 1)f_1\oplus(x_9\oplus 1)x_{10}f_2\oplus x_9(x_{10}\oplus 1)f_3\oplus x_9x_{10}f_4$, then $\sigma_F = \sigma_{f_1}+\sigma_{f_2}+\sigma_{f_3}+\sigma_{f_4} = 4\times 2^{20} = 2^{24}$; the lower bound can be reached.

Summary 1. Theorem 9 provides theoretical support for encryption algorithm, especially for the security of lightweight dynamic cryptographic algorithms in the Internet of Things [2].

4. Some Properties of Conditions (⋆) and (⋆⋆)

Theorem 9 induces an important problem: does there exist a (f_1, f_2, f_3, f_4)-pair satisfying conditions (⋆) and (⋆⋆)? We will analyze this question. We need the following lemma.

Lemma 11. *Let* $f(x), g(x), h(x)\in\mathbb{B}_n$.

(1) For any $\alpha \in \mathbb{F}_2^n$, $\triangle_f(\alpha) = \triangle_{f,g}(\alpha)$ if and only if $f(x) = g(x)$.

(2) For any $\alpha \in \mathbb{F}_2^n$, $\triangle_f(\alpha) = \triangle_{g,h}(\alpha)$; then $g(x) = h(x)$; furthermore, $\triangle_f(\alpha) = \triangle_g(\alpha) = \triangle_h(\alpha)$ for any $\alpha \in \mathbb{F}_2^n$.

(3) For any $\alpha \in \mathbb{F}_2^n$, $\triangle_{f,g}(\alpha) = \triangle_{f,h}(\alpha)$ and $\triangle_f(\alpha) = \triangle_g(\alpha) = \triangle_h(\alpha)$; then $g(x) = h(x)$.

Proof. (1) According to the relationship between the cross-correlation function and the Walsh spectrum for $f(x), g(x) \in \mathbb{B}_n$, for any $\alpha \in \mathbb{F}_2^n$, we have

$$\triangle_{f,g}(\alpha) = \frac{1}{2^n}\sum_{\omega\in\mathbb{F}_2^n}(-1)^{\omega\cdot\alpha}\mathscr{F}(f\oplus\varphi_\omega)\mathscr{F}(g\oplus\varphi_\omega). \quad (18)$$

On one hand, since $\triangle_f(\alpha) = \triangle_{f,g}(\alpha)$ for any $\alpha \in \mathbb{F}_2^n$, if $\alpha = \mathbf{0}^n$, we have

$$\begin{aligned} 2^n &= \triangle_f(\mathbf{0}^n) = \triangle_{f,g}(\mathbf{0}^n) \\ &= \frac{1}{2^n}\sum_{\omega\in\mathbb{F}_2^n}\mathscr{F}(f\oplus\varphi_\omega)\mathscr{F}(g\oplus\varphi_\omega) \end{aligned} \quad (19)$$

Thus

$$\sum_{\omega\in\mathbb{F}_2^n}\mathscr{F}(f\oplus\varphi_\omega)\mathscr{F}(g\oplus\varphi_\omega) = 2^{2n}. \quad (20)$$

Finally, by Parseval equality and (20), we have

$$\begin{aligned} \sum_{\omega\in\mathbb{F}_2^n}\left[\mathscr{F}(f\oplus\varphi_\omega) - \mathscr{F}(g\oplus\varphi_\omega)\right]^2 &= \sum_{\omega\in\mathbb{F}_2^n}\mathscr{F}^2(f\oplus\varphi_\omega) \\ &+ \sum_{\omega\in\mathbb{F}_2^n}\mathscr{F}^2(g\oplus\varphi_\omega) \\ &= -2\sum_{\omega\in\mathbb{F}_2^n}\mathscr{F}(f\oplus\varphi_\omega)\mathscr{F}(g\oplus\varphi_\omega) \\ 0 &= 2^{2n} + 2^{2n} - 2\times 2^{2n} \end{aligned} \quad (21)$$

The above equation holds if and only if $\mathscr{F}(f\oplus\varphi_\omega) = \mathscr{F}(g\oplus\varphi_\omega)$ for any $\alpha \in \mathbb{F}_2^n$, if and only if $f(x) = g(x)$.

On the other hand, if $f(x) = g(x)$, then $\triangle_f(\alpha) = \triangle_{f,g}(\alpha)$ for any $\alpha \in \mathbb{F}_2^n$.

(2) By the same method with (1), this result can be proven.

(3) On one hand, according to $\triangle_{f,g}(\alpha) = \triangle_{f,h}(\alpha)$ for any $\alpha \in \mathbb{F}_2^n$, we have

$$\begin{aligned} 0 &= \sum_{\alpha\in\mathbb{F}_2^n}\left[\triangle_{f,g}(\alpha) - \triangle_{f,h}(\alpha)\right]^2 \\ &= \sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,g}^2(\alpha) + \sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,h}^2(\alpha) \\ &\quad - 2\sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,g}(\alpha)\triangle_{f,h}(\alpha) \\ &= \sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,g}(\alpha)\triangle_{f,g}(\alpha) + \sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,h}(\alpha)\triangle_{f,h}(\alpha) \\ &\quad - 2\sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,f}(\alpha)\triangle_{g,h}(\alpha) \\ &= \sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,f}(\alpha)\triangle_{g,g}(\alpha) + \sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,f}(\alpha)\triangle_{h,h}(\alpha) \\ &\quad - 2\sum_{\alpha\in\mathbb{F}_2^n}\triangle_{f,f}(\alpha)\triangle_{g,h}(\alpha) \\ &= \sum_{\alpha\in\mathbb{F}_2^n}\triangle_f^2(\alpha) + \sum_{\alpha\in\mathbb{F}_2^n}\triangle_f^2(\alpha) - 2\sum_{\alpha\in\mathbb{F}_2^n}\triangle_f(\alpha)\triangle_{g,h}(\alpha) \\ &= 2\left(\sigma_f - \sum_{\alpha\in\mathbb{F}_2^n}\triangle_f(\alpha)\triangle_{g,h}(\alpha)\right). \end{aligned} \quad (22)$$

On the other hand, by the same method and combining the above equality, we have

$$\begin{aligned} &\sum_{\alpha\in\mathbb{F}_2^n}\left[\triangle_{f,f}(\alpha) - \triangle_{g,h}(\alpha)\right]^2 \\ &\quad = 2\left(\sigma_f - \sum_{\alpha\in\mathbb{F}_2^n}\triangle_f(\alpha)\triangle_{g,h}(\alpha)\right) = 0, \end{aligned} \quad (23)$$

and it implies that $\triangle_f(\alpha) = \triangle_{g,h}(\alpha)$ for any $\alpha \in \mathbb{F}_2^n$. According to (2), we have $g(x) = h(x)$. □

Theorem 12. *Let $f_1(x), f_2(x), f_3(x), f_4(x) \in \mathbb{B}_{n-2}$ satisfy conditions ($\star$) and ($\star\star$); then*

$$\begin{aligned} \sigma_{f_1} &= \sigma_{f_2} = \sigma_{f_3} = \sigma_{f_4} = \sigma_{f_1,f_2} = \sigma_{f_1,f_3} = \sigma_{f_1,f_4} \\ &= \sigma_{f_2,f_3} = \sigma_{f_2,f_4} = \sigma_{f_3,f_4}. \end{aligned} \quad (24)$$

Proof. According to condition ($\star$) and Lemma 5, we have

$$\begin{aligned} \sigma_{f_1} = \sigma_{f_2} &= \sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1}(\alpha)\triangle_{f_1}(\alpha) \\ &= \sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1}(\alpha)\triangle_{f_2}(\alpha) = \sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_2}^2 = \sigma_{f_1,f_2}. \end{aligned} \quad (25)$$

Table 1: The autocorrelation value distributions of 3-variable Boolean functions [13].

	ACD	$f(x) \in \mathbb{B}_3$	LS
Class 0	(8,8,8,8,8,8,8,8)	0,255	3
Class 1	(8,8,0,0,0,0,0,0)	192,48,12,252,3,243,207,63	1
Class 2	(8,0,8,0,0,0,0,0)	160,80,10,250,5,245,175,95	1
Class 3	(8,0,0,8,0,0,0,0)	96,144,6,246,9,249,111,159	1
Class 4	(8,0,0,0,8,0,0,0)	136,68,34,238,17,221,187,119	1
Class 5	(8,0,0,0,0,8,0,0)	72,132,18,222,33,237,123,183	1
Class 6	(8,0,0,0,0,0,8,0)	40,20,130,190,65,125,235,215	1
Class 7	(8,0,0,0,0,0,0,8)	24,36,66,126,129,189,219,231	1
Class 8	(8,4,4,4,4,4,4,4)	1,2,4,8,16,32,64,128,254,253,251,247,239,223,191,127	0
Class 9	(8,4,4,4,-4,-4,-4,-4)	224,208,176,112,248,244,242,14,241,13,11,7,143,79,47,31	0
Class 10	(8,4,-4,-4,4,4,-4,-4)	200,196,140,76,236,220,50,206,49,205,35,19,179,115,59,55	0
Class 11	(8,-4,4,-4,4,-4,4,-4)	168,84,162,138,42,234,186,174,81,69,21,213,117,93,171,87	0
Class 12	(8,-4,-4,4,-4,4,4,-4)	104,148,146,134,22,214,182,158,97,73,41,233,121,109,107,151	0
Class 13	(8,-4,-4,4,4,-4,-4,4)	152,100,98,70,38,230,118,110,145,137,25,217,185,157,155,103	0
Class 14	(8,-4,4,-4,-4,4,-4,4)	88,164,82,74,26,218,122,94,161,133,37,229,181,173,91,167	0
Class 15	(8,4,-4,-4,-4,-4,4,4)	56,52,44,28,188,124,194,62,193,61,131,67,227,211,203,199	0
Class 16	(8,0,0,0,0,-8,0,0)	116,139,184,71,226,29,46,209	1
Class 17	(8,0,0,0,-8,0,0,0)	120,180,210,30,225,45,75,135	1
Class 18	(8,0,0,0,0,0,-8,0)	228,216,114,78,177,141,27,39	1
Class 19	(8,0,0,0,0,0,0,-8)	212,178,142,113,77,43,23,232	1
Class 20	(8,0,0,-8,0,0,0,0)	172,92,202,58,197,53,163,83	1
Class 21	(8,0,-8,0,0,0,0,0)	108,156,198,54,201,57,99,147	1
Class 22	(8,-8,0,0,0,0,0,0)	106,154,166,86,169,89,149,101	1
Class 23	(8,8,8,8,-8,-8,-8,-8)	240,15	3
Class 24	(8,8,-8,-8,8,8,-8,-8)	204,51	3
Class 25	(8,8,-8,-8,-8,-8,8,8)	60,195	3
Class 26	(8,-8,8,-8,8,-8,8,-8)	170,85	3
Class 27	(8,-8,8,-8,-8,8,-8,8)	90,165	3
Class 28	(8,-8,-8,8,8,-8,-8,8)	102,153	3
Class 29	(8,-8,-8,8,-8,8,8,-8)	150,105	3

By the same method, we have

$$\begin{aligned}
\sigma_{f_1} &= \sigma_{f_3} = \sigma_{f_1,f_3};\\
\sigma_{f_1} &= \sigma_{f_4} = \sigma_{f_1,f_4};\\
\sigma_{f_2} &= \sigma_{f_3} = \sigma_{f_2,f_3};\\
\sigma_{f_2} &= \sigma_{f_4} = \sigma_{f_2,f_4};\\
\sigma_{f_3} &= \sigma_{f_4} = \sigma_{f_3,f_4}.
\end{aligned} \tag{26}$$

Based on condition $(\star\star)$, we have

$$\begin{aligned}
\sigma_{f_1,f_2} &= \sigma_{f_3,f_4},\\
\sigma_{f_1,f_3} &= \sigma_{f_2,f_4},
\end{aligned} \tag{27}$$

$$\begin{aligned}
\sigma_{f_1,f_4} &= \sigma_{f_2,f_3},\\
\sigma_{f_2,f_3} &= \sigma_{f_1,f_4}.
\end{aligned} \tag{28}$$

Based on (26) and (27), we complete this proof. □

Theorem 13. *Let $f_1(x), f_2(x), f_3(x), f_4(x) \in \mathbb{B}_{n-2}$ satisfy the following conditions:*

(1) $\triangle_{f_1}(\alpha) = \triangle_{f_2}(\alpha) = \triangle_{f_3}(\alpha) = \triangle_{f_4}(\alpha)$ for any $\alpha \in \mathbb{F}_2^{n-2}$.

(2) $\triangle_{f_1,f_2}(\alpha) = \triangle_{f_3,f_4}(\alpha)$ for any $\alpha \in \mathbb{F}_2^{n-2}$.

Then $\triangle_{f_1,f_3}(\alpha) = \triangle_{f_2,f_4}(\alpha)$ and $\triangle_{f_1,f_4}(\alpha) = \triangle_{f_2,f_3}(\alpha)$ for any $\alpha \in \mathbb{F}_2^{n-2}$.

Proof. According to (27), we know that $\sigma_{f_1,f_2} = \sigma_{f_3,f_4}$. Note that we also have

$$\begin{aligned}
0 &= \sum_{\alpha\in\mathbb{F}_2^{n-2}} \left[\triangle_{f_1,f_2}(\alpha) - \triangle_{f_3,f_4}(\alpha)\right]^2\\
&= \sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle^2_{f_1,f_2}(\alpha) + \sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle^2_{f_3,f_4}(\alpha)\\
&\quad - 2\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_2}(\alpha)\triangle_{f_3,f_4}(\alpha)\\
&= \sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle_{f_1,f_2}(\alpha)\triangle_{f_1,f_2}(\alpha) - 2\sum_{\alpha\in\mathbb{F}_2^{n-2}} \triangle^2_{f_1,f_2}(\alpha)
\end{aligned}$$

Table 2: The cross-correlation value distributions of Class 22.

	CCD	$f(x)\in\mathbb{B}_3$	*LS*
Class 22-1	(0,0,8,-8,0,0,0,0)	(106,154);(86,89);(166,169);(149,101)	0
Class 22-2	(0,0,0,0,8,-8,0,0)	(106,166);(86,101);(89,149);(154,169)	0
Class 22-3	(0,0,0,0,0,0,-8,8)	(106,86);(154,89);(166,101);(169,149)	0
Class 22-4	(0,0,0,0,0,0,8,-8)	(106,169);(154,166);(86,149);(89,101)	0
Class 22-5	(0,0,0,0,-8,8,0,0)	(106,89);(154,86);(166,149);(169,101)	0
Class 22-6	(-8,8,0,0,0,0,0,0)	(106,149);(154,101);(166,89);(86,169)	1
Class 22-7	(0,0,-8,8,0,0,0,0)	(106,101);(154,149);(166,86);(169,89)	0

$$\begin{aligned}
&+\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_3,f_4}(\alpha)\triangle_{f_3,f_4}(\alpha)\\
&=\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_1}(\alpha)\triangle_{f_2,f_2}(\alpha)-2\sigma_{f_1,f_2}\\
&\quad+\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_3,f_3}(\alpha)\triangle_{f_4,f_4}(\alpha)\\
&=\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1}(\alpha)\triangle_{f_2}(\alpha)-2\sigma_{f_1,f_2}\\
&\quad+\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_3}(\alpha)\triangle_{f_4}(\alpha)=2\sigma_{f_1}-2\sigma_{f_1,f_2},
\end{aligned}\tag{29}$$

and it implies that $\sigma_{f_1}=\sigma_{f_1,f_2}$. Based on this result, we have

$$\begin{aligned}
&\sum_{\alpha\in\mathbb{F}_2^{n-2}}\left[\triangle_{f_1,f_3}(\alpha)-\triangle_{f_2,f_4}(\alpha)\right]^2\\
&=\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle^2_{f_1,f_3}(\alpha)+\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle^2_{f_2,f_4}(\alpha)\\
&\quad-2\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_3}(\alpha)\triangle_{f_2,f_4}(\alpha)\\
&=\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_3}(\alpha)\triangle_{f_1,f_3}(\alpha)\\
&\quad+\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_2,f_4}(\alpha)\triangle_{f_2,f_4}(\alpha)\\
&\quad-2\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_3}(\alpha)\triangle_{f_2,f_4}(\alpha)\\
&=\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_1}(\alpha)\triangle_{f_3,f_3}(\alpha)\\
&\quad+\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_2,f_2}(\alpha)\triangle_{f_4,f_4}(\alpha)\\
&\quad-2\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1,f_2}(\alpha)\triangle_{f_3,f_4}(\alpha)\\
&=\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_1}(\alpha)\triangle_{f_3}(\alpha)-2\sigma_{f_1,f_2}\\
&\quad+\sum_{\alpha\in\mathbb{F}_2^{n-2}}\triangle_{f_2}(\alpha)\triangle_{f_4}(\alpha)=2\sigma_{f_1}-2\sigma_{f_1,f_2}=0.
\end{aligned}\tag{30}$$

It implies that $\triangle_{f_1,f_3}(\alpha)=\triangle_{f_2,f_4}(\alpha)$ for any $\alpha\in\mathbb{F}_2^{n-2}$.

By the same method, we have $\triangle_{f_1,f_4}(\alpha)=\triangle_{f_2,f_3}(\alpha)$ for any $\alpha\in\mathbb{F}_2^{n-2}$. □

Based on Theorem 13, we have the following.

Corollary 14. *Let $f_1(x), f_2(x), f_3(x), f_4(x)\in\mathbb{B}_{n-2}$. Conditions ($\star$) and ($\star\star$) are equivalent to the following:*

(a) $\triangle_{f_1}(\alpha)=\triangle_{f_2}(\alpha)=\triangle_{f_3}(\alpha)=\triangle_{f_4}(\alpha)$ for any $\alpha\in\mathbb{F}_2^{n-2}$;

(b) $\triangle_{f_1,f_2}(\alpha)=\triangle_{f_3,f_4}(\alpha)$ for any $\alpha\in\mathbb{F}_2^{n-2}$.

Based on Theorems 9 and 13, we can give an algorithm for finding all (f_1,f_2,f_3,f_4)-pairs satisfying (a) and (b).

Algorithm 15. This algorithm has three steps.

Step 1. We should firstly obtain a set $T_n(f)$, because $T_n(f)$ is a function set with the same autocorrelation distribution. It is implied that we must calculate all autocorrelation distributions with n-variable.

For $n=3$, [13] gives all autocorrelation distributions (see Table 1); there are 30 different autocorrelation distributions, where *ACD* expresses the autocorrelation distributions.

Step 2. Calculate cross-correlation distributions between any two Boolean functions with the same autocorrelation distribution.

For $n=3$, there are 30 different distributions of Table 1. In particular, Class 22 has 8 Boolean functions (106, 154, 166, 86, 169, 89, 149, 101) with the same autocorrelation distribution $(8,-8,0,0,0,0,0,0)$. We can calculate all cross-correlation distributions in Table 2. There are 7 different cross-correlation distributions, where *CCD* expresses the cross-correlation distributions.

Step 3. Calculate the number of (f_1,f_2,f_3,f_4)-pairs satisfying (a) and (b) in Theorem 9.

Table 3: The number of (f_1, f_2, f_3, f_4) with 3-variable satisfying conditions $(\star)$ and $(\star\star)$.

	(f_1, f_2, f_3, f_4)	The number of (f_1, f_2, f_3, f_4)-pairs	Class
1	(f_1, f_1, f_1, f_1)	256	Class 0 to 29
2	$(f_1, f_1, f_2, f_2), f_1 \neq f_2$	1360	Class 0 to 29
3	$(f_1, f_2, f_3, f_4) \in A$[1]	1316	Class 1 to 22

[1] $A = \{(f_1, f_2, f_3, f_4) : f_1 \neq f_2, f_1 \neq f_3, f_1 \neq f_4, f_2 \neq f_3, f_2 \neq f_4, f_3 \neq f_4\}$.

Table 4: The cross-correlation value distributions of any two 4-variable bent functions.

Cases	*TCCV*	N	*Classes*	$\sigma_{f,g}$	$\triangle_{f,g}$
1	$[16(1), 0(15)]$	6720	15 (448)	256	16
2	$[-16(1), 0(15)]$	7168	16 (448)	256	16
3	$[8(3), -8(1), 0(12)]$	107520	560 (192)	256	8
4	$[8(1), -8(3), 0(12)]$	107520	560 (192)	256	8
5	$[4(10), -4(6)]$	86016	448 (192)	256	4

(1) *TCCV* is the times of cross-correlation value; for example, in line 1, $[16(1), 0(15)]$ implies that the cross-correlation value 16 occurs one time and the cross-correlation value 0 occurs 15 times; for example, the cross-correlation distributions $(0, 16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ and $(0, 0, 16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ all belong to $[16(1), 0(15)]$.
(2) N is the number of pairs $(f(x), g(x))$ with the same *TCCV*.
(3) *Classes* express the number of each class. For example, in line 1, 15(448) denotes that 6720 can be classified into 15 classes (each class has the same cross-correlation distribution) and each class has 448 pairs (the number of any two different bent functions which have the same cross-correlation is 448).

Remark 16. Based on Theorem 13, we analyze the upper bound on σ_f in Theorem 9; this upper bound can be reached if and only if $f_1, f_2, f_3, f_4 \in \mathbb{B}_{n-2}$ satisfying conditions (a) and (b). We must consider the existence of f_1, f_2, f_3, f_4 satisfying conditions (a) and (b).

(1) Suppose that $f_1 = f_2 = f_3 = f_4$. Then conditions (a) and (b) hold.

(2) Suppose that $f_1 = f_2 = f_3 \neq f_4$. According to $\triangle_{f_1,f_2}(\alpha) = \triangle_{f_3,f_4}(\alpha)$, for any $\alpha \in \mathbb{F}_2^n$, we have $\triangle_{f_3}(\alpha) = \triangle_{f_3,f_4}(\alpha)$, for any $\alpha \in \mathbb{F}_2^n$; we know that $f_3 = f_4$. Thus, this supposition cannot be reached.

(3) Suppose that $f_1 = f_2 \neq f_3 = f_4$. Conditions (a) and (b) are equivalent to $\triangle_{f_1}(\alpha) = \triangle_{f_2}(\alpha)$ for any $\alpha \in \mathbb{F}_2^n$; obviously this holds.

(4) Suppose that f_1, f_2, f_3, f_4 are unequal to each other. We can find these (f_1, f_2, f_3, f_4)-pairs satisfying (a) and (b).

For $n = 3$, we give all Boolean functions satisfying conditions (a) and (b) in Example 17.

Example 17. (1) When $n = 3$, for *Class* 22, we will give all Boolean functions satisfying conditions (1), (2), and (4) of Remark 10 in Table 2; it implies that there are 4 pairs of Boolean functions with the same cross-correlation distribution.

(2) In Table 2, the number of Boolean functions satisfying condition (4) is 14. The number of Boolean functions satisfying condition (2) is $\binom{8}{2} = 28$. The number of Boolean functions satisfying condition (1) is $\binom{8}{1} = 8$. Thus, we find 50 (=14+28+8) Boolean functions with 3-variable satisfying (a) and (b); based on the 50 Boolean functions, we can construct 50 5-variable Boolean functions reaching the upper bound in Theorem 9 in Class 22.

(3) The rest of results from Class 0 to Class 29 can be found in Appendix (Tables 6, 7, 8, 9, 10, and 11).

Thus, we find 2932(= 256 + 1360 + 1316) Boolean functions (f_1, f_2, f_3, f_4) satisfying conditions (a) and (b) in all 3-variable Boolean functions in Table 3. By the same method, we also find many Boolean function pairs for $n \geq 4$.

Summary 2. Theorem 13 gives a theoretical result for finding Boolean functions with the same autocorrelation (or cross-correlation) distributions, but Algorithm 15 gives a specific implementation method for lightweight cryptographic decompositions in the Internet of Things [1]. According to Algorithm 15, we can find many Boolean functions with the same *GAC* and the same resistance to attacks.

5. Construction n-Variable Boolean Functions with Lower σ_f by Disjoint Spectrum Functions

Zhang and Zheng [4] showed that the smaller σ_f, the better the *GAC* of a function $f(x) \in \mathbb{B}_n$. In Lemma 6 and Theorem 9, we know that

$$\sigma_f = \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + \sigma_{f_4} + 6 \sum_{1 \leq i < j \leq 4} \sigma_{f_i,f_j} + 24 \sum_{\alpha \in \mathbb{F}_2^{n-2}} \triangle_{f_1,f_2}(\alpha) \triangle_{f_3,f_4}(\alpha) [14] . \quad (31)$$

Thus, if four decomposition functions f_1, f_2, f_3, f_4 satisfy the conditions,

(1) $\sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + \sigma_{f_4}$ is small;

(2) f_1, f_2, f_3, and f_4 are perfectly uncorrelated,

then f has lower σ_f. It implies that (1) and (2) are important for constructing a good Boolean function f with lower σ_f by the decomposition Boolean functions.

Table 5: Comparison among balanced Boolean functions.

Constructions	n even	N_f	$\triangle_f$	σ_f
[3]	$n \geq 8$	$2^{n-1} - 2^{n/2}$	2^n	2^{2n+2}
[19]	$n \geq 4$	2^{n-2}	2^n	2^{3n-2}
[19]	$n \geq 8$	$2^{n-1} - 2^{n/2}$	2^n	2^{2n+2}
[20]	$n \geq 8$	$2^{n-1} - 2^{n/2}$	–	2^{2n+2}
Theorem 20	$n \geq 6$	$2^{n-1} - 2^{n/2}$	2^n	$5 \cdot 2^{2n-1}$

Table 6: The cross-correlation value distributions of Class 0 and from Class 23 to 29.

	CCD	$f(x) \in \mathbb{B}_3$	*LS*
Class 0	(-8,-8,-8,-8,-8,-8,-8,-8)	(0,255)	3
Class 23	(-8,-8,-8,-8,8,8,8,8)	(240,15)	3
Class 24	(-8,-8,8,8,-8,-8,8,8)	(204,51)	3
Class 25	(-8,-8,8,8,8,8,-8,-8)	(60,195)	3
Class 26	(-8,8,-8,8,-8,8,-8,8)	(170,85)	3
Class 27	(-8,8,-8,8,8,-8,8,-8)	(90,165)	3
Class 28	(-8,8,8,-8,-8,8,8,-8)	(102,153)	3
Class 29	(-8,8,8,-8,8,-8,-8,8)	(150,105)	3

Theorem 9 implies that $\sigma_f = \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + \sigma_{f_4}$, if any two Boolean functions among f_1, f_2, f_3, and f_4 are perfectly uncorrelated.

Sarkar and Maitra [16] obtained the characterization of perfect uncorrelated.

Lemma 18 (see [16]). *Let $f(x), g(x) \in \mathbb{B}_n$. Then $f(x)$ and $g(x)$ are perfectly uncorrelated if and only if $\mathscr{F}(f \oplus \varphi_\alpha)\mathscr{F}(g \oplus \varphi_\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^n$.*

Disjoint spectra functions have good properties; here we first give a brief summary of pervious results related to the disjoint spectra functions.

(1) Two Boolean functions with disjoint spectra can be used to construct highly nonlinear resilient functions as clearly mentioned in [17].

(2) In 2009, [12] constructed almost optimal resilient functions with even large variables by disjoint spectra functions.

(3) Reference [4] implied $2^{2n} \leq \sigma_f \leq 2^{3n}$ for a Boolean function $f(x) \in \mathbb{B}_n$; $\sigma_f = 2^{2n}$ if and only if $f(x)$ is a Bent function. In order to construct a Boolean function with lower sum-of-squares indicator; therefore [15] constructed a Boolean function $f(x) \in \mathbb{B}_n$ with lower σ_f based on modifying Bent functions and disjoint spectra functions.

Although many authors give constructions with some cryptology properties based on disjoint spectra functions, how to construct disjoint spectra functions which are not (linearly equivalent to) partially linear functions is an open problem [12, 18].

Note that bent functions have minimum sum-of-squares indicator, but any two Bent functions $f(x), g(x) \in \mathbb{B}_n$ are not disjoint spectra functions or perfect uncorrelated. It is because that $|\mathscr{F}(f \oplus \varphi_\alpha)\mathscr{F}(g \oplus \varphi_\alpha)| = 2^n$ for any $\alpha \in \mathbb{F}_2^n$. Thus, $\sigma_{f,g} = 2^{2n}$ and $\#\{\alpha \in \mathbb{F}_2^n : \triangle_{f,g}(\alpha) = 0\} \leq 15$. That is, we cannot construct an n-variable Boolean function by $(n-2)$-variable disjoint spectra bent functions.

In order to construct an n-variable Boolean function $f(x) \in \mathbb{B}_n$ with small σ_f by $(n-2)$-variable bent functions, we give a definition of two pairs of Boolean functions.

Definition 19. Two pairs of n-variable Boolean functions $(f_1(x), f_2(x)), (f_3(x), f_4(x))$ are called to be perfectly uncorrelated if $\triangle_{f_1,f_2}(\alpha)\triangle_{f_3,f_4}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$ and are called to be uncorrelated of degree k if $\triangle_{f_1,f_2}(\alpha)\triangle_{f_3,f_4}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$ such that $0 \leq wt(\alpha) \leq k$.

Theorem 20. *Let $f(x_n, x_{n-1}, x) = (x_n \oplus 1)(x_{n-1} \oplus 1) f_1(x) \oplus (x_n \oplus 1)x_{n-1} f_2(x) \oplus x_n(x_{n-1} \oplus 1) f_3(x) \oplus x_n x_{n-1} f_4(x)$; $x_n, x_{n-1} \in \mathbb{F}_2$, $x \in \mathbb{F}_2^{n-2}$. If two pairs of $(n-2)$-variable Bent functions $(f_1(x), f_2(x)), (f_3(x), f_4(x))$ are perfectly uncorrelated, then $\sigma_f = 5 \cdot 2^{2n-1}$.*

Proof. According to the above analysis, we know that any two bent functions f_i, f_j $(1 \leq i \neq j \leq 4)$ satisfy $\sigma_{f_i,f_j} = 2^{2(n-2)}$; thus, we have

$$\begin{aligned}\sigma_f &= \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + \sigma_{f_4} + 6 \sum_{1 \leq i < j \leq 4} \sigma_{f_i,f_j} \\ &\quad + 24 \sum_{\alpha \in \mathbb{F}_2^{n-2}} \triangle_{f_1,f_2}(\alpha)\triangle_{f_3,f_4}(\alpha) \\ &= 40 \cdot 2^{2(n-2)} + 24 \sum_{\alpha \in \mathbb{F}_2^{n-2}} \triangle_{f_1,f_2}(\alpha)\triangle_{f_3,f_4}(\alpha) \\ &= 40 \cdot 2^{2(n-2)} = 5 \cdot 2^{2n-1}.\end{aligned} \tag{32}$$

□

Table 7: The cross-correlation value distributions from Class 1 to Class 7.

	CCD	$f(x) \in \mathbb{B}_3$	*LS*
Class 1-1	(0,0,8,8,0,0,0,0)	(192,48);(252,243);(207,63);(12,3)	0
Class 1-2	(0,0,0,0,8,8,0,0)	(192,12);(48,3);(252,207);(243,63)	0
Class 1-3	(0,0,0,0,0,0,-8,-8)	(192,252);(48,243);(12,207);(3,63)	0
Class 1-4	(0,0,0,0,0,0,8,8)	(192,3);(48,12);(252,63);(243,207)	0
Class 1-5	(0,0,0,0,-8,-8,0,0)	(192,243);(48,252);(12,63);(3,207)	0
Class 1-6	(0,0,-8,-8,0,0,0,0)	(192,207);(48,63);(12,252);(3,243)	0
Class 1-7	(-8,-8,0,0,0,0,0,0)	(192,63);(48,207);(12,243);(252,3)	1
Class 2-1	(0,8,0,8,0,0,0,0)	(160,80);(10,5);(250,245);(175,95)	0
Class 2-2	(0,0,0,0,8,0,8,0)	(160,10);(80,5);(250,175);(245,95)	0
Class 2-3	(0,0,0,0,0,-8,0,-8)	(160,250);(80,245);(10,175);(5,95)	0
Class 2-4	(0,0,0,0,0,8,0,8)	(160,5);(80,10);(250,95);(245,175)	0
Class 2-5	(0,0,0,0,-8,0,-8,0)	(160,245);(80,250);(10,95);(5,175)	0
Class 2-6	(0,-8,0,-8,0,0,0,0)	(160,175);(80,95);(10,250);(5,245)	0
Class 2-7	(-8,0,-8,0,0,0,0,0)	(160,95);(80,175);(10,245);(250,5)	1
Class 3-1	(0,8,8,0,0,0,0,0)	(96,144);(6,9);(246,249);(111,159)	0
Class 3-2	(0,0,0,0,8,0,0,8)	(96,6);(144,9);(246,111);(249,159)	0
Class 3-3	(0,0,0,0,0,-8,-8,0)	(96,246);(144,249);(6,111);(9,159)	0
Class 3-4	(0,0,0,0,0,8,8,0)	(96,9);(144,6); (246,159);(249,111)	0
Class 3-5	(0,0,0,0,-8,0,0,-8)	(96,249);(144,246);(6,159);(9,111)	0
Class 3-6	(0,-8,-8,0,0,0,0,0)	(96,111);(144,159);(6,246);(9,249)	0
Class 3-7	(-8,0,0,-8,0,0,0,0)	(96,159);(144,111);(6,249);(246,9)	1
Class 4-1	(0,8,0,0,0,8,0,0)	(136,68);(34,17);(238,221);(187,119)	0
Class 4-2	(0,0,8,0,0,0,8,0)	(136,34);(68,17);(238,187);(221,119)	0
Class 4-3	(0,0,0,-8,0,0,0,-8)	(136,238);(68,221);(34,187);(17,119)	0
Class 4-4	(0,0,0,8,0,0,0,8)	(136,17);(68,34);(238,119);(221,187)	0
Class 4-5	(0,0,-8,0,0,0,-8,0)	(136,221);(68,238);(34,119);(17,187)	0
Class 4-6	(0,-8,0,0,0,-8,0,0)	(136,187);(68,119);(34,238);(17,221)	0
Class 4-7	(-8,0,0,0,-8,0,0,0)	(136,119);(68,187);(34,221);(238,17)	1
Class 5-1	(0,8,0,0,8,0,0,0)	(72,132);(18,33);(222,237);(123,183)	0
Class 5-2	(0,0,8,0,0,0,0,8)	(72,18);(132,33);(222,123);(237,183)	0
Class 5-3	(0,0,0,-8,0,0,-8,0)	(72,222);(132,237);(18,123);(33,183)	0
Class 5-4	(0,0,0,8,0,0,8,0)	(72,33);(132,18);(222,183);(237,123)	0
Class 5-5	(0,0,-8,0,0,0,0,-8)	(72,237);(132,222);(18,183);(33,123)	0
Class 5-6	(0,-8,0,0,-8,0,0,0)	(72,123);(132,183);(18,222);(33,237)	0
Class 5-7	(-8,0,0,0,0,-8,0,0)	(72,183);(132,123);(18,237);(222,33)	1
Class 6-1	(0,8,0,0,0,0,0,8)	(40,20);(130,65);(190,125);(235,215)	0
Class 6-2	(0,0,8,0,8,0,0,0)	(40,130);(20,65);(190,235);(125,215)	0
Class 6-3	(0,0,0,-8,0,-8,0,0)	(40,190);(20,125);(130,235);(65,215)	0
Class 6-4	(0,0,0,8,0,8,0,0)	(40,65);(20,130);(190,215);(125,235)	0
Class 6-5	(0,0,-8,0,-8,0,0,0)	(40,125);(20,190);(130,215);(65,235)	0
Class 6-6	(0,-8,0,0,0,0,0,-8)	(40,235);(130,190);(20,215);(65,125)	0
Class 6-7	(-8,0,0,0,0,0,-8,0)	(40,215);(20,235);(130,125);(190,65)	1
Class 7-1	(0,8,0,0,0,0,8,0)	(24,36);(66,129);(126,189);(219,231)	0
Class 7-2	(0,0,8,0,0,8,0,0)	(24,66);(36,129);(126,219);(189,231)	0
Class 7-3	(0,0,0,-8,-8,0,0,0)	(24,126);(66,219);(36,189);(129,231)	0
Class 7-4	(0,0,0,8,8,0,0,0)	(24,129);(36,66);(126,231);(189,219)	0
Class 7-5	(0,0,-8,0,0,-8,0,0)	(24,189);(66,231);(36,126);(129,219)	0
Class 7-6	(0,-8,0,0,0,0,-8,0)	(24,219);(36,231);(66,126);(129,189)	0
Class 7-7	(-8,0,0,0,0,0,0,-8)	(24,231);(36,219);(66,189);(126,129)	1

Table 8: The cross-correlation value distributions from Class 8 to Class 10.

	CCD	$f(x) \in \mathbb{B}_3$	*LS*
Class 8-1	(4,8,4,4,4,4,4,4)	(1,2);(4,8);(16,32);(64,128);(254,253);(251,247);(239,223);(191,127)	0
Class 8-2	(4,4,8,4,4,4,4,4)	(1,4);(2,8);(16,64);(32,128);(254,251);(253,247);(239,191);(223,127)	0
Class 8-3	(4,4,4,8,4,4,4,4)	(1,8);(2,4);(16,128);(32,64);(254,247);(253,251);(239,127);(223,191)	0
Class 8-4	(4,4,4,4,8,4,4,4)	(1,16);(2,32);(4,64);(8,128);(254,239);(253,223);(251,191);(247,127)	0
Class 8-5	(4,4,4,4,4,8,4,4)	(1,32);(2,16);(4,128);(8,64);(254,223);(253,239);(251,127);(247,191)	0
Class 8-6	(4,4,4,4,4,4,8,4)	(1,64);(2,128);(4,16);(8,32);(254,191);(253,127);(251,239);(247,223)	0
Class 8-7	(4,4,4,4,4,4,4,8)	(1,128);(2,64);(4,32);(8,16);(254,127);(253,191);(251,223);(247,239)	0
Class 8-8	(-8,-4,-4,-4,-4,-4,-4,-4)	(1,254);(2,253);(4,251);(8,247);(16,239);(32,223);(64,191);(128,127)	0
Class 8-9	(-4,-8,-4,-4,-4,-4,-4,-4)	(1,253);(2,254);(4,247);(8,251);(16,223);(32,239);(64,127);(128,191)	0
Class 8-10	(-4,-4,-8,-4,-4,-4,-4,-4)	(1,251);(2,247);(4,254);(8,253);(16,191);(32,127);(64,239);(128,223)	0
Class 8-11	(-4,-4,-4,-8,-4,-4,-4,-4)	(1,247);(2,251);(4,253);(8,254);(16,127);(32,191);(64,223);(128,239)	0
Class 8-12	(-4,-4,-4,-4,-8,-4,-4,-4)	(1,239);(2,223);(4,191);(8,127);(16,254);(32,253);(64,251);(128,247)	0
Class 8-13	(-4,-4,-4,-4,-4,-8,-4,-4)	(1,223);(2,239);(4,127);(8,191);(16,253);(32,254);(64,247);(128,251)	0
Class 8-14	(-4,-4,-4,-4,-4,-4,-8,-4)	(1,191);(2,127);(4,239);(8,223);(16,251);(32,247);(64,254);(128,253)	0
Class 8-15	(-4,-4,-4,-4,-4,-4,-4,-8)	(1,127);(2,191);(4,223);(8,239);(16,247);(32,251);(64,253);(128,254)	0
Class 9-1	(4,8,4,4,-4,-4,-4,-4)	(224,208);(176,112);(248,244);(242,241);(14,13);(11,7);(143,79);(47,31)	0
Class 9-2	(4,4,8,4,-4,-4,-4,-4)	(224,176);(208,112);(248,242);(244,241);(14,11);(13,7);(143,47);(79,31)	0
Class 9-3	(4,4,4,8,-4,-4,-4,-4)	(224,112);(208,176);(248,241);(244,242);(14,7);(13,11);(143,31);(79,47)	0
Class 9-4	(4,4,4,4,-4,-4,-4,-8)	(224,248);(208,244);(176,242);(112,241);(14,143);(13,79);(11,47);(7,31)	0
Class 9-5	(4,4,4,4,-4,-4,-8,-4)	(224,244);(208,248);(176,241);(112,242);(14,79);(13,143);(11,31);(7,47)	0
Class 9-6	(4,4,4,4,-4,-8,-4,-4)	(224,242);(208,241);(176,248);(112,244);(14,47);(13,31);(11,143);(7,79)	0
Class 9-7	(-4,-4,-4,-4,8,4,4,4)	(224,14);(208,13);(176,11);(112,7);(248,143);(244,79);(242,47);(241,31)	0
Class 9-8	(4,4,4,4,-8,-4,-4,-4)	(224,241);(208,242);(176,244);(112,248);(14,31);(13,47);(11,79);(7,143)	0
Class 9-9	(-4,-4,-4,-4,4,8,4,4)	(224,13);(208,14);(176,7);(112,11);(248,79);(244,143);(242,31);(241,47)	0
Class 9-10	(-4,-4,-4,-4,4,4,8,4)	(224,11);(208,7);(176,14);(112,13);(248,47);(244,31);(242,143);(241,79)	0
Class 9-11	(-4,-4,-4,-4,4,4,4,8)	(224,7);(208,11);(176,13);(112,14);(248,31);(244,47);(242,79);(241,143)	0
Class 9-12	(-4,-4,-4,-8,4,4,4,4)	(224,143);(208,79);(176,47);(112,31);(248,14);(244,13);(242,11);(241,7)	0
Class 9-13	(-4,-4,-8,-4,4,4,4,4)	(224,79);(208,143);(176,31);(112,47);(248,13);(244,14);(242,7);(241,11)	0
Class 9-14	(-4,-8,-4,-4,4,4,4,4)	(224,47);(208,31);(176,143);(112,79);(248,11);(244,7);(242,14);(241,13)	0
Class 9-15	(-8,-4,-4,-4,4,4,4,4)	(224,31);(208,47);(176,79);(112,143);(248,7);(244,11);(242,13);(14,241)	0
Class 10-1	(4,8,-4,-4,4,4,-4,-4)	(200,196);(140,76);(236,220);(50,49);(206,205);(35,19);(179,115);(59,55)	0
Class 10-2	(4,4,-4,-4,8,4,-4,-4)	(200,140);(196,76);(236,206);(220,205);(50,35);(49,19);(179,59);(115,55)	0
Class 10-3	(-4,-4,4,8,-4,-4,4,4)	(200,49);(196,50);(140,19);(76,35);(236,115);(220,179);(206,55);(205,59)	0
Class 10-4	(4,4,-8,-4,4,4,-4,-4)	(200,205);(196,206);(140,220);(76,236);(50,55);(49,59);(35,115);(19,179)	0
Class 10-5	(-4,-4,4,4,-4,-4,8,4)	(200,35);(196,19);(140,50);(76,49);(236,59);(220,55);(206,179);(205,115)	0
Class 10-6	(-4,-4,4,4,-4,-4,4,8)	(200,19);(196,35);(140,49);(76,50);(236,55);(220,59);(206,115);(205,179)	0
Class 10-7	(-4,-4,4,4,-4,-8,4,4)	(200,179);(196,115);(140,59);(76,55);(236,50);(220,49);(206,35);(205,19)	0
Class 10-8	(-4,-4,4,4,-8,-4,4,4)	(200,115);(196,179);(140,55);(76,59);(236,49);(220,50);(206,19);(205,35)	0
Class 10-9	(-4,-8,4,4,-4,-4,4,4)	(200,59);(196,55);(140,179);(76,115);(236,35);(220,19);(50,206);(49,205)	0
Class 10-10	(-8,-4,4,4,-4,-4,4,4)	(200,55);(196,59);(140,115);(76,179);(236,19);(220,35);(50,205);(206,49)	0
Class 10-11	(4,4,-4,-4,4,8,-4,-4)	(200,76);(196,140);(236,205);(220,206);(50,19);(49,35);(179,55);(115,59)	0
Class 10-12	(4,4,-4,-4,4,4,-4,-8)	(200,236);(196,220);(140,206);(76,205);(50,179);(49,115);(35,59);(19,55)	0
Class 10-13	(4,4,-4,-4,4,4,-8,-4)	(200,220);(196,236);(140,205);(76,206);(50,115);(49,179);(35,55);(19,59)	0
Class 10-14	(-4,-4,8,4,-4,-4,4,4)	(200,50);(196,49);(140,35);(76,19);(236,179);(220,115);(206,59);(205,55)	0
Class 10-15	(4,4,-4,-8,4,4,-4,-4)	(200,206);(196,205);(140,236);(76,220);(50,59);(49,55);(35,179);(19,115)	0

Table 9: The cross-correlation value distributions from Class 11 to Class 13.

	CCD	$f(x) \in \mathbb{B}_3$	*LS*
Class 11-1	(-4,8,-4,4,-4,4,-4,4)	(168,84);(162,81);(138,69);(42,21);(234,213);(186,117);(174,93);(171,87)	0
Class 11-2	(4,-4,8,-4,4,-4,4,-4)	(168,162);(84,81);(138,42);(234,186);(174,171);(69,21);(213,117);(93,87)	0
Class 11-3	(4,-4,4,-4,8,-4,4,-4)	(168,138);(84,69);(162,42);(234,174);(186,171);(81,21);(213,93);(117,87)	0
Class 11-4	(4,-4,4,-4,4,-4,8,-4)	(168,42);(84,21);(162,138);(234,171);(186,174);(81,69);(213,87);(117,93)	0
Class 11-5	(4,-4,4,-4,4,-4,4,-8)	(168,234);(84,213);(162,186);(138,174);(42,171);(81,117);(69,93);(21,87)	0
Class 11-6	(4,-4,4,-4,4,-8,4,-4)	(168,186);(84,117);(162,234);(138,171);(42,174);(81,213);(69,87);(21,93)	0
Class 11-7	(4,-4,4,-8,4,-4,4,-4)	(168,174);(84,93);(162,171);(138,234);(42,186);(81,87);(69,213);(21,117)	0
Class 11-8	(-4,4,-4,8,-4,4,-4,4)	(168,81);(84,162);(138,21);(42,69);(234,117);(186,213);(174,87);(93,171)	0
Class 11-9	(-4,4,-4,4,-4,8,-4,4)	(168,69);(84,138);(162,21);(42,81);(234,93);(186,87);(174,213);(117,171)	0
Class 11-10	(-4,4,-4,4,-4,4,-4,8)	(168,21);(84,42);(162,69);(138,81);(234,87);(186,93);(174,117);(213,171)	0
Class 11-11	(-4,4,-4,4,-4,4,-8,4)	(168,213);(84,234);(162,117);(138,93);(42,87);(186,81);(174,69);(21,171)	0
Class 11-12	(-4,4,-4,4,-8,4,-4,4)	(168,117);(84,186);(162,213);(138,87);(42,93);(234,81);(174,21);(69,171)	0
Class 11-13	(-4,4,-8,4,-4,4,-4,4)	(168,93);(84,174);(162,87);(138,213);(42,117);(234,69);(186,21);(81,171)	0
Class 11-14	(4,-8,4,-4,4,-4,4,-4)	(168,171);(84,87);(162,174);(138,186);(42,234);(81,93);(69,117);(21,213)	0
Class 11-15	(-8,4,-4,4,-4,4,-4,5)	(168,87);(84,171);(162,93);(138,117);(42,213);(234,21);(186,69);(174,81)	0
Class 12-1	(-4,8,4,-4,4,-4,-4,4)	(104,148);(146,97);(134,73);(22,41);(214,233);(182,121);(158,109);(107,151)	0
Class 12-2	(-4,4,8,-4,4,-4,-4,4)	(104,146);(148,97);(134,41);(22,73);(214,121);(182,233);(158,107);(109,151)	0
Class 12-3	(-4,4,4,-4,8,-4,-4,4)	(104,134);(148,73);(146,41);(22,97);(214,109);(182,107);(158,233);(121,151)	0
Class 12-4	(-4,4,4,-4,4,-4,-4,8)	(104,22);(148,41);(146,73);(134,97);(214,107);(182,109);(158,121);(233,151)	0
Class 12-5	(-4,4,4,-4,4,-4,-8,4)	(104,214);(148,233);(146,121);(134,109);(22,107);(182,97);(158,73);(41,151)	0
Class 12-6	(-4,4,4,-4,4,-8,-4,4)	(104,182);(148,121);(146,233);(134,107);(22,109);(214,97);(158,41);(73,151)	0
Class 12-7	(-4,4,4,-8,4,-4,-4,4)	(104,158);(148,109);(146,107);(134,233);(22,121);(214,73);(182,41);(97,151)	0
Class 12-8	(4,-4,-4,8,-4,4,4,-4)	(104,97);(148,146);(134,22);(214,182);(158,151);(73,41);(233,121);(109,107)	0
Class 12-9	(4,-4,-4,4,-4,8,4,-4)	(104,73);(148,134);(146,22);(214,158);(182,151);(97,41);(233,109);(121,107)	0
Class 12-10	(4,-4,-4,4,-4,4,8,-4)	(104,41);(148,22);(146,134);(214,151);(182,158);(97,73);(233,107);(121,109)	0
Class 12-11	(4,-4,-4,4,-4,4,4,-8)	(104,233);(148,214);(146,182);(134,158);(22,151);(97,121);(73,109);(41,107)	0
Class 12-12	(4,-4,-4,4,-8,4,4,-4)	(104,121);(148,182);(146,214);(134,151);(22,158);(97,233);(73,107);(41,109)	0
Class 12-13	(4,-4,-8,4,-4,4,4,-4)	(104,109);(148,158);(146,151);(134,214);(22,182);(97,107);(73,233);(41,121)	0
Class 12-14	(4,-8,-4,4,-4,4,4,-4)	(104,107);(148,151);(146,158);(134,182);(22,214);(97,109);(73,121);(41,233)	0
Class 12-15	(-8,4,4,-4,4,-4,-4,4)	(104,151);(148,107);(146,109);(134,121);(22,233);(214,41);(182,73);(158,97)	0
Class 13-1	(-4,8,4,-4,-4,4,4,-4)	(152,100);(98,145);(70,137);(38,25);(230,217);(118,185);(110,157);(155,103)	0
Class 13-2	(-4,4,8,-4,-4,4,4,-4)	(152,98);(100,145);(70,25);(38,137);(230,185);(118,217);(110,155);(157,103)	0
Class 13-3	(-4,4,4,-4,-4,8,4,-4)	(152,70);(100,137);(98,25);(38,145);(230,157);(118,155);(110,217);(185,103)	0
Class 13-4	(-4,4,4,-4,-4,4,4,-8)	(152,230);(100,217);(98,185);(70,157);(38,155);(118,145);(110,137);(25,103)	0
Class 13-5	(-4,4,4,-4,-8,4,4,-4)	(152,118);(100,185);(98,217);(70,155);(38,157);(230,145);(110,25);(137,103)	0
Class 13-6	(-4,4,4,-4,-4,4,8,-4)	(152,38);(100,25);(98,137);(70,145);(230,155);(118,157);(110,185);(217,103)	0
Class 13-7	(-4,4,4,-8,-4,4,4,-4)	(152,110);(100,157);(98,155);(70,217);(38,185);(230,137);(118,25);(145,103)	0
Class 13-8	(4,-4,-4,8,4,-4,-4,4)	(152,145);(100,98);(70,38);(230,118);(110,103);(137,25);(217,185);(157,155)	0
Class 13-9	(4,-4,-4,4,8,-4,-4,4)	(152,137);(100,70);(98,38);(230,110);(118,103);(145,25);(217,157);(185,155)	0
Class 13-10	(4,-4,-4,4,4,-4,-4,8)	(152,25);(100,38);(98,70);(230,103);(118,110);(145,137);(217,155);(185,157)	0
Class 13-11	(4,-4,-4,4,4,-4,-8,4)	(152,217);(100,230);(98,118);(70,110);(38,103);(145,185);(137,157);(25,155)	0
Class 13-12	(4,-4,-4,4,4,-8,-4,4)	(152,185);(100,118);(98,230);(70,103);(38,110);(145,217);(137,155);(25,157)	0
Class 13-13	(4,-4,-8,4,4,-4,-4,4)	(152,157);(100,110);(98,103);(70,230);(38,118);(145,155);(137,217);(25,185)	0
Class 13-14	(4,-8,-4,4,4,-4,-4,4)	(152,155);(100,103);(98,110);(70,118);(38,230);(145,157);(137,185);(25,217)	0
Class 13-15	(-8,4,4,-4,-4,4,4,-4)	(152,103);(100,155);(98,157);(70,185);(38,217);(230,25);(118,137);(110,145)	0

Table 10: The cross-correlation value distributions from Class 14 to Class 15.

	CCD	$f(x) \in \mathbb{B}_3$	*LS*
Class 14-1	(-4,8,-4,4,4,-4,4,-4)	(88,164);(82,161);(74,133);(26,37);(218,229);(122,181);(94,173);(91,167)	0
Class 14-2	(4,-4,8,-4,-4,4,-4,4)	(88,82);(164,161);(74,26);(218,122);(94,91);(133,37);(229,181);(173,167)	0
Class 14-3	(4,-4,4,-4,-4,8,-4,4)	(88,74);(164,133);(82,26);(218,94);(122,91);(161,37);(229,173);(181,167)	0
Class 14-4	(4,-4,4,-4,-4,4,-4,8)	(88,26);(164,37);(82,74);(218,91);(122,94);(161,133);(229,167);(181,173)	0
Class 14-5	(4,-4,4,-4,-4,4,-8,4)	(88,218);(164,229);(82,122);(74,94);(26,91);(161,181);(133,173);(37,167)	0
Class 14-6	(4,-4,4,-4,-8,4,-4,4)	(88,122);(164,181);(82,218);(74,91);(26,94);(161,229);(133,167);(37,173)	0
Class 14-7	(4,-4,4,-8,-4,4,-4,4)	(88,94);(164,173);(82,91);(74,218);(26,122);(161,167);(133,229);(37,181)	0
Class 14-8	(-4,4,-4,8,4,-4,4,-4)	(88,161);(164,82);(74,37);(26,133);(218,181);(122,229);(94,167);(173,91)	0
Class 14-9	(-4,4,-4,4,8,-4,4,-4)	(88,133);(164,74);(82,37);(26,161);(218,173);(122,167);(94,229);(181,91)	0
Class 14-10	(-4,4,-4,4,4,-4,8,-4)	(88,37);(164,26);(82,133);(74,161);(218,167);(122,173);(94,181);(229,91)	0
Class 14-11	(-4,4,-4,4,4,-4,4,-8)	(88,229);(164,218);(82,181);(74,173);(26,167);(122,161);(94,133);(37,91)	0
Class 14-12	(-4,4,-4,4,4,-8,4,-4)	(88,181);(164,122);(82,229);(74,167);(26,173);(218,161);(94,37);(133,91)	0
Class 14-13	(-4,4,-8,4,4,-4,4,-4)	(88,173);(164,94);(82,167);(74,229);(26,181);(218,133);(122,37);(161,91)	0
Class 14-14	(4,-8,4,-4,-4,4,-4,4)	(88,91);(164,167);(82,94);(74,122);(26,218);(161,173);(133,181);(37,229)	0
Class 14-15	(-8,4,-4,4,4,-4,4,-4)	(88,167);(164,91);(82,173);(74,181);(26,229);(218,37);(122,133);(94,161)	0
Class 15-1	(4,8,-4,-4,-4,-4,4,4)	(56,52);(44,28),(188,124);(194,193);(62,61);(131,67);(203,199);(227,211)	0
Class 15-2	(4,4,-4,-4,-4,-4,8,4)	(56,44);(52,28);(188,62);(124,61);(194,131);(193,67);(227,203);(211,199)	0
Class 15-3	(4,4,-4,-4,-4,-4,4,8)	(56,28);(52,44);(188,61);(124,62);(194,67);(193,131);(227,199);(211,203)	0
Class 15-4	(4,4,-4,-4,-4,-8,4,4)	(56,188);(52,124);(44,62);(28,61);(194,227);(193,211);(131,203);(67,199)	0
Class 15-5	(4,4,-4,-4,-8,-4,4,4)	(56,124);(52,188);(44,61);(28,62);(194,211);(193,227);(131,199);(67,203)	0
Class 15-6	(-4,-4,8,4,4,4,-4,-4)	(56,194);(52,193);(44,131);(28,67);(188,227);(124,211);(62,203);(61,199)	0
Class 15-7	(4,4,-4,-8,-4,-4,4,4)	(56,62);(52,61);(44,188);(28,124);(194,203);(193,199);(131,227);(67,211)	0
Class 15-8	(-4,-4,4,8,4,4,-4,-4)	(56,193);(52,194);(44,67);(28,131);(188,211);(124,227);(62,199);(61,203)	0
Class 15-9	(4,4,-8,-4,-4,-4,4,4)	(56,61);(52,62);(44,124);(28,288);(194,199);(193,203);(131,211);(67,227)	0
Class 15-10	(-4,-4,4,4,8,4,-4,-4)	(56,131);(52,67);(44,194);(28,193);(188,203);(124,199);(62,227);(61,211)	0
Class 15-11	(-4,-4,4,4,4,8,-4,-4)	(56,67);(52,131);(44,193);(28,194);(188,199);(124,203);(62,211);(61,227)	0
Class 15-12	(-4,-4,4,4,4,4,-4,-8)	(56,227);(52,211);(44,203);(28,199);(188,194);(124,193);(62,131);(61,67)	0
Class 15-13	(-4,-4,4,4,4,4,-8,-4)	(56,211);(52,227);(44,199);(28,203);(188,193);(124,194);(62,67);(61,131)	0
Class 15-14	(-4,-8,4,4,4,4,-4,-4)	(56,203);(52,199);(44,227);(28,211);(188,131);(124,67);(194,62);(193,61)	0
Class 15-15	(-8,-4,4,4,4,4,-4,-4)	(56,199);(52,203);(44,211);(28,227);(188,67);(124,131);(194,61);(62,193)	0

In Theorem 20, we can give many n-variable Boolean functions by using $(n-2)$-variable decomposition Bent functions.

Example 21. For $n = 4$, we give the cross-correlation value distribution between any two bent functions in Table 4.

(1) We find that the number of the cross-correlation distributions of any two bent functions from 896 bent functions is 2047 (=15+16+560+560+448) classes; that is, there are 2047 different cross-correlation distributions of any two bent functions.

(2) We obtain that the number of perfect uncorrelated pairs is 201210 among 2047 different cross-correlation distributions. It implies that one can find many Bent functions-pairs satisfying disjoint spectrum; that is, we can construct lots of Boolean functions $f(x) \in \mathbb{B}_n$ with $\sigma_f = 5 \cdot 2^{2n-1}$ in Theorem 20. Meanwhile, by Theorem 20, we can obtain many balanced Boolean functions $f(x)$, if bent Boolean functions f_1, f_2, f_3, f_4 satisfy $wt(f_1)+wt(f_2)+wt(f_3)+wt(f_4) = 2^{n-1}$; it is easy to find f_1, f_2, f_3, f_4 satisfying $wt(f_1) + wt(f_2) + wt(f_3) + wt(f_4) = 2^{n-1}$. For example, $wt(f_1) = wt(f_3) = 2^{n-3}+2^{(n-2)/2-1}$ and $wt(f_2) = wt(f_4) = 2^{n-3}-2^{(n-2)/2-1}$. Thus, if bent Boolean functions f_1, f_2, f_3, f_4 satisfy the following conditions,

(1) $wt(f_1) + wt(f_2) + wt(f_3) + wt(f_4) = 2^{n-1}$;

(2) two pairs of $(n-2)$-variable Bent functions $(f_1(x), f_2(x)), (f_3(x), f_4(x))$ are perfectly uncorrelated,

then f is a balanced Boolean function with $\sigma_f = 5 \cdot 2^{2n-1}$.

In stream cipher, constructing Boolean function f with high nonlinearity $\mathcal{N}_f$ and very good *GAC* property (low absolute indicator $\triangle_f$ and low sum-of-squares indicator σ_f) is favored. Addressing this problem, many works have been done; see, for instance, [3, 19, 20], which are summarized in Table 5; we find that our result is better than their methods.

Summary 3. Theorem 20 provides a construction for use in lightweight dynamic cryptographic algorithms, especially some 3-variable or 4-variable Boolean functions for encryption algorithm in the Internet of Things [2]; that is, we find many alternative cryptographic components with the same cryptographic properties.

Table 11: The cross-correlation value distributions from Class 16 to Class 21.

	CCD	$f(x) \in \mathbb{B}_3$	*LS*
Class 16-1	(-8,0,0,0,0,8,0,0)	(116,139);(184,71);(226,29);(46,209)	1
Class 16-2	(0,8,0,0,-8,0,0,0)	(116,184);(139,71);(226,209);(29,46)	0
Class 16-3	(0,-8,0,0,8,0,0,0)	(116,71);(226,46);(29,209);(139,184)	0
Class 16-4	(0,0,0,8,0,0,-8,0)	(116,226);(139,29);(184,209);(71,46)	0
Class 16-5	(0,0,0,-8,0,0,8,0)	(116,29);(139,226);(184,46);(71,209)	0
Class 16-6	(0,0,-8,0,0,0,0,8)	(116,46);(139,209);(184,29);(71,226)	0
Class 16-7	(0,0,8,0,0,0,0,-8)	(116,209);(139,46);(184,226);(71,29)	0
Class 17-1	(0,8,0,0,0,-8,0,0)	(120,180);(210,225);(30,45);(75,135)	0
Class 17-2	(0,0,8,0,0,0,-8,0)	(120,210);(180,225);(30,75);(45,135)	0
Class 17-3	(0,0,0,-8,0,0,0,8)	(120,30);(180,45);(210,75);(225,135)	0
Class 17-4	(0,0,0,8,0,0,0,-8)	(120,225);(180,210);(30,135);(45,75)	0
Class 17-5	(0,0,-8,0,0,0,8,0)	(120,45);(180,30);(210,135);(225,75)	0
Class 17-6	(0,-8,0,0,0,8,0,0)	(120,75);(180,135);(210,30);(225,45)	0
Class 17-7	(-8,0,0,0,8,0,0,0)	(120,135);(180,75);(210,45);(30,225)	1
Class 18-1	(0,8,0,0,0,0,0,-8)	(228,216);(114,177);(78,141);(27,39)	0
Class 18-2	(0,0,0,8,0,-8,0,0)	(228,114);(78,39);(141,27);(216,177)	0
Class 18-3	(0,0,-8,0,8,0,0,0)	(228,78);(114,39);(177,27);(216,141)	0
Class 18-4	(0,0,8,0,-8,0,0,0)	(228,177);(216,114);(78,27);(141,39)	0
Class 18-5	(0,0,0,-8,0,8,0,0)	(228,141);(216,78);(114,27);(177,39)	0
Class 18-6	(-8,0,0,0,0,0,8,0)	(228,27);(216,39);(114,141);(78,177)	1
Class 18-7	(0,-8,0,0,0,0,0,8)	(228,39);(216,27);(114,78);(177,141)	0
Class 19-1	(0,0,0,8,-8,0,0,0)	(212,178);(142,23);(113,232);(77,43)	0
Class 19-2	(0,0,-8,0,0,8,0,0)	(212,142);(178,23);(113,43);(77,232)	0
Class 19-3	(0,0,8,0,0,-8,0,0)	(212,113);(178,232);(142,43);(77,23)	0
Class 19-4	(0,0,0,-8,8,0,0,0)	(212,77);(178,43);(142,232);(113,23)	0
Class 19-5	(-8,0,0,0,0,0,0,8)	(212,43);(178,77);(142,113);(23,232)	1
Class 19-6	(0,-8,0,0,0,0,8,0)	(212,23);(178,142);(113,77);(43,232)	0
Class 19-7	(0,8,0,0,0,0,-8,0)	(212,232);(178,113);(142,77);(43,23)	0
Class 20-1	(0,8,-8,0,0,0,0,0)	(172,92);(163,83);(202,197);(58,53)	0
Class 20-2	(0,0,0,0,8,0,0,-8)	(172,202);(92,197);(58,163);(53,83)	0
Class 20-3	(0,0,0,0,0,-8,8,0)	(172,58);(92,53);(202,163);(197,83)	0
Class 20-4	(0,0,0,0,0,8,-8,0)	(172,197);(92,202);(58,83);(53,163)	0
Class 20-5	(0,0,0,0,-8,0,0,8)	(172,53);(92,58);(202,83);(197,163)	0
Class 20-6	(0,-8,8,0,0,0,0,0)	(172,163);(92,83);(202,58);(197,53)	0
Class 20-7	(-8,0,0,8,0,0,0,0)	(172,83);(92,163);(202,53);(58,197)	1
Class 21-1	(0,8,0,-8,0,0,0,0)	(108,156);(198,201);(54,57);(99,147)	0
Class 21-2	(0,0,0,0,8,0,-8,0)	(108,198);(156,201) (54,99);(57,147)	0
Class 21-3	(0,0,0,0,0,-8,0,8)	(108,54);(156,57);(198,99);(201,147)	0
Class 21-4	(0,0,0,0,0,8,0,-8)	(108,201);(156,198);(54,147);(57,99)	0
Class 21-5	(0,0,0,0,-8,0,8,0)	(108,57);(156,54);(198,147);(201,99)	0
Class 21-6	(0,-8,0,8,0,0,0,0)	(108,99);(156,147);(198,54);(201,57)	0
Class 21-7	(-8,0,8,0,0,0,0,0)	(108,147);(156,99);(198,57);(54,201)	1

6. Conclusions

In this paper, we have derived a construction method to obtain a Boolean function with small sum-of-squares indicator by decomposition Boolean functions; some properties and a search algorithm of Boolean functions with the same autocorrelation (or cross-correlation) distribution are given. We put up a new definition of two pairs of Boolean functions; this definition plays an important role in our construction. We believe that these conclusions and properties can be widely studied in designing the stream ciphers and block ciphers. In particular, Boolean functions with the same autocorrelation (or cross-correlation) distribution provide optional components for lightweight cryptographic algorithms in the Internet of Things. Using these Boolean functions makes cryptographic algorithms dynamic but does not change the security strength of cryptographic algorithms.

Appendix

See Tables 6, 7, 8, 9, 10, and 11.

Data Availability

All data used to support the findings of this study are included within the article (e.g., Table 1, Table 2, $\cdots$, Table 11); no other data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest in the publication of this paper.

Acknowledgments

The first author is supported by the National Key R&D Program of China (nos. 2017YFB0802000 and 2017YFB0802004). The second author is supported by the National Key R&D Program of China (no. 2017YFB0802000) and in part by the National Natural Science Foundation of China (nos. 61572148 and 61872103). The last author is supported by Jiangsu Natural Science Foundation (BK20181352) and in part by the Fundamental Research Funds for the Central Universities (no. 2015XKMS058).

References

[1] D. Evans, *The Internet of Things How the next Evolution of the Internet is Changing Everything*, Cisco Internet Business Solutions Group (IBSG), April 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[2] K. Brockmeier, "Gartner Adds Big Date, Gamification, and Internet of Things to Its Hype Cycle, Read Write Enterprise," *Trend Analysis*, 2011, https://readwrite.com/2011/08/11/gartner-adds-big-data-gamifica/.

[3] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation immunity of highly nonlinearity Boolean functions," in *Advances in Cryptology - EUROCRYPT 2000*, vol. 1807 of *Lecture Notes in Computer Sceince*, pp. 507–522, Springer, Berlin, 2000.

[4] X.-M. Zhang and Y. Zheng, "GAC- the criterion for global avalanche characteristics of cryptographic functions," *The Journal of Universal Computer Science*, vol. 1, no. 5, pp. 320–337, 1995.

[5] N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in cryptology—EUROCRYPT 2003*, vol. 2656 of *Lecture Notes in Computer Sceince*, pp. 345–359, Springer, Berlin, 2003.

[6] Q. Wang and P. Stănică, "Transparency order for Boolean functions: analysis and construction," *Designs, Codes and Cryptography*, pp. 1–17, 2019.

[7] J. J. Son, J. I. Lim, S. Chee, and S. H. Sung, "Global avalanche characteristics and nonlinearity of balanced Boolean function," *Information Processing Letters*, vol. 65, no. 3, pp. 139–144, 1998.

[8] S. H. Sung, S. Chee, and C. Park, "Global avalanche characteristics and propagation criterion of balanced Boolean functions," *Information Processing Letters*, vol. 69, no. 1, pp. 21–24, 1999.

[9] Y. Zhou, M. Xie, and G. Xiao, "On the global avalanche characteristics of two Boolean functions and the higher order nonlinearity," *Information Sciences*, vol. 180, no. 2, pp. 256–265, 2010.

[10] Y. Zhou, X. Dong, W. Zhang, and B. Zeng, "New bounds on the sum-of-squares indicator," in *Proceedings of the 7th International ICST Conference on Communications and Networking in China (CHINACOM '12)*, pp. 173–178, Kun Ming, August 2012.

[11] D. Tang, W. Zhang, and X. Tang, "Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties," *Designs, Codes and Cryptography. An International Journal*, vol. 67, no. 1, pp. 77–91, 2013.

[12] W. Zhang and G. Xiao, "Constructions of almost optimal resilient Boolean functions on large even number of variables," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5822–5831, 2009.

[13] Y. Zhou, "On the distribution of auto-correlation value of balanced Boolean functions," *Advances in Mathematics of Communications*, vol. 7, no. 3, pp. 335–347, 2013.

[14] Z. Zhuo, J. Chong, R. Yu, and M. Ren, "Global avalanche characteristics of Boolean functions by concatenation," *Journal of Harbin Institute of Technology (New Series)*, vol. 23, no. 3, pp. 91–96, 2016.

[15] Y. Zhou, W. Zhang, S. Zhu, and G. Xiao, "The global avalanche characteristics of two Boolean functions and algebraic immunity," *International Journal of Computer Mathematics*, vol. 89, no. 16, pp. 2165–2179, 2012.

[16] P. Sarkar and S. Maitra, "Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes," *Theory of Computing Systems*, vol. 35, no. 1, pp. 39–57, 2002.

[17] E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar, "New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity," in *Proceedings of the Workshop o Coding and Cryptography - WCC '01*, vol. 6 of *Electronic Notes in Discrete Mathematics*, pp. 158–167, Amsterdam, The Netherlands: Elsevier Science, Paris, France, 2001.

[18] F. Zhang, Y. Wei, E. Pasalic, and S. Xia, "Large sets of disjoint spectra plateaued functions inequivalent to partially linear functions," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 64, no. 4, part 2, pp. 2987–2999, 2018.

[19] P. Stănică, "Nonlinearity, local and global avalanche characteristics of balanced Boolean functions," *Discrete Mathematics*, vol. 248, no. 1-3, pp. 181–193, 2002.

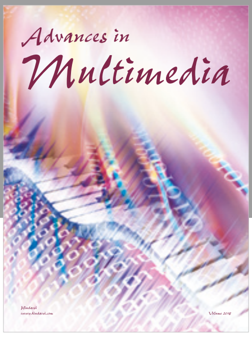
[20] P. Stănică and S. H. Sung, "Improving the nonlinearity of certain balanced Boolean functions with good local and global avalanche characteristics," *Information Processing Letters*, vol. 79, no. 4, pp. 167–172, 2001.

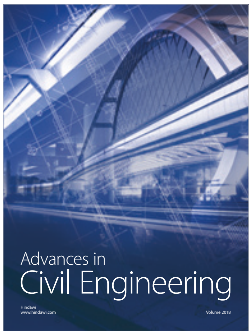
Journal of
Engineering

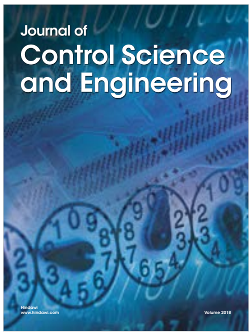
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

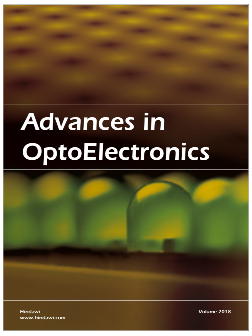

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

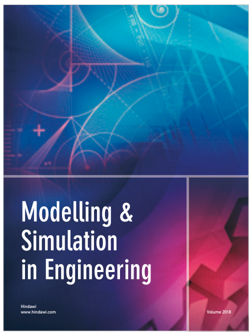
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

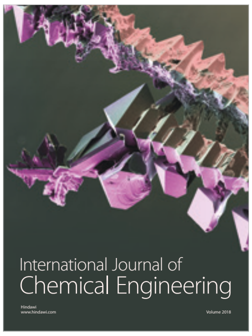

Advances in
OptoElectronics

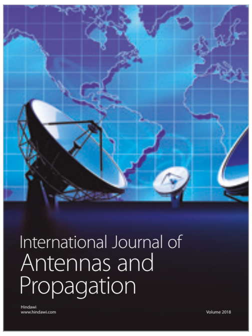
VLSI Design

International Journal of
Navigation and
Observation

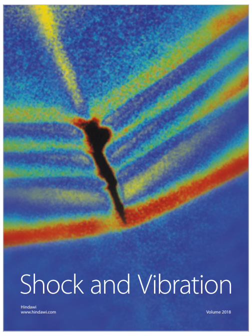

Modelling &
Simulation
in Engineering

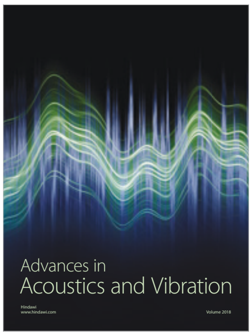
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration