Research Article

Yu Zhou*, Daoguang Mu, and Xinfeng Dong

On cryptographic properties of $(n + 1)$ -bit S-boxes constructed by known n -bit S-boxes

<https://doi.org/10.1515/jmc-2020-0004>

Received Jan 31, 2020; accepted Oct 12, 2020

Abstract: S-box is the basic component of symmetric cryptographic algorithms, and its cryptographic properties play a key role in security of the algorithms. In this paper we give the distributions of Walsh spectrum and the distributions of autocorrelation functions for $(n + 1)$ -bit S-boxes in [12]. We obtain the nonlinearity of $(n + 1)$ -bit S-boxes, and one necessary and sufficient conditions of $(n + 1)$ -bit S-boxes satisfying m -order resilient. Meanwhile, we also give one characterization of $(n + 1)$ -bit S-boxes satisfying t -order propagation criterion. Finally, we give one relationship of the sum-of-squares indicators between an n -bit S-box S_0 and the $(n + 1)$ -bit S-box S (which is constructed by S_0).

Keywords: S-boxes, Walsh spectrum, Autocorrelation distribution

2020 Mathematics Subject Classification: 94C10; 94A60; 06E30

1 Introduction

S-boxes are the most key components of encryption algorithms, diffusion and confusion [11] are two important properties of a block cipher (such as DES, AES, etc). It is very important to construct an S-box that satisfies the linear and differential properties [2, 9]. There are well studied criteria that a good S-box make the cipher resistant against differential and linear cryptanalyses.

So far, there are two main ways to produce S-boxes.

1. Test a random S-box.

First, it is necessary to generate many random S-boxes, and then select S-boxes that meet certain encryption characteristics from the random S-boxes.

2. Construct an S-box that satisfies certain cryptographic properties through mathematical methods.

In the second way, some results have been obtained.

1. Based on the disjoint linear codes, Zhang, et al. [14] proposed put up a construction of unknown resilient S-Boxes with strictly almost optimal nonlinearity. These functions reached the Siegenthaler's bound, and can be of optimal algebraic immunity or suboptimal algebraic immunity. In 2016, a construction of resilient S-boxes with higher-dimensional vectorial outputs and strictly almost optimal

Article note: This work was supported in part by the National Key R&D Program of China (No. 2017YFB0802000), and by the Sichuan Science and Technology Program (No. 2020JDJQ0076).

***Corresponding Author: Yu Zhou:** Science and Technology on Communication Security Laboratory, Chengdu 610041, China; Email: zhouyu.zhy@tom.com

Daoguang Mu: Science and Technology on Communication Security Laboratory, Chengdu 610041, China

Xinfeng Dong: Center for Cyber Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China; Science and Technology on Communication Security Laboratory, Chengdu 610041, China

non-linearity was presented in [15]. A construction of highly nonlinear (n, m, t, d) resilient S-boxes with given algebraic degree was given in [6].

2. In 2014, Li, et al. [8] gave the construction of S-boxes for lightweight ciphers with the feistel structure. Later, the linear and differential cryptanalysis of small-sized random (n, m) -S-boxes were analyzed in [1].
3. In 2019, Varici, et al. [12] constructed the $(n + 1)$ -bit S-boxes from n -bit S-boxes with known sharings, and investigated the self-equivalency of S-boxes. Meanwhile, the classification of all 3-bit S-boxes and 4-bit S-boxes according to affine equivalency were given for the first time in [4, 7], respectively.

In this paper, we focus on $(n + 1)$ -bit S-boxes constructed by n -bit S-boxes in [12]. From [12], some results on the presence of self-equivalent S-boxes and involutions in affine equivalence classes were presented. But they did not give cryptographic properties of $(n + 1)$ -bit S-boxes, such as resilient, the propagation criterion, the distribution of the Walsh spectrums and the autocorrelation functions, etc. Therefore, we give these cryptographic properties in this paper. These results, which are obtained in this paper, can help us to further understand the cryptographic properties of such construction method.

The organization of this paper is as follows. In Section 2, the basic concepts and notions are presented. In Section 3, we give some cryptographic properties of this construction. Section 4 concludes this paper.

2 Preliminaries

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

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

where the coefficients $a_0, a_i, a_{i,j}, \dots, a_{1,\dots,n} \in \mathbb{F}_2$. The algebraic degree, $\deg(f)$, is the number of variables in the highest order term with non-zero coefficient.

The support of a Boolean function $f \in \mathbb{B}_n$ is defined as $\text{Supp}(f) = \{(x_1, \dots, x_n) \mid f(x_1, \dots, x_n) = 1\}$. We say that a Boolean function f is balanced if its truth table contains an equal number of ones and zeros, i.e., if $|\text{Supp}(f)| = 2^{n-1}$. 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 its constant term equal to zero is called a linear function.

Definition 2.1. Let $f \in \mathbb{B}_n$. The Walsh spectrum of f is defined as

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

where $\varphi_\alpha(x) = \alpha x = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \dots \oplus \alpha_n x_n$.

Furthermore, then the nonlinearity of f is defined as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |\mathcal{F}(f \oplus \varphi_\alpha)|.$$

$f \in \mathbb{B}_n$ is m -resilient if and only if $\mathcal{F}(f \oplus \varphi_\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$ and $\text{wt}(\alpha) \leq m$ in [13].

Definition 2.2. Let $f, g \in \mathbb{B}_n$. The cross-correlation function between f and g is defined as

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

Thus, if $f = g$, then the auto-correlation function of $f \in \mathbb{B}_n$ is

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

Let $f, g \in \mathbb{B}_n$, then f and g are perfectly uncorrelated, if $\triangle_{f,g}(\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^n$.

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

Definition 2.3. The two indicators (σ_f and $\triangle_f$) are called the global avalanche characteristics of Boolean functions $f, g \in \mathbb{B}_n$ (GAC [16]).

$$\sigma_f = \sum_{\alpha \in \mathbb{F}_2^n} [\triangle_f(\alpha)]^2, \quad \triangle_f = \max_{\alpha \in \mathbb{F}_2^n, \text{wt}(\alpha) \neq 0^n} |\triangle_f(\alpha)|,$$

where 0^n is the zero vector of $\mathbb{F}_2^n$.

The research of this paper is based on the following construction methods.

Definition 2.4. ([12]) Let $S_1(x) = (t_1, t_2, \dots, t_n)$ and $S_2(x) = (u_1, u_2, \dots, u_n)$ be two $n \times n$ S-boxes (bijections), where $x = (x_1, x_2, \dots, x_n)$. An $(n+1) \times (n+1)$ S-box (not always a bijection) $\mathfrak{S}(x_1, x_2, \dots, x_n, x_{n+1}) = (y_1, y_2, \dots, y_{n+1})$:

$$\begin{aligned} y_i &= x_{n+1}t_i \oplus (1 \oplus x_{n+1})u_i, i = 1, 2, \dots, n; \\ y_{n+1} &= x_{n+1}F(x) \oplus (1 \oplus x_{n+1})G(x), \end{aligned}$$

where $G, F \in \mathbb{B}_n$.

From Definition 2.4, if $x_{n+1} = 0$, then $\mathfrak{S}(x, x_{n+1}) = (S_2(x), G(x))$, if $x_{n+1} = 1$, then $\mathfrak{S}(x, x_{n+1}) = (S_1(x), F(x))$.

Lemma 2.5. ([12]) $\mathfrak{S}$ is a bijection if and only if $G(x) = F(S_1^{-1}(S_2(x))) \oplus 1, x \in \mathbb{F}_2^n$.

In this paper, we suppose that $S_1(x) = S_2(x) = S(x)$ ($S_1(x), S_2(x)$ are $n \times n$ bijections in $\mathbb{F}_2^n$) and $F(x) = G(x) \oplus 1$ for any $x \in \mathbb{F}_2^n$ in Lemma 2.5. Then an $(n+1) \times (n+1)$ S-box (a bijection) $\mathfrak{S}'(x_1, x_2, \dots, x_n, x_{n+1}) = (y_1, y_2, \dots, y_{n+1})$ in Definition 2.4 is:

$$\begin{aligned} y_i &= S_i, i = 1, 2, \dots, n; \\ y_{n+1} &= x_{n+1} \oplus G(x). \end{aligned}$$

3 Main result

In this section, we give the distributions of Walsh spectrum and the autocorrelation functions, respectively.

3.1 The distributions of Walsh spectrum of $\mathfrak{S}'$

We give the Walsh spectrum of $\mathfrak{S}'$, and obtain some properties in this subsection.

Lemma 3.1. ([5]) Let $f, g \in \mathbb{B}_n$. For any $\text{wt}(\omega) \neq 0$ and $\omega \in \mathbb{F}_2^n$, then

$$\mathcal{F}((f \oplus g) \oplus \varphi_\omega) = \mathcal{F}(f \oplus \varphi_\omega) + \mathcal{F}(g \oplus \varphi_\omega) - 2\mathcal{F}(f \cdot g \oplus \varphi_\omega).$$

Based on Lemma 3.1 and Definition 2.1, we have Theorem 3.2.

Theorem 3.2. Let $\mathfrak{S}'$ be an $(n + 1) \times (n + 1)$ bijection. Then the Walsh spectrum $\mathcal{F}((v, v_{n+1}) \cdot \mathfrak{S}' \oplus \varphi_{(\omega, \omega_{n+1})})$ (denoted by $\mathcal{F}_{\mathfrak{S}'}$) of $(v, v_{n+1}) \cdot \mathfrak{S}'$ ($v \in \mathbb{F}_2^n, v_{n+1} \in \mathbb{F}_2$) satisfies:

$$\mathcal{F}_{\mathfrak{S}'} = \begin{cases} 2\mathcal{F}(v \cdot S \oplus \varphi_\omega), & \omega_{n+1} = 0, wt(\omega) \neq 0, v_{n+1} = 0; \\ 0, & \omega_{n+1} = 0, wt(\omega) \neq 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 1, wt(\omega) \neq 0, v_{n+1} = 0; \\ 2\mathcal{F}(v \cdot S \oplus \varphi_\omega) \\ - 4\mathcal{F}((v \cdot S)G \oplus \varphi_\omega) \\ + 2\mathcal{F}(G \oplus \varphi_\omega), & \omega_{n+1} = 1, wt(\omega) \neq 0, v_{n+1} = 1; \\ 2 \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S}, & \omega_{n+1} = 0, wt(\omega) = 0, v_{n+1} = 0; \\ 0, & \omega_{n+1} = 0, wt(\omega) = 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 1, wt(\omega) = 0, v_{n+1} = 0; \\ 2 \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S \oplus G}, & \omega_{n+1} = 1, wt(\omega) = 0, v_{n+1} = 1. \end{cases}$$

Proof. According to the definition of Walsh spectrum, we have

$$\begin{aligned} \mathcal{F}((v, v_{n+1}) \cdot \mathfrak{S}' \oplus \varphi_{(\omega, \omega_{n+1})}) &= \sum_{x \in \mathbb{F}_2^n, x_{n+1} \in \mathbb{F}_2} (-1)^{(v, v_{n+1}) \cdot \mathfrak{S}' \oplus \omega \cdot x \oplus \omega_{n+1} \cdot x_{n+1}} \\ &= \sum_{x \in \mathbb{F}_2^n, x_{n+1} = 0} (-1)^{(v, v_{n+1}) \cdot (S, G) \oplus \omega \cdot x} \\ &\quad + \sum_{x \in \mathbb{F}_2^n, x_{n+1} = 1} (-1)^{(v, v_{n+1}) \cdot (S, G \oplus 1) \oplus \omega \cdot x \oplus \omega_{n+1}} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{(v, v_{n+1}) \cdot (S, G) \oplus \omega \cdot x} \\ &\quad + (-1)^{\omega_{n+1}} \sum_{x \in \mathbb{F}_2^n} (-1)^{(v, v_{n+1}) \cdot (S, G \oplus 1) \oplus \omega \cdot x} \\ &= (1 + (-1)^{v_{n+1} \oplus \omega_{n+1}}) \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S(x) \oplus v_{n+1} \cdot G(x) \oplus \omega \cdot x} \end{aligned}$$

We prove it for two cases.

Case 1. When $wt(\omega) = 0$, that is, $\omega = \mathbf{0}^n$. Then $\mathcal{F}((v, v_{n+1}) \cdot \mathfrak{S}' \oplus \varphi_{(\mathbf{0}^n, \omega_{n+1})})$

$$\begin{aligned} &= \sum_{x \in \mathbb{F}_2^n} (-1)^{(v, v_{n+1}) \cdot (S, G)} + (-1)^{\omega_{n+1}} \sum_{x \in \mathbb{F}_2^n} (-1)^{(v, v_{n+1}) \cdot (S, G \oplus 1)} \\ &= \left[1 + (-1)^{v_{n+1} \oplus \omega_{n+1}} \right] \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S \oplus v_{n+1} \cdot G} \\ &= \begin{cases} 2 \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S}, & \omega_{n+1} = 0, wt(\omega) = 0, v_{n+1} = 0; \\ 0, & \omega_{n+1} = 0, wt(\omega) = 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 1, wt(\omega) = 0, v_{n+1} = 0; \\ 2 \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S \oplus G}, & \omega_{n+1} = 1, wt(\omega) = 0, v_{n+1} = 1. \end{cases} \end{aligned}$$

Case 2. When $wt(\omega) \neq 0$, that is, $\omega \neq \mathbf{0}^n$. By Lemma 3.1 we have $\mathcal{F}((v, v_{n+1}) \cdot \mathfrak{S}' \oplus \varphi_{(\omega, \omega_{n+1})})$

$$\begin{aligned}
 &= \sum_{x \in \mathbb{F}_2^n} (-1)^{(v, v_{n+1}) \cdot (S, G) \oplus \omega \cdot x} + (-1)^{\omega_{n+1}} \sum_{x \in \mathbb{F}_2^n} (-1)^{(v, v_{n+1}) \cdot (S, G \oplus 1) \oplus \omega \cdot x} \\
 &= \left[(1 + (-1)^{v_{n+1} \oplus \omega_{n+1}}] \mathcal{F}((v \cdot S \oplus v_{n+1} \cdot G) \oplus \varphi_{(\omega, \omega_{n+1})}) \right. \\
 &= \left[1 + (-1)^{v_{n+1} \oplus \omega_{n+1}} \right] \{ \mathcal{F}((v \cdot S) \oplus \varphi_{(\omega)}) + \mathcal{F}((v_{n+1} \cdot G) \oplus \varphi_{(\omega)}) \\
 &\quad - 2\mathcal{F}((v \cdot S) \cdot (v_{n+1} \cdot G)) \oplus \varphi_{(\omega)} \} \\
 &= \begin{cases} 2\mathcal{F}((v \cdot S) \oplus \varphi_{\omega}), & \omega_{n+1} = 0, wt(\omega) \neq 0, v_{n+1} = 0; \\ 0, & \omega_{n+1} = 0, wt(\omega) \neq 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 1, wt(\omega) \neq 0, v_{n+1} = 0; \\ 2[\mathcal{F}((v \cdot S) \oplus \varphi_{\omega}) \\ + \mathcal{F}((G) \oplus \varphi_{\omega}) \\ - 2\mathcal{F}(((v \cdot S) \cdot G) \oplus \varphi_{\omega})], & \omega_{n+1} = 1, wt(\omega) \neq 0, v_{n+1} = 1. \end{cases}
 \end{aligned}$$

□

Particularly, we obtain Corollary 3.3.

Corollary 3.3. Let $\mathfrak{S}'$ be an $(n+1) \times (n+1)$ bijection. Then the Walsh spectrum $\mathcal{F}((v, v_{n+1}) \cdot \mathfrak{S}' \oplus \varphi_{(\omega, \omega_{n+1})})$ (denoted by $\mathcal{F}_{\mathfrak{S}'}$) of $(v, v_{n+1}) \cdot \mathfrak{S}'$ ($v \in \mathbb{F}_2^n, v_{n+1} \in \mathbb{F}_2$) satisfies:

1. When $v \neq \mathbf{0}^n$.

$$\mathcal{F}_{\mathfrak{S}'} = \begin{cases} 2\mathcal{F}(v \cdot S \oplus \varphi_{\omega}), & \omega_{n+1} = 0, wt(\omega) \neq 0, v_{n+1} = 0; \\ 0, & \omega_{n+1} = 0, wt(\omega) \neq 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 1, wt(\omega) \neq 0, v_{n+1} = 0; \\ 2\mathcal{F}(v \cdot S \oplus \varphi_{\omega}) \\ - 4\mathcal{F}((v \cdot S)G \oplus \varphi_{\omega}) \\ + 2\mathcal{F}(G \oplus \varphi_{\omega}), & \omega_{n+1} = 1, wt(\omega) \neq 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 0, wt(\omega) = 0, v_{n+1} = 0; \\ 0, & \omega_{n+1} = 0, wt(\omega) = 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 1, wt(\omega) = 0, v_{n+1} = 0; \\ 2 \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S \oplus G}, & \omega_{n+1} = 1, wt(\omega) = 0, v_{n+1} = 1. \end{cases}$$

2. When $v = \mathbf{0}^n$.

$$\mathcal{F}_{\mathfrak{S}'} = \begin{cases} 0, & \omega_{n+1} = 0, wt(\omega) \neq 0, v_{n+1} = 1; \\ 2\mathcal{F}(G \oplus \varphi_{\omega}), & \omega_{n+1} = 1, wt(\omega) \neq 0, v_{n+1} = 1; \\ 0, & \omega_{n+1} = 0, wt(\omega) = 0, v_{n+1} = 1; \\ 2(2^n - 2wt(G)), & \omega_{n+1} = 1, wt(\omega) = 0, v_{n+1} = 1. \end{cases}$$

Proof. 1. When $v \neq \mathbf{0}^n$.

Because $\mathfrak{S}'$ is a bijection, $(v, v_{n+1}) \cdot \mathfrak{S}'$ is a balanced function for any $wt(v, v_{n+1}) \neq \mathbf{0}^{n+1}$. Thus, $v_{n+1} = 1$ or $v_{n+1} = 0$. Note that S is a balanced bijection, thus $v \cdot S$ is a balanced function for any $wt(v) \neq 0$, that is, $\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S} = 0$.

2. When $v = \mathbf{0}^n$.

Because $\mathfrak{S}'$ is a bijection, $v_{n+1} = 1$. Then

$$\mathcal{F}(v \cdot S \oplus \varphi_{\omega}) = \mathcal{F}((v \cdot S) \cdot G \oplus \varphi_{\omega}) = \mathcal{F}(\varphi_{\omega}) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\omega \cdot x} = 0, \quad \omega \neq \mathbf{0}^n.$$

□

Form the distributions of Walsh Spectrum in Theorem 3.2 and Corollary 3.3, we deduce Corollary 3.4.

Corollary 3.4. *Let $\mathfrak{S}'$ be an $(n+1) \times (n+1)$ bijection. If G is a balanced function, then the nonlinearity $\mathcal{N}_{(v, v_{n+1}) \cdot \mathfrak{S}'}$ satisfies:*

$$\mathcal{N}_{(v, v_{n+1}) \cdot \mathfrak{S}'} = 2^{n-1} - \frac{1}{2} \cdot N_{\max},$$

where $N_{\max} = \max\{\max_{\omega \in \mathbb{F}_2^n} |\mathcal{F}(G \oplus \varphi_\omega)|, \max_{\omega \in \mathbb{F}_2^n} |\mathcal{F}((v \cdot S) \oplus \varphi_\omega)|, \max_{\omega \in \mathbb{F}_2^n} |\mathcal{F}((v \cdot S) \oplus G \oplus \varphi_\omega)|\}$.

Combining the resilient functions and the distributions of Walsh Spectrum, we obtain Corollary 3.5.

Corollary 3.5. *Let $\mathfrak{S}'$ be an $(n+1) \times (n+1)$ bijection. If G is a balanced function, then*

1. *When $v = \mathbf{0}^n$, $(v, v_{n+1}) \cdot \mathfrak{S}'$ is a t -th resilient function for $v_{n+1} = 1$ if and only if G is a t -th resilient function.*
2. *When $v \neq \mathbf{0}^n$, $(v, v_{n+1}) \cdot \mathfrak{S}'$ is a t -th resilient function for any $v_{n+1} \in \mathbb{F}_2$ and given v if and only if G , $v \cdot S$ and $(v \cdot S) \cdot G$ all are t -th resilient functions.*

3.2 The distributions of the autocorrelation function of $\mathfrak{S}'$

Based on Definition 2.2 and Definition 2.4, we give the distributions of the autocorrelation function of this S-box.

Theorem 3.6. *Let $\mathfrak{S}'$ be an $(n+1) \times (n+1)$ bijection. Then the autocorrelation function of $(v, v_{n+1}) \cdot \mathfrak{S}'$ ($v \in \mathbb{F}_2^n, v_{n+1} \in \mathbb{F}_2$) satisfies:*

$$\Delta_{((v, v_{n+1}) \cdot \mathfrak{S}')}(\alpha, \alpha_{n+1}) = \begin{cases} 2\Delta_{(v \cdot S)}(\alpha), & \alpha_{n+1} = 0, v_{n+1} = 0; \\ 2\Delta_{(v \cdot S) \oplus G}(\alpha), & \alpha_{n+1} = 0, v_{n+1} = 1; \\ 2\Delta_{(v \cdot S)}(\alpha), & \alpha_{n+1} = 1, v_{n+1} = 0; \\ -2\Delta_{(v \cdot S) \oplus G}(\alpha), & \alpha_{n+1} = 1, v_{n+1} = 1; \end{cases} \quad \alpha \in \mathbb{F}_2^n.$$

Proof. According to the autocorrelation function, we have $\Delta_{((v, v_{n+1}) \cdot \mathfrak{S}')}(\alpha, \alpha_{n+1})$ (denoted by $\Delta_{\mathfrak{S}'}$).

$$\begin{aligned} \Delta_{\mathfrak{S}'} &= \sum_{x \in \mathbb{F}_2^n, x_{n+1} \in \mathbb{F}_2} (-1)^{(v, v_{n+1}) \cdot \mathfrak{S}'(x, x_{n+1}) \oplus (v, v_{n+1}) \cdot \mathfrak{S}'(x \oplus \alpha, x_{n+1} \oplus \alpha_{n+1})} \\ &= \underbrace{\sum_{x \in \mathbb{F}_2^n, x_{n+1}=0} (-1)^{(v, v_{n+1}) \cdot \mathfrak{S}'(x, 0) \oplus (v, v_{n+1}) \cdot \mathfrak{S}'(x \oplus \alpha, \alpha_{n+1})}}_{\text{denoted by } I_1} \\ &\quad + \underbrace{\sum_{x \in \mathbb{F}_2^n, x_{n+1}=1} (-1)^{(v, v_{n+1}) \cdot \mathfrak{S}'(x, 1) \oplus (v, v_{n+1}) \cdot \mathfrak{S}'(x \oplus \alpha, 1 \oplus \alpha_{n+1})}}_{\text{denoted by } I_2} \\ &= I_1 + I_2. \end{aligned}$$

According to the expression of $\mathfrak{S}'$ in Definition 2.4, we have

$$\begin{aligned}
 I_1 &= \sum_{x \in \mathbb{F}_2^n} \{(-1)^{(v \cdot S(x)) \oplus \alpha_{n+1}(v \cdot S(x \oplus \alpha)) \oplus (1 \oplus \alpha_{n+1})(v \cdot S(x \oplus \alpha)) \oplus v_{n+1} \cdot G(x)} \\
 &\quad (-1)^{\oplus v_{n+1} \cdot \alpha_{n+1} \cdot (G(x \oplus \alpha) \oplus 1) \oplus v_{n+1} \cdot (1 \oplus \alpha_{n+1}) \cdot G(x \oplus \alpha)}\} \\
 &= (-1)^{\alpha_{n+1} \cdot v_{n+1}} \sum_{x \in \mathbb{F}_2^n} (-1)^{(v \cdot (S \oplus S(x \oplus \alpha))) \oplus v_{n+1} \cdot (G(x) \oplus G(x \oplus \alpha))} \\
 &= \begin{cases} \Delta_{(v \cdot S)}(\alpha), & \alpha_{n+1} = 0, v_{n+1} = 0; \\ \Delta_{(v \cdot S) \oplus G}(\alpha), & \alpha_{n+1} = 0, v_{n+1} = 1; \\ \Delta_{(v \cdot S)}(\alpha), & \alpha_{n+1} = 1, v_{n+1} = 0; \\ -\Delta_{(v \cdot S) \oplus G}(\alpha), & \alpha_{n+1} = 1, v_{n+1} = 1. \end{cases}
 \end{aligned}$$

and

$$\begin{aligned}
 I_2 &= \sum_{x \in \mathbb{F}_2^n} \{(-1)^{(v \cdot S(x)) \oplus (1 \oplus \alpha_{n+1})(v \cdot S(x)) \oplus \alpha_{n+1}(v \cdot S(x \oplus \alpha)) \oplus v_{n+1} G(x)} \\
 &\quad (-1)^{\oplus v_{n+1} \oplus (1 \oplus \alpha_{n+1})v_{n+1} G(x \oplus \alpha) \oplus v_{n+1} (1 \oplus \alpha_{n+1}) \oplus v_{n+1} \alpha_{n+1} G(x \oplus \alpha)}\} \\
 &= (-1)^{\oplus v_{n+1} \alpha_{n+1}} \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot (S(x) \oplus S(x \oplus \alpha)) \oplus v_{n+1} (G(x) \oplus G(x \oplus \alpha))} \\
 &= \begin{cases} \Delta_{(v \cdot S)}(\alpha), & \alpha_{n+1} = 0, v_{n+1} = 0; \\ \Delta_{(v \cdot S) \oplus G}(\alpha), & \alpha_{n+1} = 0, v_{n+1} = 1; \\ \Delta_{(v \cdot S)}(\alpha), & \alpha_{n+1} = 1, v_{n+1} = 0; \\ -\Delta_{(v \cdot S) \oplus G}(\alpha), & \alpha_{n+1} = 1, v_{n+1} = 1. \end{cases}
 \end{aligned}$$

Thus, we prove this result. $\square$

Based on the distribution of autocorrelation functions in Theorem 3.6, we have this Corollary 3.7.

Corollary 3.7. *Let $\mathfrak{S}'$ be an $(n+1) \times (n+1)$ bijection. The propagation criterion of $\sigma_{(v, v_{n+1}) \cdot \mathfrak{S}'}$ satisfies:*

1. *When $v_{n+1} = 0$, $\sigma_{(v, v_{n+1}) \cdot \mathfrak{S}'}$ satisfies the propagation criterion $PC(t)$ for given $v \in \mathbb{F}_2^n$ and $wt(v) \neq 0$ if and only if $(v \cdot S)$ satisfies the propagation criterion $PC(t)$.*
2. *When $v_{n+1} = 1$, $\sigma_{(v, v_{n+1}) \cdot \mathfrak{S}'}$ satisfies the propagation criterion $PC(t)$ for given $v \in \mathbb{F}_2^n$ if and only if $(v \cdot S) \oplus G$ satisfies the propagation criterion $PC(t)$.*

Thus, for any $wt(v, v_{n+1}) \neq 0$, $\sigma_{(v, v_{n+1}) \cdot \mathfrak{S}'}$ satisfies the propagation criterion $PC(t)$ if and only if $(v \cdot S) \oplus G$ satisfies the propagation criterion $PC(t)$.

Finally, we give one relationship between $\sigma_{\mathfrak{S}'}$ and σ_S .

Corollary 3.8. *Let $\mathfrak{S}'$ be an $(n+1) \times (n+1)$ bijection. The the sum-of-squares indicator $(\sigma_{(v, v_{n+1}) \cdot \mathfrak{S}'})$ satisfies*

$$\sigma_{(v, v_{n+1}) \cdot \mathfrak{S}'} = \begin{cases} 2\sigma_{v \cdot S}, & v_{n+1} = 0; \\ 2\sigma_{v \cdot S \oplus G}, & v_{n+1} = 1; \end{cases} \quad \text{for given } v \in \mathbb{F}_2^n.$$

4 Conclusions

In this paper, we give the distributions of Walsh spectrum and the distributions of the autocorrelation functions for $(n+1)$ -bit S-boxes in [12], and obtain the correlation immunity, propagation criterion, etc. Our results are a supplement to the result in [12]. Meanwhile, these results of this paper are given for any n -bit S-box and

any $G \in \mathbb{B}_n$, if G is replaced with the rotation symmetric Boolean function [3], then more specific results can be obtained. These properties can help us to evaluate whether the S-boxes can be used in Block cipher or Stream cipher or not.

In the next step, it will be an important issue to study the difference properties, the algebraic immunity [10], and the global avalanche characteristics of cross-correlation function [18] of the S-box in this paper. It is also interesting to extend the method [12] for constructing new S-boxes.

Acknowledgement: The authors also are grateful to Dr. Wang Lin for some valuable suggestions. The authors wish to thank the anonymous referees for their valuable comments to improve the presentation of this paper.

References

- [1] Y. Alsalamy, C. Y. Yeun, T. Martin, M. Khonji, Linear and differential cryptanalysis of small-sized random (n, m) S-boxes, 2016 11-th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 447–454, 2016.
- [2] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, In International Cryptology Conference on Advances in Cryptology, CRYPTO 1990, Springer-Verlag, London, pp. 2–21, 1991.
- [3] T. W. Cusick, K. V. Lakshmy, M. Sethumadhavan, Affine equivalence of monomial rotation symmetric Boolean functions: A Pólya's theorem approach, *Journal of Mathematical Cryptology*, **10** (3-4) (2016), 145–156.
- [4] C. De Canniere, Analysis and Design of Symmetric Encryption Algorithms, PhD thesis, KU Leuven, 2007.
- [5] C. Ding, G. Xiao, W. Shan, The stability Theory of Stream Ciphers, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, **561**, 1991.
- [6] S. Fu, K. Matsuura, C. Li, L. Qu, Construction of highly nonlinear resilient S-boxes with given degree, *Designs, Codes and Cryptography*, **64** (3) (2012), 241–253.
- [7] G. Leander, A. Poschmann, On the classification of 4 bit S-boxes, *WAIFI 2007* (2007), 159–176.
- [8] Y. Li, M. Wang, Constructing S-boxes for lightweight cryptography with feistel structure, In International Workshop on Cryptographic Hardware and Embedded Systems, Springer, pp. 127–146, 2014.
- [9] M. Matsui, A. Yamagishi, A new method for known plaintext attack of FEAL cipher, In Advances in Cryptology - EUROCRYPT 1992, Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 81–91, 1993.
- [10] W. Meier, E. Pasalic, C. Carlet, Algebraic attacks and decomposition of Boolean functions. In Advances in Cryptology-Eurocrypt, 2004, Berlin: Springer-Verlag, LNCS **3027** (2004), 474–491.
- [11] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, **28** (4) (1949), 656–715.
- [12] K. Varici, S. Nikova, V. Nikov, V. Rijmen, Constructions of S-boxes with uniform sharing, *Cryptography and Communications*, **11**(3) (2019), 385–398.
- [13] G. Xiao, J. L. Massey, A spectral characterization of correlation-immune combining function, *IEEE Trans. Information Theory*, **34** (3) (1988), 569–571.
- [14] W. Zhang, E. Pasalic, Highly nonlinear balanced S-boxes with good differential properties, *IEEE Transactions on Information Theory*, **60** (12) (2014), 7970–7979.
- [15] W. Zhang, L. Li, E. Pasalic, Construction of resilient S-boxes with higher-dimensional vectorial outputs and strictly almost optimal non-linearity, *IET Information Security*, **11** (4) (2016), 199–203.
- [16] X. M. Zhang, Y. L. Zheng, GAC- the criterion for global avalanche characteristics of cryptographic functions, *Journal for Universal Computer Science*, **1** (5)(1995), 316–333.
- [17] Y. Zhou, M. Xie, G. Xiao, On the global avalanche characteristics of two Boolean functions and the higher order nonlinearity, *Information Sciences*, **180** (2010), 256–265.
- [18] Y. Zhou, W. Zhang, J. Li, X. Dong, G. Xiao, The autocorrelation distribution of balanced Boolean function, *Frontier of Computer Science*, **7** (2) (2013), 272–278.