DESIGN OF S-BOXES BY CONCATENATION OF ROTATION-SYMMETRIC S-BOXES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

SEVDENUR BALOĞLU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2016

Approval of the thesis:

DESIGN OF S-BOXES BY CONCATENATION OF ROTATION-SYMMETRIC S-BOXES

submitted by **SEVDENUR BALOĞLU** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak
Supervisor, **Cryptography, METU**

Assist. Prof. Dr. Selçuk Kavut
Co-supervisor, **Computer Engineering, Balıkesir University**

Examining Committee Members:

Prof. Dr. Ferruh Özbudak
Cryptography, METU

Assoc. Prof. Dr. Murat Cenk
Cryptography, METU

Assoc. Prof. Dr. Sedat Akleylek
Computer Engineering, Ondokuz Mayıs University

Date:

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: SEVDENUR BALOĞLU

Signature :

ABSTRACT

DESIGN OF S-BOXES BY CONCATENATION OF ROTATION-SYMMETRIC S-BOXES

Baloğlu, Sevdenur

M.S., Department of Cryptography

Supervisor : Prof. Dr. Ferruh Özbudak

Co-Supervisor : Assist. Prof. Dr. Selçuk Kavut

September 2016, 57 pages

In most of the block cipher cryptosystems, the substitution boxes, or so-called S-boxes, are the only nonlinear components, and hence the strength of these cryptosystems depends heavily on the cryptographic properties of the S-boxes. In this thesis, it is aimed to design S-boxes which are on one hand strong in terms of traditional cryptographic properties such as nonlinearity, differential uniformity, absolute indicator and algebraic degree, and on the other hand resistant to side-channel attacks such as differential power analysis (DPA). In the direction of this aim, an efficient exhaustive search algorithm is proposed to generate 6×6 bijective S-boxes situated in a class of symmetric S-boxes under the permutation $\tau(x) = (x_0, x_2, x_3, x_4, x_5, x_1)$, where $x = (x_0, x_1, ..., x_5) \in \mathbb{F}_2^6$. Due to the symmetry property of $\tau(S(x)) = S(\tau(x))$ for all x, any S-box S in this class can be considered as a construction obtained by the concatenation of 5×5 rotation-symmetric S-boxes (RSSBs). In this algorithm, using the combinatorial properties of RSSBs and eliminating the affine equivalent concatenations, the search space of this class is reduced from $2^{61.28}$ to $2^{48.47}$. At the end of this search, it is found that in this class there exist $2^{37.56}$ S-boxes having the best known nonlinearity 24 and among them the number of differentially 4-uniform ones is $2^{33.99}$, which indicates that the concatenation method provides a rich class in terms of high nonlinearity and low differential uniformity.

Keywords : Block ciphers, S-boxes, rotation-symmetric S-boxes, concatenations, Boolean functions.

ÖZ

DÖNGÜSEL SİMETRİK S-KUTULARININ BAĞLAŞIMI İLE S-KUTULARININ TASARLANMASI

Baloğlu, Sevdenur
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak
Ortak Tez Yöneticisi : Yrd. Doç. Dr. Selçuk Kavut

Eylül 2016, 57 sayfa

S-kutuları olarak da isimlendirilen yerleştirme kutuları blok şifreli kriptosistemlerin birçoğunda doğrusal olmayan tek bileşenlerdir. Bu yüzden bu kriptosistemlerin dayanıklılığı ağırlıklı olarak S-kutularının kriptografik özelliklerine bağlıdır. Bu tezde, hem doğrusal olmama, farksal birbiçimlilik, mutlak gösterge ve cebirsel derece gibi geleneksel kriptografik özellikleri bakımından güçlü, hem de farksal güç analizi (DPA) gibi yan kanal saldırılarına karşı dayanıklı S-kutularının tasarımı amaçlanmaktadır. Bu amaç doğrultusunda, 6×6 bijektif S-kutularını üretmek için verimli bir tüketici arama algoritması tasarlanmıştır. Bu S-kutuları, $x = (x_0, x_1, ..., x_5) \in \mathbb{F}_2^6$ iken $\tau(x) = (x_0, x_2, x_3, x_4, x_5, x_1)$ permütasyonu altındaki simetrik S-kutularının oluşturduğu sınıfta bulunmaktadır. Bu sınıftaki her bir S-kutusu S'nin, her x için taşıdığı simetri özelliği $\tau(S(x)) = S(\tau(x))$ dolayısıyla S, 5×5 döngüsel simetrik S-kutularının (DSSK'ların) bağlaşımı yöntemiyle elde edilen bir yapı olarak düşünülebilir. Bu algoritmada DSSK' ların kombinasyonel özellikleri kullanılarak ve afin denkliğe sahip bağlaşımlar elenerek, $2^{61.28}$ olan arama uzayı $2^{48.47}$'ye düşürülmüştür. Bu araştırmanın sonucunda, bu sınıfta $2^{37.56}$ tane doğrusal olmama koşutu 24 (6×6 bijektif S-kutuları için bilinen en yüksek değer) olan S-kutusunun var olduğu ve bunlar içinde farksal birbiçimliliği 4 olan S-kutusu sayısının $2^{33.99}$ olduğu bulunmuştur. Bu da bağlaşım yönteminin, doğrusal olmama koşutunun yüksek olması ve farksal birbiçimliliğinin düşük olması açısından zengin bir sınıf sağladığını gösterir.

Anahtar Kelimeler : Blok şifreler, S-kutuları, döngüsel simetrik S-kutuları, bağlaşımlar, Boole fonksiyonları.

To My Family

ACKNOWLEDGMENTS

Throughout the two-year period of my master of education, I met with too many people, each of whom contributed value to my life from different viewpoints, I enjoyed too many friendships, I learned too much things in both life and education. There is a life goal I wanted to achieve for the years, and consequently I stepped forward one more time with the aid of too many people in my life. Now, I would like to gratefully acknowledge each of them for their support and contribution.

First of all, I would like to thank our dearest academic member of our department, Assoc. Prof. Murat Cenk for his willingness to educate us, his fair treatment, encouragements, valuable advices every time. Also, I want to thank Assoc. Prof. Ali Doğanaksoy and Dr. Muhiddin Uğuz for being good coordinators of our research groups and teaching us a lot of things, and for their enthusiasm in this field.

I also would like to express my gratitude to my co-advisor Assist. Prof. Selçuk Kavut for his guidance in this research. He helped me a lot to learn most of the things in my thesis. I am also grateful to my supervisor Prof. Ferruh Özbudak. His curiosity and interest in this field made me more studious and enthusiastic.

I owe a debt of gratitude to my dearest friends for their valuable friendships, especially to Duygu, Emre and Erkan. From the beginning, they have always been good fellows that companions me in this journey. One of these friends to be thanked is Alperen, his manners to me have always been supportive. I also thank to my friends in other departments.

I am very grateful to research assistant Ahmet Sınak. He helped me a lot during this period. Beside being a good instructor, he has also been a good friend. Also, I want to thank research assistants Eda Tekin and Bilgi Yılmaz for their kind and warm manners all the time.

Finally and mostly, I appreciate my family for their moral and material support, and their encouragement all the time. They always make me proud of being a part of this family. Very special thanks to my sisters and Mustafa for their cheerful manners which make me stand all the difficulties of this process.

As a remark, this work is an outcome of a project which is coordinated by Assist. Prof. Selçuk Kavut and supported financially by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under the grant 114E486. It is also an elaborated version of the paper which is named by ”Classification of 6×6 S-boxes Obtained by Concatenation of RSSBs” and recently accepted to the conference of LightSec 2016.

TABLE OF CONTENTS

CHAPTERS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

$\mathbb{Z}$	The set of integers
$\mathbb{F}_2$	Binary finite field
$\oplus$	XOR addition
$\mathcal{F}_n$	The set of n-variable Boolean functions
$\mathcal{A}_n$	The set of n-variable affine functions
$w_H(f)$	Hamming weight of f
$d(f, g)$	Distance between f and g
$W_f(w)$	Walsh value of the Boolean function f at w
$W_S(w, c)$	Walsh value of the S-box S at (w, c)
W_f	Walsh spectrum of f
$\mathcal{N}_f$	Nonlinearity of f
$C_{f,g}$	Correlation function of f and g
$\Delta_f(d)$	Auto-correlation function of f at d
Δ_f	Correlation immunity of f
$deg(f)$	Algebraic degree of f
$d_{\min}$	Minimum algebraic degree among component functions of an S-box
$d_{\max}$	Maximum algebraic degree among coordinate functions of an S-box
δ_S	Differential uniformity of S
γ_S	Transparency order (TO) of S
ρ^k	k-th cyclic shift operator
G_n	Generator of the orbits of $\mathbb{F}_2^n$ under the action of ρ^k
g_n	The number of orbits of $\mathbb{F}_2^n$
Λ	Orbit representative
$\|\|$	Concatenation symbol
gcd	Greatest common divisor
lcm	Least common multiple
ANF	Algebraic Normal Form
$RSBF$	Rotation-symmetric Boolean function
$RSSB$	Rotation-symmetric S-box

CHAPTER 1

INTRODUCTION

The subjects of cryptography as a science of secrecy, are divided into two parts: symmetric (secret key) cryptography and asymmetric (public key) cryptography. In the systems of both types of cryptography there is data to be encrypted, an algorithm which is used for the encryption of this data, and a secret key that is integrated in the encryption algorithm to make the output incomprehensible. For the first type of system, this data can be a secret message between the sender and the receiver. If this is the case, the secret key is shared between both parties and hidden from everybody else. If the public key cryptosystem is in question, in which there is more than one sender or receiver, anybody in this system has his own secret key and also a public key which is known by everyone.

The ciphers of symmetric cryptography are categorized into two class: block ciphers and stream ciphers. Block ciphers are the encryption algorithms that divide input into blocks and encrypt each block separately by a sequence of permutation and substitution operations, whereas stream ciphers that can be considered as block ciphers with block size 1, encrypt the input by only binary addition. Most of the block ciphers process the data by iterations of rounds for which each round consists of a round function and a key schedule. Key schedule is the procedure that states each round key from the secret key, and each round key is integrated into the system by an XOR-operation which is a permutation operation. To protect the key, each round function includes substitution operations, e.g. S-boxes, so as to add confusion into the system. The properties of diffusion and confusion (defined in [26]) are the two properties each cipher should have for the security, and the property of diffusion is satisfied by the permutation operations. This thesis mainly focuses on S-boxes, and hence for more information about other parts, see [11, 29].

One example for the S-boxes is displayed in Fig. 1.1, which is a substitution-permutation network (SPN) taken from [8]. As can be seen from this figure, the only nonlinear part of the system is S-boxes, and thus the security of the system mainly depends on them. This requires the S-boxes to be cryptographically strong against any attack of the adversary. The known leading attacks against block ciphers are linear and differential attacks. The linear attack, publicized by [15], is based on high probability occurrences of the linear equations that are constructed by XORing of the bits of input, output and the key. On the other hand, the differential attack, introduced by [1], is based on high probability of certain occurrences of the input and output differences where if x

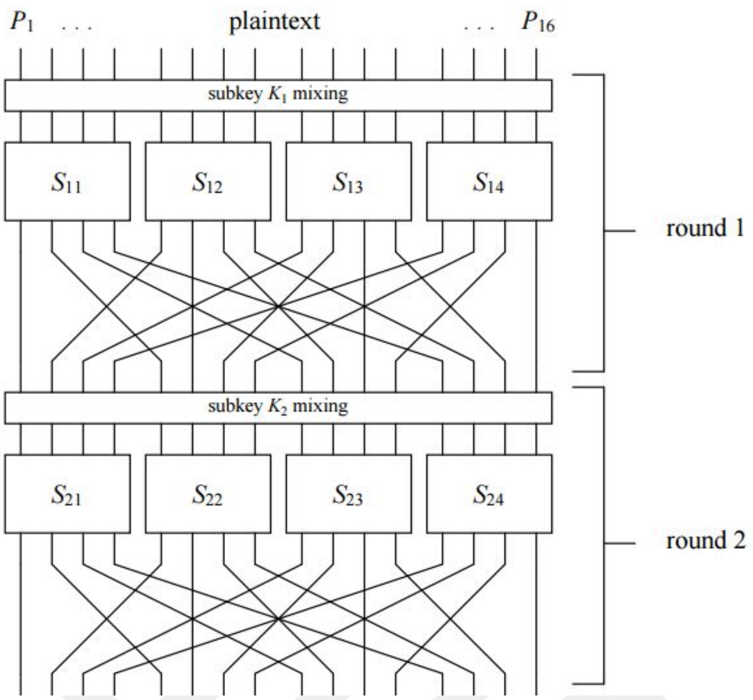

Figure 1.1: Two rounds of a basic substitution-permutation network (SPN)

and x' are two different inputs for a block cipher, then their difference is defined by $\Delta x = x \oplus x'$. As a result of these attacks, two design criteria for an S-box are specified as high nonlinearity and low differential uniformity. In addition to these attacks, the higher order differential attack [14] indicates that S-boxes should have high algebraic degree.

As being vectorial Boolean function in terms of mathematics, another criterion for an S-box is bijectivity, especially for SPN-typed block ciphers. It is clear that the set of inputs must meet with the set of outputs, and this function should have an inverse function in order to allow decryption. This requires one-to-one correspondence. To design a strong S-box, the S-box should meet all of the four criteria. One good example of such structure is the S-box of AES (Advanced Encryption Standard) which uses an irreducible polynomial over $\mathbb{F}_{2^8}$ while achieving the best possible trade-off in dimension 8, i.e. the nonlinearity 112, differential uniformity 4, and maximum possible algebraic degree 7. However, most of the S-boxes can not meet all these criteria. There are very few differentially 4-uniform bijective constructions with maximum nonlinearity. In fact, some of them have vulnerability to higher order differential attack due to the low algebraic degree.

Another attack, which depends on the hardware or software of the cryptosystem, is the side channel analysis (SCA) that can be mounted by the information leaked through its implementation such as the timing of operations [13], power consumption [12], and electromagnetic radiation [24]. Therefore, the resistance of cryptographic primitives against SCA attacks is of great importance as well. In this class of attacks, one of the most powerful is the differential power analysis (DPA) attack. In 2005, the DPA resistivity of an S-box was quantified [23] introducing the notion of transparency order (TO). A decade later, the definition of TO was modified [5] by taking the cross-correlation terms between the coordinate functions into account. In this thesis, the former definition [23] is used for the classification of S-boxes since its validity has been verified by several implementation results on cryptographic devices such as SASEBO-GII board [16, 17, 18] and ATmega163 smartcard [20, 21].

In this thesis, it is aimed to construct 6×6 bijective symmetric S-boxes under the permutation $\tau(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0, x_2, x_3, x_4, x_5, x_1)$. For this reason, an efficient exhaustive search algorithm which generates mentioned constructions with nonlinearity ≥ 24 (the best known nonlinearity among 6×6 S-boxes according to [6] is 24), and with the differential uniformity ≤ 4 is proposed. The motivation comes from the paper named by "Results on RSSBs" [9]. In this paper, all 6×6 symmetric S-boxes were classified up to the linear equivalence, and 11 different classes out of $6!$ classes (due to the $6!$ permutations) were obtained. Among these classes, the one of which the S-boxes are symmetric under the representative permutation $\sigma(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0, x_4, x_1, x_2, x_5, x_3)$ seems to be rich in terms of desirable cryptographic properties, since by heuristic search, it was found that there exist in this class highly nonlinear S-boxes with low differential uniformity. Furthermore, the S-boxes in this class are linearly equivalent to the symmetric S-boxes under the permutation $\tau(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0, x_2, x_3, x_4, x_5, x_1)$ by the Prop.13 of [9]. It is more easier to construct the latter class than the former one by interpreting the construction of the latter class as the concatenation of 5×5 rotation-symmetric S-boxes (RSSBs) due to the symmetry property of $\tau(S(x_0, x_1, ..., x_5)) = S(\tau(x_0, x_1, ..., x_5))$ for all $(x_0, x_1, ..., x_5) \in \mathbb{F}_2^6$. Hence, in this thesis all 6×6 bijective symmetric S-boxes under the permutation τ with nonlinearity ≥ 24 are generated in the search space of size $2^{61.28}$ and the differentially 4-uniform ones are classified with respect to absolute indicator, algebraic degree and transparency order.

The S-boxes of mentioned construction can be expressed in the form of $S = (f, S_1||S_2)$, where f is the 6-variable Boolean function corresponding to the first coordinate function of S, and S_1, S_2 are 5×5 RSSBs. To generate the S-boxes in this form, an efficient exhaustive search algorithm is used. This algorithm includes a three-step procedure that reduces the search space from $2^{61.28}$ to $2^{48.47}$. In the first step of the algorithm, all affine equivalent S-boxes of this construction are eliminated. In the second step, the RSSBs S_1's and S_2's that will never meet the requirement of nonlinearity condition, i.e. the ones having nonlinearity < 8 and the others for which the addition of Walsh spectra of the component functions of S_1 and S_2 will never be ≥ 24, are sieved. Consequently, in the final step all possible concatenations of the sets of S_1's and S_2's are extracted and the ones having nonlinearity < 24 are eliminated, and all possible coordinate functions f's are added to the remaining concatenations.

This thesis is organized as follows:

- In chapter 2, the preliminaries, which are divided into two sections as Boolean functions and S-boxes, are presented. These two sections are also partitioned into two subsections with respect to the rotation-symmetry and the concatenation.

- In chapter 3, the construction of $S = (f, S_1||S_2)$ is made in detail, where f is a 6-variable Boolean function and S_1, S_2 are 5×5 RSSBs.
- In chapter 4, the three steps of the efficient exhaustive search algorithm is proposed.
- The 5th chapter gives the results of the aforementioned search algorithm.
- Finally, the conclusion is made in chapter 6.

CHAPTER 2

PRELIMINARIES

2.1 Boolean functions

An n-variable *Boolean function* is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, where $\mathbb{F}_2$ is the finite field with two elements. The set of all n-variable Boolean functions is denoted by $\mathcal{F}_n$, and $|\mathcal{F}_n| = 2^{2^n}$.

Any Boolean function $f(x_1, ..., x_n)$ can be basically represented by a binary string of length 2^n such that

$$f = [f(0, 0, ..., 0), f(0, 0, ..., 1), \dots, f(1, 1, ..., 1)],$$

which is called the *truth table* of f. The weight of this binary string, i.e. the size of the support function $supp(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$ of f is called the *Hamming weight* of f, and it is denoted by $w_H(f)$. When f has equal number of 0's and 1's, i.e. $w_H(f) = 2^{n-1}$, we say that f is a *balanced* Boolean function.

The Boolean function f can also be represented uniquely as an n-variable polynomial over $\mathbb{F}_2$, which is called the *algebraic normal form (ANF)* of f,

$$f(x_1, x_2, ..., x_n) = a_0 + \sum_{I \subseteq \{1,...,n\}} a_I x^I,$$

where the monomial x^I is the product $x^I = \prod_{i \in I} x_i$, and $a_0, a_I \in \mathbb{F}_2$. The *algebraic degree* of f, denoted by $deg(f)$, is the highest degree of all the monomials in ANF of f, for which the degree of a monomial is the number of variables in that monomial. If the algebraic degree of f is at most 1, f is an *affine* function. The set of all n-variable affine functions is denoted by $\mathcal{A}_n$, and $|\mathcal{A}_n| = 2^{n+1}$. Moreover, if $a_0 = 0$, then f is a *linear* function.

The *Walsh-Hadamard transform* of f is an integer valued function over $\mathbb{F}_2^n$ which is defined as

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + w \cdot x},$$

where $w \in \mathbb{F}_2^n$ and the inner product $w \cdot x$ is over $\mathbb{F}_2$. Then, the string

$$W_f = [W_f(0, 0, ..., 0), W_f(0, 0, ..., 1), \dots, W_f(1, 1, ..., 1)]$$

is called the *Walsh spectrum* of f. A Boolean function f is balanced if and only if $W_f(0) = 0$.

The *nonlinearity* of f is the minimum distance to the set of all affine functions where the *distance* between two Boolean functions f and g is defined as $d(f, g) = w_H(f \oplus g)$. In terms of the Walsh transform, the nonlinearity is computed as

$$\begin{aligned} \mathcal{N}_f &= \min_{g \in \mathcal{A}_n} \{d(f, g)\} \\ &= \min_{w, x \in \mathbb{F}_2^n} \{d(f, w \cdot x), d(f, w \cdot x \oplus 1)\} \\ &= \min_{w, x \in \mathbb{F}_2^n} \{d(f, w \cdot x), (2^n - d(f, w \cdot x))\} \\ &= \min_{w \in \mathbb{F}_2^n} \{2^{n-1} - \frac{W_f(w)}{2}, 2^{n-1} + \frac{W_f(w)}{2}\} \\ &= 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} \{|W_f(w)|\}. \end{aligned}$$

If the Walsh spectrum of f consists of only the values $\pm 2^{n/2}$, i.e. if $W_f(w) = \pm 2^{n/2}$ for all $w \in \mathbb{F}_2^n$, we say that f is *bent*. In this case, the nonlinearity of f will be $\mathcal{N}_f = 2^{n-1} - 2^{n/2-1}$ (when n is even). Note that this is the maximum nonlinearity any n-variable Boolean function can have.

In Ex.2.1, the given cryptographic properties of a 3-variable Boolean function is examined.

Example 2.1. Let the truth table of a 3-variable Boolean function f be

$$f(x_1, x_2, x_3) = [1, 0, 1, 1, 0, 0, 0, 1].$$

Then, the Hamming weight of f is $w_H(f) = 4$. Since $w_H(f) = 2^2$, f is a balanced Boolean function. Using Butterfly Algorithm, the coefficients of algebraic normal form of f are computed in Tab.2.1. Thus, the polynomial representation of f is

$$f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_1 + x_3 + 1,$$

and $deg(f) = 2$. The Walsh spectrum of f is found as

$$W_f = [0, 0, 4, -4, -4, -4, 0, 0],$$

after the Walsh transform of f for all $w \in \mathbb{F}_2^3$ is computed. To illustrate for $w = (0, 1, 1)$,

$$\begin{aligned} W_f(0,1,1) = \sum_{x \in \mathbb{F}_2^3} (-1)^{f(x)+((0,1,1)\cdot x)} &= \sum_{x \in \mathbb{F}_2^3} (-1)^{f(x)} (-1)^{x_2 \oplus x_3} \\ &= -1 - 1 + 1 - 1 + 1 - 1 - 1 - 1 = -4, \end{aligned}$$

which corresponds to 4th value of the Walsh spectrum. The nonlinearity of f, then, is computed as $\mathcal{N}_f = 2^2 - \frac{1}{2} \cdot 4 = 2$ since the maximum value of the absolute of the Walsh spectrum is 4. Also, observing the values of Walsh spectrum, it is concluded that f is not bent.

Table 2.1: Finding coefficients of ANF of f using Butterfly Algorithm

$\boldsymbol{x}$	$\boldsymbol{f}$	**Step 1**	$\boldsymbol{A_1}$	**Step 2**	$\boldsymbol{A_2}$	**Step 3**	$\boldsymbol{A_3}$
000	1	$\rightarrow$	1	$\rightarrow$	1	$\rightarrow$	1
001	0	$\searrow$	1	$\rightarrow$	1	$\rightarrow$	1
010	1	$\rightarrow$	1	$\searrow$	0	$\rightarrow$	0
011	1	$\searrow$	0	$\searrow$	1	$\rightarrow$	1
100	0	$\rightarrow$	0	$\rightarrow$	0	$\searrow$	1
101	0	$\searrow$	0	$\rightarrow$	0	$\searrow$	1
110	0	$\rightarrow$	0	$\searrow$	0	$\searrow$	0
111	1	$\searrow$	1	$\searrow$	1	$\searrow$	0

The *correlation* between any two Boolean functions $f, g \in \mathbb{F}_2^n$ is the degree of similarity of these two functions, which can be defined as

$$C_{f,g} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)}(-1)^{g(x)},$$

and $-2^n \leq C_{f,g} \leq 2^n$. The *auto-correlation* of f, in this case, the degree of the similarity between the output and subsets of inputs of f, which can be described as

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

where $d \in \mathbb{F}_2^n$. Among all nonzero $d \in \mathbb{F}_2^n$, the maximum of the absolute of $\Delta_f(d)$ is called the *absolute indicator* of f [30], and it is denoted by simply Δ_f.

The Boolean function f is *correlation immune of order m* [27] if and only if $W_f(w) = 0$ for all $w \in \mathbb{F}_2^n$ such that $1 \leq w_H(w) \leq m$. This means that the output of f and any m input variables are statistically independent. If f is also a balanced function, then it is called *m-resilient*.

Any Boolean function $f \in \mathbb{F}_2^n$ is *symmetric* [3] if $f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$ for all permutations σ of $\{1, 2, ..., n\}$.

2.1.1 Rotation-symmetric Boolean functions

There is a class in $\mathcal{F}_n$ whose elements are invariant under some permutations of $\{1, 2, ..., n\}$, which is called *rotation-symmetric* Boolean functions (RSBFs). For this class, the operator which determines these permutations is defined on $\mathbb{F}_2^n$ as

$$\rho^k(x_i) = \begin{cases} x_{i+k}, & \text{if } i + k \leq n \\ x_{i+k-n}, & \text{if } i + k > n \end{cases},$$

and it is called k-th cyclic shift operator. Under this operation, any Boolean function f is said to be *rotation-symmetric* if $f(\rho^k(x_1, x_2, ..., x_n)) = f(x_1, x_2, ..., x_n)$ for all $(x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$, and for any $1 \leq k \leq n$.

Table 2.2: The list of all 3-variable RSBFs

x	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
000	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
001	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
010	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
011	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
100	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
101	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
110	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
111	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

According to this definition, it is observed that the cyclic shift operator divides the set of inputs into partitions so that each partition consists of all cyclic rotations of any input. For example, if k is chosen to be equal to 1, then for any $(x_1, x_2, ..., x_n)$ this partition is determined in such a way that:

- $f(\rho^1(x_1, x_2, ..., x_n)) = f(x_2, ..., x_n, x_1) = f(x_1, x_2, ..., x_n)$,
- $f(\rho^1(x_2, ..., x_n, x_1)) = f(x_3, ..., x_1, x_2) = f(x_2, ..., x_n, x_1) = f(x_1, x_2, ..., x_n)$,
- $f(\rho^1(x_3, ..., x_1, x_2)) = f(x_4, ..., x_2, x_3) = f(x_3, ..., x_1, x_2) = f(x_2, ..., x_n, x_1)$

  $= f(x_1, x_2, ..., x_n)$,

$$\vdots$$

- $f(\rho^1(x_n, x_1, ..., x_{n-1})) = f(x_1, x_2, ..., x_n) = f(x_n, x_1, ..., x_{n-1})$

  $= f(x_{n-1}, x_n, ..., x_{n-2}) = \ldots = f(x_2, ..., x_n, x_1)$.

$$\Longrightarrow \{(x_1, x_2, ..., x_n), (x_2, ..., x_n, x_1), ..., (x_n, x_1, ..., x_{n-1})\}$$

As the one above, these partitions are called *orbits* and each orbit is generated by

$$G_n(x_1, x_2, ..., x_n) = \{\rho^k(x_1, x_2, ..., x_n) \mid 1 \leq k \leq n\}.$$

The number of such partitions, denoted by g_n, is found as $\frac{1}{n}\sum_{t/n}\phi(t)2^{n/t}(\approx \frac{2^n}{n})$ [28], using Burnside's Lemma.

The lexicographically first element in each orbit, denoted by Λ_i for $i = 1, 2, ..., g_n$ is called the *representative* element of that orbit. As can be seen, any RSBF f takes the same value for all elements in each orbit. Since there are g_n orbits in $\mathbb{F}_2^n$, the set of RSBFs consists of 2^{g_n} Boolean functions. In Ex.2.2, the orbits of $\mathbb{F}_2^3$ are found, and in Tab.2.2, all RSBFs in that field are listed.

Table 2.3: The permutations of $\{x_1, x_2, x_3\}$

All permutations	**Permutations for RSBFs**
$\sigma_1(x_1, x_2, x_3) = (x_1, x_2, x_3)$	$\rho^1(x_1, x_2, x_3) = (x_2, x_3, x_1)$
$\sigma_2(x_1, x_2, x_3) = (x_1, x_3, x_2)$	$\rho^2(x_1, x_2, x_3) = (x_3, x_1, x_2)$
$\sigma_3(x_1, x_2, x_3) = (x_2, x_1, x_3)$	$\rho^3(x_1, x_2, x_3) = (x_1, x_2, x_3)$
$\sigma_4(x_1, x_2, x_3) = (x_2, x_3, x_1)$	
$\sigma_5(x_1, x_2, x_3) = (x_3, x_1, x_2)$	
$\sigma_6(x_1, x_2, x_3) = (x_3, x_2, x_1)$	

Table 2.4: The permutations σ_2, σ_3 and σ_6 for all $(x_1, x_2, x_3) \in \mathbb{F}_2^3$

The permutation $\boldsymbol{\sigma_2}$	**The permutation $\boldsymbol{\sigma_3}$**	**The permutation $\boldsymbol{\sigma_6}$**
$\sigma_2(0,0,0) = (0,0,0)$	$\sigma_3(0,0,0) = (0,0,0)$	$\sigma_6(0,0,0) = (0,0,0)$
$\sigma_2(0,0,1) = (0,1,0)$	$\sigma_3(0,0,1) = (0,0,1)$	$\sigma_6(0,0,1) = (1,0,0)$
$\sigma_2(0,1,0) = (0,0,1)$	$\sigma_3(0,1,0) = (1,0,0)$	$\sigma_6(0,1,0) = (0,1,0)$
$\sigma_2(0,1,1) = (0,1,1)$	$\sigma_3(0,1,1) = (1,0,1)$	$\sigma_6(0,1,1) = (1,1,0)$
$\sigma_2(1,0,0) = (1,0,0)$	$\sigma_3(1,0,0) = (0,1,0)$	$\sigma_6(1,0,0) = (0,0,1)$
$\sigma_2(1,0,1) = (1,1,0)$	$\sigma_3(1,0,1) = (0,1,1)$	$\sigma_6(1,0,1) = (1,0,1)$
$\sigma_2(1,1,0) = (1,0,1)$	$\sigma_3(1,1,0) = (1,1,0)$	$\sigma_6(1,1,0) = (0,1,1)$
$\sigma_2(1,1,1) = (1,1,1)$	$\sigma_3(1,1,1) = (1,1,1)$	$\sigma_6(1,1,1) = (1,1,1)$

Example 2.2. There are 4 orbits in $\mathbb{F}_2^3$ such that:

$$\begin{aligned} G_3(0,0,0) &= \{(0,0,0)\}, \\ G_3(0,0,1) = G_3(0,1,0) = G_3(1,0,0) &= \{(0,0,1),(0,1,0),(1,0,0)\}, \\ G_3(0,1,1) = G_3(1,1,0) = G_3(1,0,1) &= \{(0,1,1),(1,1,0),(1,0,1)\}, \\ G_3(1,1,1) &= \{(1,1,1)\}. \end{aligned}$$

This implies that if $f(0,0,1) = f(0,1,0) = f(1,0,0)$ and $f(0,1,1) = f(1,1,0) = f(1,0,1)$ for any $f \in \mathbb{F}_2^3$, then f is rotation-symmetric. There are 2^4 RSBFs in $\mathbb{F}_2^3$ listed in Tab.2.2.

Lemma 2.1. *Every symmetric Boolean function is rotation-symmetric.*

Proof. This fact is clear since the permutations $\rho^1, \rho^2, ..., \rho^n$ belong to the set of permutations of $\{x_1, x_2, ..., x_n\}$. □

Note that there are 6 permutations of $\{x_1, x_2, x_3\}$ and 3 of them help to form rotation-symmetric Boolean functions in $\mathcal{F}_3$. It can be seen from Tab.2.3 that $\rho^1 = \sigma_4$, $\rho^2 = \sigma_5$, and $\rho^3 = \sigma_1$. From the point of symmetry, the permutations of RSBFs do not violate the permutations of σ_2, σ_3, and σ_6 since the field $\mathbb{F}_2$ consists of only two elements. This fact is presented in Tab.2.4. As a result, the permutations that contributes symmetry and rotation-symmetry to Boolean functions generate the same set of Boolean functions. In other words, the Boolean functions in Tab.2.2 are symmetric as well as being rotation-symmetric.

Corollary 2.2. *All rotation-symmetric Boolean functions in $\mathcal{F}_3$ are also symmetric.*

However, this result is valid only for $n = 3$. The set of rotation-symmetric Boolean functions is a larger set as it includes the set of symmetric Boolean functions for $n > 3$. The example of a 4-variable Boolean function which is not symmetric but rotation-symmetric is presented below.

Example 2.3. There are 6 orbits in $\mathbb{F}_2^4$ such that:

$$\begin{aligned}
G_4(0,0,0,0) &= \{(0,0,0,0)\},\\
G_4(0,0,0,1) &= \{(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0)\},\\
G_4(0,0,1,1) &= \{(0,0,1,1),(0,1,1,0),(1,1,0,0),(1,0,0,1)\},\\
G_4(0,1,0,1) &= \{(0,1,0,1),(1,0,1,0)\},\\
G_4(0,1,1,1) &= \{(0,1,1,1),(1,1,1,0),(1,1,0,1),(1,0,1,1)\},\\
G_4(1,1,1,1) &= \{(1,1,1,1)\}.
\end{aligned}$$

With respect to these, the output of a 4-variable RSBF f should be the same for the inputs belonging the same orbits. Let the truth table of f be

$$f = [0,0,0,1,0,0,1,0,0,1,0,0,1,0,0,0].$$

Clearly, f is a RSBF since $f(0,0,1,1) = f(0,1,1,0) = f(1,1,0,0) = f(1,0,0,1) = 1$ and for the rest of the inputs $f = 0$. From its truth table, the ANF of f can be found as

$$f(x_1,x_2,x_3,x_4) = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_4.$$

Now, take the permutation $\sigma(x_1,x_2,x_3,x_4) = (x_1,x_2,x_4,x_3)$. Then,

$$\begin{aligned}
f(\sigma(x_1,x_2,x_3,x_4)) = f(x_1,x_2,x_4,x_3) &= x_1x_2 + x_2x_4 + x_1x_3 + x_3x_4\\
&\neq f(x_1,x_2,x_3,x_4).
\end{aligned}$$

Hence, f is not symmetric, although it is rotation-symmetric.

2.1.2 Concatenation of Boolean Functions

An $(n+1)$-variable Boolean function f can be constructed by the *concatenation* of two n-variable Boolean functions g and h. In this case, f can be defined as

$$f(x_0,x_1,...,x_n) = \begin{cases} g(x_1,x_2,...,x_n), & \text{if } x_0 = 0\\ h(x_1,x_2,...,x_n), & \text{if } x_0 = 1 \end{cases},$$

for all $(x_0,x_1,...,x_n) \in \mathbb{F}_2^{n+1}$. In notation, f is shown by $f = g||h$.

The Walsh values of f can be computed directly from the Walsh values of g and h:

$$W_f(w_0, w_1, ..., w_n) = \begin{cases} (W_g + W_h)(w_1, w_2, ..., w_n), & \text{if } w_0 = 0 \\ (W_g - W_h)(w_1, w_2, ..., w_n), & \text{if } w_0 = 1 \end{cases},$$

for all $(w_0, w_1, ..., w_n) \in \mathbb{F}_2^{n+1}$. This result can be observed by the last step of the algorithm of Fast Walsh-Hadamard Transform. Consequently, the Walsh spectrum of f is

$$W_f = [W_g + W_h,\ W_g - W_h],$$

where W_g and W_h are the Walsh spectra of g and h, respectively.

Notice that

$$\begin{aligned} \max_{w \in \mathbb{F}_2^{n+1}} \{|W_f(w)|\} &= \max_{u \in \mathbb{F}_2^n} \{|(W_g + W_h)(u)|\} \\ &= \max_{u \in \mathbb{F}_2^n} \{|W_g(u)| + |W_h(u)|\}. \end{aligned}$$

Then, the nonlinearity of f is equal to

$$\begin{aligned} \mathcal{N}_f &= 2^n - \frac{1}{2} \max_{w \in \mathbb{F}_2^{n+1}} \{|W_f(w)|\} \\ &= 2^n - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} \{|W_g(u)| + |W_h(u)|\}. \end{aligned}$$

Here, if the nonlinearity of f is bounded greater than $\alpha \in \mathbb{Z}$, then the relation between nonlinearity of f and the nonlinearities of g and h is presented below:

$$\begin{aligned} \mathcal{N}_f \geq \alpha &\implies 2^n - \frac{1}{2}\left(\max_{w \in \mathbb{F}_2^{n+1}} \{|W_f(w)|\} \right) \geq \alpha \\ &\implies 2^{n+1} - 2\alpha \geq \max_{w \in \mathbb{F}_2^{n+1}} \{|W_f(w)|\} \\ &\implies \max_{u \in \mathbb{F}_2^n} \{|W_g(u)| + |W_h(u)|\} \leq 2^{n+1} - 2\alpha \\ &\implies \max_{u \in \mathbb{F}_2^n} \{|W_g(u)|\},\ \max_{v \in \mathbb{F}_2^n} \{|W_h(v)|\} \leq 2^{n+1} - 2\alpha \\ &\implies \mathcal{N}_g, \mathcal{N}_h \geq 2^{n-1} - 2^n + \alpha. \end{aligned}$$

Proposition 2.3. *Let $f : \mathbb{F}_2^{n+1} \to \mathbb{F}_2$ be an $(n+1)$-variable Boolean function constructed by the concatenation of two n-variable Boolean functions g and h. Then, the Walsh spectrum of f will be*

$$W_f = [W_g + W_h,\ W_g - W_h],$$

where W_g and W_h are the Walsh spectra of g and h, respectively. If $\max_w\{|W_f(w)|\}$ for $w \in \mathbb{F}_2^{n+1}$ is bounded by $\beta_f \in \mathbb{Z}$, then the nonlinearities of g and h will be bounded below

$$\mathcal{N}_g, \mathcal{N}_h \geq 2^{n-1} - \frac{1}{2}\beta_f.$$

Proof. Let $f : \mathbb{F}_2^{n+1} \to \mathbb{F}_2$, $f = g||h$, and $W_f = [W_g + W_h,\ W_g - W_h]$. Clearly,

$$\max_{w \in \mathbb{F}_2^{n+1}} \{|W_f(w)|\} = \max_{u \in \mathbb{F}_2^n} \{|W_g(u)| + |W_h(u)|\}.$$

Then, the restriction of the maximum Walsh value of f with $\beta_f \in \mathbb{Z}$ implies:

$$\begin{aligned} \max_{w \in \mathbb{F}_2^{n+1}} \{|W_f(w)|\} \leq \beta_f \quad &\Longrightarrow \quad \max_{u \in \mathbb{F}_2^n} \{|W_g(u)|\},\ \max_{v \in \mathbb{F}_2^n} \{|W_h(v)|\} \leq \beta_f \\ &\Longrightarrow \quad \mathcal{N}_g, \mathcal{N}_h \geq 2^{n-1} - \frac{1}{2}\beta_f. \end{aligned}$$

□

2.2 S-boxes

An $n \times m$ *S-box* is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, where $\mathbb{F}_2$ is the finite field with two elements. To obtain a bijective (invertible) mapping, m should be chosen to be equal to n. Moreover, any $n \times m$ S-box S can be represented as a combination of Boolean functions such that

$$S(x) = (f_1(x), f_2(x), \ldots, f_m(x)),$$

where the functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ for $i = 1, 2, ..., m$ are called the *coordinate* functions. Any linear combination $c \cdot S(x)$ of the coordinate functions with non-zero *coefficient* vector $c \in \mathbb{F}_2^{m*}$ are called the *component* functions. Now, the cryptographic properties of Boolean functions can be extended to S-boxes via the component functions.

The *Walsh-Hadamard transform* of S is an even integer-valued function $W_S : \mathbb{F}_2^n \times \mathbb{F}_2^{m*} \to [-2^n, 2^n]$ which can be formulated by

$$W_S(w, c) = \sum_{x \in \mathbb{F}_2^n} (-1)^{c \cdot S(x) + w \cdot x},$$

where $w \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2^{m*}$, and the inner product is over $\mathbb{F}_2$. Then, the Walsh spectrum of S can be interpreted as an $2^n \times (2^m - 1)$-matrix such that each entry corresponds to one Walsh value and each column corresponds to the Walsh spectrum of one of the component functions. Note that these Walsh spectra of the component functions are alined lexicographically to this matrix. In simple terms this matrix can be indicated as

$$\begin{aligned} W_S &= [W_S(w, (0, 0, ..., 1)), W_S(w, (0, ..., 1, 0)), \ldots, W_S(w, (1, 1, ..., 1)] \\ &= [W_{f_m}, W_{f_{m-1}}, \ldots, W_{f_1 \oplus f_2 \oplus \ldots \oplus f_m}]. \end{aligned}$$

The *nonlinearity* $\mathcal{N}_S$ of S is defined as the worst case nonlinearity among the nonlinearities of the component functions, that is,

$$\begin{aligned}\mathcal{N}_S &= \min_{c\in\mathbb{F}_2^{m*}} \{\mathcal{N}_{c\cdot S(x)}\} \\ &= \min_{c\in\mathbb{F}_2^{m*}} \left\{2^{n-1} - \frac{1}{2}\max_{w\in\mathbb{F}_2^n}\{|W_S(w,c)|\}\right\} \\ &= 2^{n-1} - \frac{1}{2}\max_{\substack{w\in\mathbb{F}_2^n,\\ c\in\mathbb{F}_2^{m*}}}\{|W_S(w,c)|\},\end{aligned}$$

where $\mathcal{N}_{c\cdot S(x)}$ is the nonlinearity of the component function $c \cdot S(x)$.

The two notions of the *algebraic degree* of S [4] are the maximum degree of the coordinate functions and the minimum degree of the component functions, which are denoted by $d_{\max}$ and $d_{\min}$, respectively. The degree of any component (or coordinate) function can be computed using its algebraic normal form (ANF). Note that ANF of any Boolean function was formerly defined in the first section.

In Ex.2.4, an 3×3 S-box is examined in terms of Walsh spectrum, nonlinearity, and algebraic degree ($d_{\min}$).

Example 2.4. Let $S(x) = (f_1(x), f_2(x), f_3(x))$ be an 3×3 S-box defined from $\mathbb{F}_2^3$ to $\mathbb{F}_2^3$ where the truth tables of the coefficient vectors are $f_1 = [0,1,0,1,1,1,0,0]$, $f_2 = [1,0,0,1,1,0,1,0]$, and $f_3 = [1,0,0,1,0,1,0,1]$. Observe that 7 component functions for $2^3 - 1 = 7$ different coefficient vectors are computed similarly as in the case of $c = (1,0,1)$:

$$\begin{aligned}(1,0,1)\cdot S(x) &= (1,0,1)\cdot(f_1(x),f_2(x),f_3(x)) = (f_1 \oplus f_3)(x) \\ &\implies f_1 \oplus f_3 = [1,1,0,0,1,0,0,1].\end{aligned}$$

In Tab.2.5, the S-box S and its all component functions are presented. The Walsh values of the component functions of S are computed using the transform $W_S(w,c)$. For example, the Walsh value of the component function $(f_1 \oplus f_3)(x)$ at $w = (0,0,1)$ is

$$\begin{aligned}W_S((0,0,1),(1,0,1)) &= \sum_{x\in\mathbb{F}_2^3} (-1)^{(1,0,1)\cdot S(x)}(-1)^{(0,0,1)\cdot x} \\ &= \sum_{x\in\mathbb{F}_2^3} (-1)^{(f_1\oplus f_3)(x)}(-1)^{x_3} \\ &= -1+1+1-1-1-1+1+1 = 0.\end{aligned}$$

After the computation of all Walsh values, the 8×7-matrix of Walsh spectra of the 7 component functions is formed as

$$W_S = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & -4 & 0 & 4 & 0 & 0 & 4 \\ 0 & 0 & 0 & -4 & -4 & -4 & 4 \\ -4 & -4 & 0 & 0 & -4 & 4 & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 & 0 \\ -4 & 4 & 0 & 4 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 & -4 & -4 & -4 \\ -4 & -4 & 0 & 0 & 4 & -4 & 0 \end{bmatrix},$$

where the first column corresponds to the lexicographically first coefficient vector $c = (0,0,1)$. As can be seen, the maximum of the absolute Walsh values of 6 component functions is 4, while one of them is 8. Therefore,

$$\begin{aligned} \mathcal{N}_{f_1} = \mathcal{N}_{f_2} = \mathcal{N}_{f_3} = \mathcal{N}_{f_1 \oplus f_2} = \mathcal{N}_{f_1 \oplus f_3} = \mathcal{N}_{f_1 \oplus f_2 \oplus f_3} &= 2^2 - \frac{1}{2} \cdot 4 = 2, \\ \mathcal{N}_{f_2 \oplus f_3} &= 2^2 - \frac{1}{2} \cdot 8 = 0, \end{aligned}$$

and this implies that $\mathcal{N}_S = \min\{0, 2\} = 0$. Using Butterfly Algorithm, the ANF of the component functions can be found as

$$\begin{aligned} f_1(x_1,x_2,x_3) = x_1x_2 + x_1x_3 + x_1 + x_3 &\implies deg(f_1) = 2, \\ f_2(x_1,x_2,x_3) = x_1x_2 + x_2 + x_3 + 1 &\implies deg(f_2) = 2, \\ f_3(x_1,x_2,x_3) = x_1x_3 + x_2 + 1 &\implies deg(f_3) = 2, \\ (f_1 \oplus f_2)(x_1,x_2,x_3) = x_1x_3 + x_1 + x_2 + 1 &\implies deg(f_1 \oplus f_2) = 2, \\ (f_1 \oplus f_3)(x_1,x_2,x_3) = x_1x_3 + x_2 + 1 &\implies deg(f_1 \oplus f_3) = 2, \\ (f_2 \oplus f_3)(x_1,x_2,x_3) = x_1 &\implies deg(f_2 \oplus f_3) = 1, \\ (f_1 \oplus f_2 \oplus f_3)(x_1,x_2,x_3) = x_1x_2 + x_1x_3 + x_3 &\implies deg(f_1 \oplus f_2 \oplus f_3) = 2. \end{aligned}$$

According to this, the minimum algebraic degree belongs to the polynomial $(f_2 \oplus f_3)(x_1,x_2,x_3)$, and it is equal to 1. This shows that the algebraic degree of the S-box, $d_{\min}$, is also 1.

The *auto-correlation* function can also be defined for the S-boxes as

$$\Delta_S(d,c) = \sum_{x \in \mathbb{F}_2^n} (-1)^{c \cdot S(x)} (-1)^{c \cdot S(x \oplus d)},$$

where $d \in \mathbb{F}_2^n$. Among all nonzero $d \in \mathbb{F}_2^n$, except the point $(\mathbf{0},\mathbf{0})$, the maximum of the absolute of $\Delta_S(d,c)$ is called the *absolute indicator* of S, and it is denoted by simply Δ_S. Note that $\mathbf{0}$ denotes all-zero vector.

Table 2.5: The S-box S in Ex.2.4 and its component functions

x	$S(x)$	f_3	f_2	$f_2 \oplus f_3$	f_1	$f_1 \oplus f_3$	$f_1 \oplus f_2$	$f_1 \oplus f_2 \oplus f_3$
000	011	1	1	0	0	1	1	0
001	100	0	0	0	1	1	1	1
010	000	0	0	0	0	0	0	0
011	111	1	1	0	1	0	0	1
100	110	0	1	1	1	1	0	0
101	101	1	0	1	1	0	1	0
110	010	0	1	1	0	0	1	1
111	001	1	0	1	0	1	0	1

The *differential uniformity* δ_S [19] of S is defined as the maximum number of solutions of the equation $S(x) \oplus S(x \oplus \alpha) = \beta$ for all $\alpha \in \mathbb{F}_2^n$, $\alpha \neq \mathbf{0}$ and $\beta \in \mathbb{F}_2^m$. In other words, if

$$|\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \alpha) = \beta\}| \leq \delta_S,$$

for all $\alpha \in \mathbb{F}_2^{n*}$ and $\beta \in \mathbb{F}_2^m$, then S is called differentially δ-uniform.

The *transparency order (TO)* is described in [5], which is the simplified version of the original definition in [23], as the quantifier of the resistance of S to DPA attacks. It is formulated by

$$\gamma_S = m - \frac{1}{2^{2n} - 2^n} \sum_{d \in \mathbb{F}_2^{n*}} \left| \sum_{\substack{c \in \mathbb{F}_2^m, \\ w_H(c)=1}} \Delta_S(d, c) \right|,$$

where $w_H(c)$ denotes the Hamming weight of the coefficient vector c and $\Delta_S(d, c)$ denotes the auto-correlation function of S.

2.2.1 Rotation-symmetric S-boxes

In this section, the concept of the rotation-symmetric Boolean functions is extended to S-boxes. Let S be an $n \times m$ S-box from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. If S satisfies the equation

$$\rho^k(S(x)) = S(\rho^k(x)) \text{ for all } x = (x_1, x_2, ..., x_n) \in \mathbb{F}_2^n,$$

and for any $1 \leq k \leq n$ where ρ^k is the k-th cyclic shift operator defined in Sec.2.1.1, then S is called *rotation-symmetric*. Moreover, S is called *k-rotation-symmetric* [9] if it satisfies this equation only for k's, where k divides n.

In this definition, if $gcd(n, m) = 1$, this means that the outputs of the S-box comprise of only all-zero and all-one vectors. Otherwise if $gcd(n, m) \neq 1$, the orbits of the input field $\mathbb{F}_2^n$ should be matched with the orbits of the output field $\mathbb{F}_2^m$ such that the size of the output orbit should divide the size of the corresponding orbit of the input field.

Table 2.6: The examples of S-boxes about rotation-symmetry

$\boldsymbol{x}$	$\boldsymbol{S_1(x)}$	$\boldsymbol{x}$	$\boldsymbol{S_2(x)}$	$\boldsymbol{x}$	$\boldsymbol{S_3(x)}$	$\boldsymbol{x}$	$\boldsymbol{S_4(x)}$
000	00	000	111	00	0000	00	1111
001	00	001	101	01	0101	01	0001
010	11	010	011	10	1010	10	0010
011	00	011	001	11	1111	11	0000
100	00	100	110				
101	11	101	100				
110	11	110	010				
111	11	111	000				

Lemma 2.4. *Let S be an $n \times m$ S-box from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ such that $gcd(n, m) = 1$. Then, S is rotation-symmetric if the output of S only consists of all-zero or all-one vectors.*

Proof. For the simplicity, take $m = 2$, and let n be any odd integer. Clearly, $gcd(n, m)$ $= 1$. Then, S can be defined as $S(x_1, x_2, ..., x_n) = (y_1, y_2)$ where $(x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$ and $(y_1, y_2) \in \mathbb{F}_2^2$. Assume that S is rotation-symmetric. This implies that

$$\rho^k(S(x_1, x_2, ..., x_n)) = \rho^k(y_1, y_2) = S(\rho^k(x_1, x_2, ..., x_n)),$$

for all $(x_1, x_2, ..., x_n)$, and for any $1 \leq k \leq n$. If $k = 1$, then

$$\rho^1(S(x_n, x_1, ..., x_{n-1})) = S(\rho^1(x_n, x_1, ..., x_{n-1}))$$

$$\begin{aligned} &\Longrightarrow \quad \rho^1(y_1, y_2) = S(x_1, x_2, ..., x_n) \\ &\Longrightarrow \quad (y_2, y_1) = (y_1, y_2) \\ &\Longrightarrow \quad y_1 = y_2. \end{aligned}$$

Here, $S(x_n, x_1, ..., x_{n-1}) = (y_1, y_2)$ since n is odd. Similarly if $k = 2$, then

$$\rho^2(S(x_{n-1}, x_n, ..., x_{n-2})) = S(\rho^2(x_{n-1}, x_n, ..., x_{n-2}))$$

implies that $y_1 = y_2$. Maintaining the same procedure for the other cases, it is stated that $y_1 = y_2$, for any $1 \leq k \leq n$. Hence, the output of S can only be $(0, 0)$ or $(1, 1)$ in $\mathbb{F}_2^2$. □

Three examples of rotation-symmetric S-boxes, and one example of S-box which is not rotation-symmetric are presented in Tab.2.6. S_4 is not rotation-symmetric because the size of the orbit generated by $G_4(0, 0, 0, 1)$ is equal to 4, while the one of $G_2(0, 1)$ is 2. To be more clear, if the inputs of S_4 are rotated once, the third vector of S_4 will be $(0, 0, 0, 1)$, but $(0, 0, 0, 1) \neq \rho^1(S(1, 0))$ which is $(0, 1, 0, 0)$. This situation holds also for $k = 2$. However, in S_3 the condition of rotation-symmetry is satisfied for both $k = 1, 2$ since both of the sizes of the orbits generated by $G_2(0, 1)$ and $G_4(0, 1, 0, 1)$

are 2. Moreover, S_1 is an example of first case of $gcd(3, 2) = 1$, and S_2 is an example to 3×3 bijective rotation-symmetric S-boxes.

The number of the rotation-symmetric $n \times m$ S-boxes changes according to the conditions that n and m generate. However, for the bijective ones this number can be found easily, as proposed in [9]. The adapted form of this proposition is below:

Proposition 2.5. *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an $n \times n$ bijective S-box which is symmetric under the action of a permutation group. If the size of the output orbits is denoted by s, and the number of the orbits having the same size s is represented by t, the number of such S-boxes can be found by the formula*

$$\prod_{i=1}^{d} t_i! s_i^{t_i},$$

where d is the number of distinct orbit sizes.

For an application of this proposition, take $n = 3$. As in Ex.2.2, there are 4 orbits in $\mathbb{F}_2^3$ that two of them have size 1, and other two have size 3. With respect to these information, $d = 2$. Thus, there exist $(2! \cdot 1^2) \cdot (2! \cdot 3^2) = 36$ bijective rotation-symmetric S-boxes for $n = 3$. On the other hand, for the verification of this number observe that the input orbits can match with the output orbits that both of the orbits have the same size, since the S-box is bijective. Therefore, $G_3(0, 0, 0)$ can match with itself or with $G_3(1, 1, 1)$. After it matches, the output vector of $G_3(1, 1, 1)$ can be automatically placed. This makes 2! placements. Similarly, for the output orbit choice of $G_3(0, 0, 1)$ there are two options, and after the choice of the output orbit, the decision of which orbit elements will be the output of $(0, 0, 1)$ leads to 3 options. Then, the outputs of 1 and 2-rotation of this vector can be automatically placed. In a similar way, there are 3 options for $(0, 1, 1)$. This makes $2! \cdot 2! \cdot \binom{3}{1} \cdot \binom{3}{1} = 36$ ways to replace all vectors of $\mathbb{F}_2^3$ in a way that the resultant S-box is bijective and rotation-symmetric.

Let S be an $n \times n$ bijective rotation-symmetric S-box satisfying the condition

$$\rho^k(S(x)) = S(\rho^k(x)) \text{ for all } x = (x_1, x_2, ..., x_n) \in \mathbb{F}_2^n,$$

and for any $1 \leq k \leq n$. Then, there are g_n orbits partitioning the vector space of $\mathbb{F}_2^n$. Recall that the lexicographically first element of each orbit is denoted by Λ_i for $i = 1, 2, .., g_n$. Then, each orbit is generated by $G_n(\Lambda_i) = \{\rho^k(\Lambda_i) \mid 1 \leq k \leq n\}$. As aforementioned, for the two different orbit representatives Λ_i and Λ_j,

$$S(\Lambda_i) = \rho^l(\Lambda_j) \text{ for } 1 \leq l \leq n \text{ if and only if } |G_n(\Lambda_i)| = |G_n(\Lambda_j)|.$$

The bijectivity of S does not let the output of any orbit representative to be all-zero or all-one unless $|G_n(\Lambda_i)| = 1$. Also, after the match-up of $S(\Lambda_i) = \rho^l(\Lambda_j)$, the outputs of the rotations of Λ_i automatically match with the rotations of $\rho^l(\Lambda_j)$. For instance, if

$$|G_n(\Lambda_i)| = a \implies S(\rho^b(\Lambda_i)) = \rho^{b+l}(\Lambda_j) \text{ for all } 1 \leq b \leq a.$$

Thus, the S-box S can be expressed in terms of the orbit representatives such that

$$S(\Lambda_1, \Lambda_2, \ldots, \Lambda_{g_n}) = (\rho^{l_1}(\Lambda_{j_1}), \rho^{l_2}(\Lambda_{j_2}), \ldots, \rho^{l_{g_n}}(\Lambda_{j_{g_n}})),$$

for $1 \leq l_1, ..., l_{g_n} \leq n$, and $j_1, j_2, ..., j_{g_n} \in \{1, 2, ..., g_n\}$ with $j_1 \neq j_2 \neq ... \neq j_{g_n}$.

2.2.2 Concatenations of S-boxes

If the case of *concatenation of S-boxes* is considered, it is to obtain an $(n+1) \times n$ S-box constructed by the concatenation of two $n \times n$ S-boxes S_1 and S_2. In this case, the concatenation F can be described as

$$F(x_0; x) = \begin{cases} S_1(x), & \text{if } x_0 = 0 \\ S_2(x), & \text{if } x_0 = 1 \end{cases},$$

for all $(x_0; x) = (x_0, x_1, ..., x_n) \in \mathbb{F}_2^{n+1}$. In other description,

$$F(x_0; x) = (x_0 \oplus 1)S_1(x) + x_0 S_2(x),$$

for all $(x_0; x) \in \mathbb{F}_2^{n+1}$. In notation, F is shown by $F = S_1 || S_2$. As mentioned before, any S-box can be represented by its coordinate functions. Let

$$S_1(x) = (f_1(x), f_2(x), ..., f_n(x)) \text{ and } S_2(x) = (g_1(x), g_2(x), ..., g_n(x))$$

for $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$. Then, the concatenation

$$F(x_0; x) = ((f_1 || g_1)(x_0; x), (f_2 || g_2)(x_0; x), \ldots, (f_n || g_n)(x_0; x)).$$

Now, the definitions of Walsh value, Walsh spectrum and nonlinearity of the concatenation F can be stated using the properties of the concatenation of Boolean functions by associating these properties with S-boxes.

The Walsh value of F at any point $((w_0; w), c)$ can be computed directly from the Walsh values of S_1 and S_2 at the point (w, c):

$$W_F((w_0; w), c) = \begin{cases} W_{S_1}(w, c) + W_{S_2}(w, c), & \text{if } w_0 = 0 \\ W_{S_1}(w, c) - W_{S_2}(w, c), & \text{if } w_0 = 1 \end{cases},$$

for $(w_0; w) \in \mathbb{F}_2^{n+1}$, and $c \in \mathbb{F}_2^{n*}$. Consequently, the Walsh spectrum of F is an $2^{n+1} \times (2^n - 1)$-matrix constructed by alining the Walsh spectra of the component functions in lexicographical order, which is defined as

$$W_F = [W_{f_n || g_n}, W_{f_{n-1} || g_{n-1}}, \ldots, W_{f_1 || g_1 \oplus f_2 || g_2 \oplus \ldots \oplus f_n || g_n}],$$

and each of the component refers to

$$W_{f_p || g_q} = [W_{f_p} + W_{g_q},\ W_{f_p} - W_{g_q}],$$

where f_p's and g_q's are the component functions of S_1 and S_2 corresponding to $p = c \cdot S_1(x)$ and $q = c \cdot S_2(x)$ for $c \in \mathbb{F}_2^{n*}$. In shortly,

$$W_F = [W_{S_1} + W_{S_2},\ W_{S_1} - W_{S_2}],$$

where W_{S_1} and W_{S_2} are the Walsh spectra of S_1 and S_2 in matrix form, respectively.

Following the subjacent steps, the nonlinearity of F is expressed in terms of Walsh values of S_1 and S_2:

$$\begin{aligned}
\mathcal{N}_F &= \min_{c\in\mathbb{F}_2^{n*}} \{\mathcal{N}_{c\cdot F}\} \\
&= \min_{c\in\mathbb{F}_2^{n*}} \{\mathcal{N}_{c\cdot(S_1||S_2)(x_0;x)}\} \\
&= \min_{c\in\mathbb{F}_2^{n*}} \{\mathcal{N}_{(c\cdot S_1||c\cdot S_2)(x_0;x)}\} \\
&= \min_{c\in\mathbb{F}_2^{n*}} \left\{2^n - \frac{1}{2}\max_{u\in\mathbb{F}_2^n}\{|W_{S_1}(u,c)| + |W_{S_2}(u,c)|\}\right\} \\
&= 2^n - \frac{1}{2}\max_{\substack{u\in\mathbb{F}_2^n,\\ c\in\mathbb{F}_2^{n*}}}\{|W_{S_1}(u,c)| + |W_{S_2}(u,c)|\}.
\end{aligned}$$

If the nonlinearity of F is bounded greater than $\alpha \in \mathbb{Z}$, then the relation between nonlinearity of F and the nonlinearities of S_1 and S_2 is presented below:

$$\begin{aligned}
\mathcal{N}_F \geq \alpha &\implies \min_{c\in\mathbb{F}_2^{n*}} \{\mathcal{N}_{c\cdot F}\} \geq \alpha \\
&\implies \min_{c\in\mathbb{F}_2^{n*}} \{\mathcal{N}_{(c\cdot S_1||c\cdot S_2)(x_0;x)}\} \geq \alpha \\
&\implies \mathcal{N}_{(c\cdot S_1||c\cdot S_2)(x_0;x)} \geq \alpha, \ \ \forall c \in \mathbb{F}_2^{n*} \\
&\implies 2^n - \frac{1}{2}\max_{u\in\mathbb{F}_2^n}\{|W_{S_1}(u,c)| + |W_{S_2}(u,c)|\} \geq \alpha, \ \ \forall c \in \mathbb{F}_2^{n*} \\
&\implies \max_{u\in\mathbb{F}_2^n}\{|W_{S_1}(u,c)| + |W_{S_2}(u,c)|\} \leq 2^{n+1} - 2\alpha, \ \ \forall c \in \mathbb{F}_2^{n*} \\
&\implies \max_{u\in\mathbb{F}_2^n}\{|W_{S_1}(u,c)|\}, \max_{v\in\mathbb{F}_2^n}\{|W_{S_2}(v,c)|\} \leq 2^{n+1} - 2\alpha, \ \ \forall c \in \mathbb{F}_2^{n*} \\
&\implies \mathcal{N}_{S_1}, \mathcal{N}_{S_2} \geq 2^{n-1} - 2^n + \alpha.
\end{aligned}$$

Proposition 2.6. *Let $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^n$ be an $(n+1) \times n$ S-box which is constructed by the concatenation of two $n \times n$ S-boxes S_1 and S_2. Then, the Walsh spectrum of F is an $2^{n+1} \times (2^n - 1)$-matrix constructed by alining the Walsh spectra of component functions of F such that*

$$W_F = [W_{S_1} + W_{S_2},\ W_{S_1} - W_{S_2}],$$

where W_{S_1} and W_{S_2} are the matrices of the Walsh spectra of S_1 and S_2, respectively. If the maximum of the absolute of the Walsh spectrum of each component function $c \cdot F$, i.e. $\max_{w\in\mathbb{F}_2^{n+1}, c\in\mathbb{F}_2^{n*}}\{|W_F(w,c)|\}$, is bounded by $\beta_F \in \mathbb{Z}$, then the nonlinearities of S_1 and S_2 will be bounded below

$$\mathcal{N}_{S_1}, \mathcal{N}_{S_2} \geq 2^n - \frac{1}{2}\beta_F.$$

Proof. Let $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^n$ with $F = S_1||S_2$, and let $c \cdot S_1$ and $c \cdot S_2$ denote the component functions of S_1 and S_2. Then, the component function of F will be

$$c \cdot F(x_0; x) = c \cdot S_1(x)||c \cdot S_2(x),$$

where $(x_0; x) \in \mathbb{F}_2^{n+1}$, and $c \in \mathbb{F}_2^{n*}$. Following this, the Walsh spectrum of F can be defined as an $2^{n+1} \times (2^n - 1)$-matrix constructed by alining the Walsh spectra of component functions of F such that

$$W_F = [W_{S_1} + W_{S_2},\ W_{S_1} - W_{S_2}],$$

where W_{S_1} and W_{S_2} are the matrices of the Walsh spectra of S_1 and S_2, respectively. Since F is a composition of the concatenations of Boolean functions,

$$\max_{\substack{w \in \mathbb{F}_2^{n+1}, \\ c \in \mathbb{F}_2^{n*}}} \{|W_F(w, c)|\} = \max_{\substack{u \in \mathbb{F}_2^n, \\ c \in \mathbb{F}_2^{n*}}} \{|W_{S_1}(u, c)| + |W_{S_2}(u, c)|\}.$$

Then, the restriction of the maximum of the absolute value of each column of W_F with $\beta_F \in \mathbb{Z}$ implies:

$$\begin{aligned}
\max_{\substack{w \in \mathbb{F}_2^{n+1}, \\ c \in \mathbb{F}_2^{n*}}} \{|W_F(w, c)|\} \leq \beta_F \quad &\Longrightarrow \quad \max_{\substack{u \in \mathbb{F}_2^n, \\ c \in \mathbb{F}_2^{n*}}} \{|W_{S_1}(u, c)|\},\ \max_{\substack{v \in \mathbb{F}_2^n, \\ c \in \mathbb{F}_2^{n*}}} \{|W_{S_2}(v, c)|\} \leq \beta_F \\
&\Longrightarrow \quad \mathcal{N}_{S_1}, \mathcal{N}_{S_2} \geq 2^n - \frac{1}{2}\beta_F.
\end{aligned}$$

□

2.2.2.1 Concatenation of Rotation-symmetric S-boxes

In the case of the concatenation of rotation-symmetric S-boxes, the rotation-property of S-boxes is carried to the concatenation, and it is integrated with the properties of concatenations. Let F be an $(n + 1) \times n$ S-box which is constructed by the concatenation of two $n \times n$ rotation-symmetric S-boxes S_1 and S_2. Then, S_1 and S_2 satisfy the equations

$$\rho^k(S_1(x)) = S_1(\rho^k(x)), \text{ and } \rho^k(S_2(x)) = S_2(\rho^k(x)),$$

for all $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$, and for any $1 \leq k \leq n$.

Observe that the concatenation F is not rotation-symmetric unless both of the S_1 and S_2 consist of only all-zero and all-one vectors. However, F is symmetric under the permutation $\tau(x_0, x_1, ..., x_n) = (x_0, x_2, ..., x_1)$. Since the rotations of the vector $(x_0, x_1, ..., x_n)$ do not depend on x_0, the concatenation will continue to carry the properties of rotation-symmetry. Thus, F satisfies the equation

$$\tau^t(F(x_0; x)) = F(\tau^t(x_0; x)) = F(x_0; \rho^t(x)),$$

where $1 \leq t \leq n$ for all $(x_0; x) \in \mathbb{F}_2^{n+1}$. If S_1 is an k-RSSB and S_2 is an l-RSSB, then $t = lcm(k, l)$. k-rotation-symmetric S-boxes (k-RSSBs) are defined in the former section.

According to this permutation, the vector field $\mathbb{F}_2^{n+1}$ is divided into $2g_n$ partitions, i.e. the number of the orbits of that field is $2g_n$, since the same orbits of the field $\mathbb{F}_2^n$ under the rotation-symmetry are included to the orbits of $\mathbb{F}_2^{n+1}$ for $x_0 = 0$, and also for $x_0 = 1$. Therefore, it can be said that the orbits are generated by

$$H_{n+1}(x_0; x) = \{\tau^t(x_0; x) = (x_0; \rho^t(x)) \mid 1 \leq t \leq n\},$$

and the sizes of the orbits $H_{n+1}(x_0; x)$ and $G_n(x)$ are equal for all $(x_0; x)$.

The S-box F can be also expressed in terms of the orbit representatives of the orbits generated by $G_n(x)$ as

$$F(x_0; \Lambda_i) = \rho^r(\Lambda_j), \text{ for any } 1 \leq r \leq n,$$

where $|G_n(\Lambda_i)| = |G_n(\Lambda_j)|$ or $|G_n(\Lambda_j)|$ divides $|G_n(\Lambda_i)|$ for $i, j = 1, 2, ..., g_n$. Since F is a concatenation of S_1 and S_2, this expression can be adapted to

$$F(x_0; \Lambda_i) = \begin{cases} S_1(\Lambda_i) = \rho^p(\Lambda_{j_1}), & \text{if } x_0 = 0 \\ S_2(\Lambda_i) = \rho^q(\Lambda_{j_2}), & \text{if } x_0 = 1 \end{cases}, \text{ for any } 1 \leq p, q \leq n,$$

where the property about the size of $G_n(\Lambda_j)$ in the former sentence is extended to the orbits $G_n(\Lambda_{j_1})$, and $G_n(\Lambda_{j_2})$ for $j_1, j_2 = 1, 2, ..., g_n$. After the match-ups of Λ_i's with $\rho^p(\Lambda_{j_1})$'s and $\rho^q(\Lambda_{j_2})$'s, the rotations of the inputs automatically match with the rotations of outputs. For this reason, all inputs of F can be reduced to all representative elements and consequently F can be described by only the outputs of the orbit representatives:

$$F = [S_1(\Lambda_1), S_1(\Lambda_2), ..., S_1(\Lambda_{g_n}), S_2(\Lambda_1), S_2(\Lambda_2), ..., S_2(\Lambda_{g_n})].$$

Now, the direction of this thesis turns to obtain $(n+1) \times (n+1)$ bijective S-boxes which are constructed by the addition of $(n+1)$-variable Boolean function to the concatenation of $n \times n$ rotation-symmetric S-boxes. In this construction, the resultant S-boxes are symmetric under the permutation $\tau(x_0, x_1, ..., x_n) = (x_0, x_2, ..., x_1)$ since the rotation-property is carried to this permutation by fixing the x_0-term.

To be an $(n+1) \times (n+1)$ bijective S-box, it is clear that it should include all vectors of $\mathbb{F}_2^n$ two times in the outputs of the concatenation. Then, adding the $(n+1)$-variable Boolean functions in such a way that the output of this function for one of the double vectors of $\mathbb{F}_2^n$ is equal to 0, as for the other one of the double vectors it equals to 1, makes all vectors of $\mathbb{F}_2^{n+1}$ to appear in the outputs of the S-box. As a remark, the rotation-symmetric S-boxes that will be concatenated need not to be bijective. It is enough for the concatenation to contain all the vectors of $\mathbb{F}_2^n$ two times in its outputs. That is to say, the outputs of the rotation-symmetric S-boxes can consist of both of the double vectors.

Let $S : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ be an S-box of above construction which is in the form of $S = (f, F)$, where f is an $(n+1)$-variable Boolean function determining the first term of the outputs of S, and $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^n$ is a concatenation of two $n \times n$ rotation-symmetric S-boxes S_1 and S_2. Then, for all $(x_0; x) \in \mathbb{F}_2^{n+1}$, S can be defined as

$$S(x_0; x) = (f(x_0; x), F(x_0; x)) = (f(x_0; x), S_1(x)||S_2(x)),$$

where $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$. Assuming that for all x,

$$\rho^k(S_1(x)) = S_1(\rho^k(x)) \text{ and } \rho^k(S_2(x)) = S_2(\rho^k(x)), \text{ for any } 1 \leq k \leq n,$$

the S-box S will be symmetric under the permutation $\tau(x_0, x_1, ..., x_n) = (x_0, x_2, ..., x_1)$ since

$$\begin{aligned} \tau^t(S(x_0; x)) = \tau^t(f(x_0; x), F(x_0; x)) &= (f(x_0; x), \rho^t(S_1(x)||S_2(x))) \\ &= S(x_0; \rho^t(x)) = S(\tau^t(x_0; x)), \end{aligned}$$

where $1 \leq t \leq n$, for all $(x_0; x)$. If S_1 is an k-RSSB and S_2 is an l-RSSB, then $t = lcm(k, l)$.

As said before, there are $2g_n$ orbits dividing the vector space of $\mathbb{F}_2^{n+1}$ under the permutation τ, which are generated by

$$H_{n+1}(x_0; x) = \{\tau^t(x_0; x) = (x_0; \rho^t(x)) \mid 1 \leq t \leq n\},$$

and $|H_{n+1}(x_0; x)| = |G_n(x)|$ for all $(x_0; x)$. Moreover, S can be expressed in terms of the orbit representatives of the orbits generated by $G_n(x)$ such that

$$S(x_0; \Lambda_i) = (f(x_0; \Lambda_i), \rho^r(\Lambda_j)), \text{ for any } 1 \leq r \leq n,$$

where $|G_n(\Lambda_i)| = |G_n(\Lambda_j)|$ for $i, j = 1, 2, ..., g_n$. Here, Λ_i's should be matched only with the some rotations of Λ_j's that both of their orbits have equal size. Otherwise, the bijectivity is not verified. Furthermore, the adjusted form of this expression to the cases of x_0 is

$$S(x_0; \Lambda_i) = \begin{cases} (f(0, \Lambda_i), \rho^p(\Lambda_{j_1})), & \text{if } x_0 = 0 \\ (f(1, \Lambda_i), \rho^q(\Lambda_{j_2})), & \text{if } x_0 = 1 \end{cases}, \text{ for any } 1 \leq p, q \leq n,$$

where $|G_n(\Lambda_i)| = |G_n(\Lambda_{j_1})| = |G_n(\Lambda_{j_2})|$ for $j_1, j_2 = 1, 2, ..., g_n$. In this expression, the rotation of the input means the rotation of the output and consequently the elements of the orbit of $G_n(\Lambda_i)$ match with the elements of the orbit of $G_n(\Lambda_{j_1})$ if $x_0 = 0$. For the other case, they match with the elements of the orbit of $G_n(\Lambda_{j_2})$. This means that if $\rho^p(\Lambda_{j_1}) = \rho^q(\Lambda_{j_2})$, or if they are the elements of the same orbit, both of these elements generate the same orbit, separately. Hence, the function f is equal to 0 for one of these orbits, and it is equal to 1 for the other orbit.

Similar to the case of the concatenation F, S can be described by the outputs of the orbit representatives:

$$S = [S(0; \Lambda_1), S(0; \Lambda_2), ..., S(0; \Lambda_{g_n}), S(1; \Lambda_1), S(1; \Lambda_2), ..., S(1; \Lambda_{g_n})].$$

The number of such S-boxes can be found by Prop.2.5. Under the permutation τ, the number of $(n+1) \times (n+1)$ bijective S-boxes constructed by the addition of $(n+1)$-variable Boolean function to the concatenation of $n \times n$ rotation-symmetric S-boxes can be found by doubling t values while leaving the sizes s unchanged in the formula of Prop.2.5. Here, t values are doubled since the number of orbits are doubled by the construction. The sizes are unchanged, because of the permutation, the number of rotation of any input remains the same as in the case of the rotation of any elements of $\mathbb{F}_2^n$. Thus, the formula for this case can be defined as

$$\prod_{i=1}^{d}(2t_i)!s_i^{2t_i},$$

where d is the number of distinct orbit sizes, s denotes the size of the output orbits and t represents the number of the orbits having the same size s.

Another statement about this construction is the nonlinearity of $S = (f, F)$. How can the nonlinearity of F be found is examined in the Sec.2.2.2. After the nonlinearity of f is found as an $(n + 1)$-variable Boolean function, the nonlinearity of S will be the minimum of the nonlinearities of f and F, i.e. $\mathcal{N}_S = \min\{\mathcal{N}_f, \mathcal{N}_F\}$.

2.3 Affine Equivalence

Let f and g be two n-variable Boolean functions. It is said that f is *affine equivalent* to g if there exists a binary invertible $n \times n$-matrix A, vectors $b, c \in \mathbb{F}_2^n$, and $d \in \mathbb{F}_2$ such that

$$g(x) = f(Ax + b) + cx + d \quad \text{for all } x \in \mathbb{F}_2^n.$$

Remark that the distribution of the absolute of the Walsh spectra of f is the same with that of g as stated in [22]. Thus, their nonlinearities are also equal. Moreover, the distribution of the absolute of the auto-correlation function of f is the same with that of g. This implies that the absolute indicators of both of f and g are equal.

Let S and T be two $n \times n$ S-boxes. They are called *affine equivalent* [2] if there exists two binary invertible $n \times n$-matrices A and B, two vectors $c, d \in \mathbb{F}_2^n$ such that

$$T(x) = S(Ax + c)B + d \quad \text{for all } x \in \mathbb{F}_2^n.$$

CHAPTER 3

CONSTRUCTION OF 6 $\times$ 6 BIJECTIVE S-BOXES

The primary concern of this thesis is to obtain 6×6 bijective S-boxes that are symmetric under the permutation $\tau(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0, x_2, x_3, x_4, x_5, x_1)$ for all $(x_0, x_1, ..., x_5) \in \mathbb{F}_2^6$. The reason behind it, this class of S-boxes is linear equivalent to a rich class in terms of desirable cryptographic properties such as high nonlinearity and low differential uniformity which is identified by the symmetric S-boxes under the permutation $\sigma(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0, x_4, x_1, x_2, x_5, x_3)$ among 11 classes stated in [9]. These 11 classes are obtained by the elimination of linear equivalent ones among all classes which are formed by $6!$ permutations of 6 variables. Also, there is an opportunity to construct such S-boxes, which are symmetric under τ, since these S-boxes can be interpreted as the concatenations of 5×5 rotation-symmetric S-boxes by the addition of 6-variable Boolean function in front of them.

Now, the construction method mentioned in Sec.2.2.2.1 is applied for the 6×6 bijective S-boxes. Let S be an 6×6 bijective S-box which is symmetric under the permutation $\tau(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0, x_2, x_3, x_4, x_5, x_1)$ where $(x_0, x_1, ..., x_5) \in \mathbb{F}_2^6$. Then, for all $(x_0; x) = (x_0, x_1, ..., x_5)$,

$$\tau^t(S(x_0; x)) = S(\tau^t(x_0; x)) \implies \tau^t(S(x_0, x_1, ..., x_5)) = S(x_0, \rho^t(x)),$$

where ρ^t is the t-th cyclic shift operator on $\mathbb{F}_2^5$, and $1 \leq t \leq 5$. Thus, S can be interpreted as an S-box constructed by the addition of 6-variable Boolean function f to the concatenation F of two 5×5 rotation-symmetric S-boxes S_1 and S_2. Shortly, S is in the form of $S = (f, F) = (f, S_1 || S_2)$, where the first bits of the outputs values of S constitutes f.

Here, observe that for a 5×5 RSSB, $gcd(5, 5) = 1$. This implies that the size of the output orbits divides the size of the input orbits. Additionally, the orbits generated by $G_5(x)$ have size only 1 and 5. To divide 1 and 5, all input orbits should be matched with the orbits of the size 1 or the input orbits should be matched with the output orbits for which their orbit sizes are equal. Since S is bijective, the RSSBs S_1 and S_2 contain all the output orbits generated by $G_5(x)$ for $x \in \mathbb{F}_2^5$. Therefore, the only possibility for the outputs of the input orbits is to have the same orbit size with the input orbits. For this reason, S_1 and S_2 can not be k-RSSB and they satisfy for all $1 \leq k \leq 5$,

$$\rho^k(S_1(x)) = S_1(\rho^k(x)) \text{ and } \rho^k(S_2(x)) = S_2(\rho^k(x)), \text{ for all } x.$$

Table 3.1: The orbits generated by $H_6(x_0; x)$ for $(x_0; x) \in \mathbb{F}_2^6$

#	$(\boldsymbol{x_0}; \boldsymbol{x})$	$\boldsymbol{H_6(x_0; x)}$
1	$(0,0,0,0,0,0)$	$\{(0,0,0,0,0,0)\}$
2	$(0,0,0,0,0,1)$	$\{(0,0,0,0,0,1),(0,0,0,0,1,0),(0,0,0,1,0,0),(0,0,1,0,0,0),(0,1,0,0,0,0)\}$
3	$(0,0,0,0,1,1)$	$\{(0,0,0,0,1,1),(0,0,0,1,1,0),(0,0,1,1,0,0),(0,1,1,0,0,0),(0,1,0,0,0,1)\}$
4	$(0,0,0,1,0,1)$	$\{(0,0,0,1,0,1),(0,0,1,0,1,0),(0,1,0,1,0,0),(0,0,1,0,0,1),(0,1,0,0,1,0)\}$
5	$(0,0,0,1,1,1)$	$\{(0,0,0,1,1,1),(0,0,1,1,1,0),(0,1,1,1,0,0),(0,1,1,0,0,1),(0,1,0,0,1,1)\}$
6	$(0,0,1,0,1,1)$	$\{(0,0,1,0,1,1),(0,1,0,1,1,0),(0,0,1,1,0,1),(0,1,1,0,1,0),(0,1,0,1,0,1)\}$
7	$(0,0,1,1,1,1)$	$\{(0,0,1,1,1,1),(0,1,1,1,1,0),(0,1,1,1,0,1),(0,1,1,0,1,1),(0,1,0,1,1,1)\}$
8	$(0,1,1,1,1,1)$	$\{(0,1,1,1,1,1)\}$
9	$(1,0,0,0,0,0)$	$\{(1,0,0,0,0,0)\}$
10	$(1,0,0,0,0,1)$	$\{(1,0,0,0,0,1),(1,0,0,0,1,0),(1,0,0,1,0,0),(1,0,1,0,0,0),(1,1,0,0,0,0)\}$
11	$(1,0,0,0,1,1)$	$\{(1,0,0,0,1,1),(1,0,0,1,1,0),(1,0,1,1,0,0),(1,1,1,0,0,0),(1,1,0,0,0,1)\}$
12	$(1,0,0,1,0,1)$	$\{(1,0,0,1,0,1),(1,0,1,0,1,0),(1,1,0,1,0,0),(1,0,1,0,0,1),(1,1,0,0,1,0)\}$
13	$(1,0,0,1,1,1)$	$\{(1,0,0,1,1,1),(1,0,1,1,1,0),(1,1,1,1,0,0),(1,1,1,0,0,1),(1,1,0,0,1,1)\}$
14	$(1,0,1,0,1,1)$	$\{(1,0,1,0,1,1),(1,1,0,1,1,0),(1,0,1,1,0,1),(1,1,1,0,1,0),(1,1,0,1,0,1)\}$
15	$(1,0,1,1,1,1)$	$\{(1,0,1,1,1,1),(1,1,1,1,1,0),(1,1,1,1,0,1),(1,1,1,0,1,1),(1,1,0,1,1,1)\}$
16	$(1,1,1,1,1,1)$	$\{(1,1,1,1,1,1)\}$

Recall that the orbits generated by

$$H_6(x_0; x) = \{\tau^t(x_0; x) = (x_0; \rho^t(x)) \mid 1 \leq t \leq 5\}$$

divide into partitions of the set of all inputs of S, and $|H_6(x_0; x)| = |G_5(x)|$ for all $(x_0; x)$. However, the number of orbits generated by $H_6(x_0; x)$ are double of the number of orbits generated by $G_5(x)$ due to the two values of x_0. Thus, there are 4 orbits of size 1, and 12 orbits of size 5 generated by $H_6(x_0; x)$ that partition the vector space of $\mathbb{F}_2^6$. These orbits and their elements can be seen from Tab.3.1.

The number of 6×6 bijective S-boxes that are symmetric under τ can be found by using Prop.2.5. Regarding this proposition, there are two different orbit sizes, i.e. the sizes of 1 and 5, which implies that $d = 2$, $s_1 = 1$, and $s_2 = 5$. Additionally, the number of orbits of size s_1 is 4, while the number of orbits of size s_2 is 12. This implies that $t_1 = 4$ and $t_2 = 12$. Thus, if these values are substituted in the formula, the number is found as

$$\prod_{i=1}^{2} t_i! s_i^{t_i} = (t_1! s_1^{t_1})(t_2! s_2^{t_2}) = (4! 1^4)(12! 5^{12}) \approx 2^{61.28}.$$

Hence, there are $2^{61.28}$ bijective S-boxes that are symmetric under τ.

The S-box S, to be bijective, the orbits of the set of inputs of S should be matched with the orbits of the set of outputs of S such that no unmatched orbit remains after this match-up. Following the case of 5×5 RSSB, only the orbits of equal size can be matched with each other in Tab.3.1.

Let the lexicographically first element of the orbits generated by $G_5(x) = \{\rho^t(x) \mid 1 \leq t \leq 5\}$ be Λ_i for $i = 1, 2, ..., 8$. Then,

$$S(x_0; \Lambda_i) = (f(x_0; \Lambda_i), \rho^r(\Lambda_j)), \text{ for any } 1 \leq r \leq 5,$$

where $|G_5(\Lambda_i)| = |G_5(\Lambda_j)|$ for $i, j = 1, 2, ..., 8$. Furthermore, the adjusted form of this expression to the cases of x_0 is

$$S(x_0; \Lambda_i) = \begin{cases} (f(0, \Lambda_i), \rho^p(\Lambda_{j_1})), & \text{if } \ x_0 = 0 \\ (f(1, \Lambda_i), \rho^q(\Lambda_{j_2})), & \text{if } \ x_0 = 1 \end{cases}, \text{ for any } 1 \leq p, q \leq 5,$$

where $|G_n(\Lambda_i)| = |G_n(\Lambda_{j_1})| = |G_n(\Lambda_{j_2})|$ for $j_1, j_2 = 1, 2, ..., 8$. In this expression, the rotation of the input means the rotation of the output, that is,

$$\begin{aligned} \tau^t(S(x_0; \Lambda_i)) = S(\tau^t(x_0; \Lambda_i)) &= S(x_0, \rho^t(\Lambda_i)) \\ &= (f(x_0; \rho^t(\Lambda_i)), \rho^{t+r}(\Lambda_j)) \\ &= \begin{cases} (f(0, \rho^t(\Lambda_i)), \rho^{t+p}(\Lambda_{j_1})), & \text{if } \ x_0 = 0 \\ (f(1, \rho^t(\Lambda_i)), \rho^{t+q}(\Lambda_{j_2})), & \text{if } \ x_0 = 1 \end{cases}, \end{aligned}$$

where $\rho^{t+r} = \rho^{(t+r-5)}$, if $t + r > 5$. This is the same for the cases of $t + p > 5$ and $t + q > 5$. For example, if $|G_5(\Lambda_i)| = 5$, and

$$\begin{aligned} S(x_0; \Lambda_i) = (f(x_0; \Lambda_i), \rho^3(\Lambda_j)) \quad &\Longrightarrow \quad \tau^1(S(x_0; \Lambda_i)) = (f(x_0; \rho^1(\Lambda_i)), \rho^4(\Lambda_j)), \\ &\Longrightarrow \quad \tau^2(S(x_0; \Lambda_i)) = (f(x_0; \rho^2(\Lambda_i)), \rho^5(\Lambda_j)), \\ &\Longrightarrow \quad \tau^3(S(x_0; \Lambda_i)) = (f(x_0; \rho^3(\Lambda_i)), \rho^1(\Lambda_j)), \\ &\Longrightarrow \quad \tau^4(S(x_0; \Lambda_i)) = (f(x_0; \rho^4(\Lambda_i)), \rho^2(\Lambda_j)), \\ &\Longrightarrow \quad \tau^5(S(x_0; \Lambda_i)) = (f(x_0; \rho^5(\Lambda_i)), \rho^3(\Lambda_j)). \end{aligned}$$

All of these imply that

$$\begin{aligned} \tau^1(S(x_0; \Lambda_i)) \quad &= \quad (f(x_0; \rho^1(\Lambda_i)), \rho^4(\Lambda_j)) \\ &\Longrightarrow \quad \begin{cases} (f(0, \rho^1(\Lambda_i)), \rho^{p+4}(\Lambda_{j_1})), & \text{if } \ x_0 = 0 \\ (f(1, \rho^1(\Lambda_i)), \rho^{q+4}(\Lambda_{j_2})), & \text{if } \ x_0 = 1 \end{cases}, \end{aligned}$$

$$\begin{aligned} \tau^2(S(x_0; \Lambda_i)) \quad &= \quad (f(x_0; \rho^2(\Lambda_i)), \rho^5(\Lambda_j)) \\ &\Longrightarrow \quad \begin{cases} (f(0, \rho^2(\Lambda_i)), \rho^{p+5}(\Lambda_{j_1})), & \text{if } \ x_0 = 0 \\ (f(1, \rho^2(\Lambda_i)), \rho^{q+5}(\Lambda_{j_2})), & \text{if } \ x_0 = 1 \end{cases}, \end{aligned}$$

$$\begin{aligned} \tau^3(S(x_0; \Lambda_i)) \quad &= \quad (f(x_0; \rho^3(\Lambda_i)), \rho^1(\Lambda_j)) \\ &\Longrightarrow \quad \begin{cases} (f(0, \rho^3(\Lambda_i)), \rho^{p+1}(\Lambda_{j_1})), & \text{if } \ x_0 = 0 \\ (f(1, \rho^3(\Lambda_i)), \rho^{q+1}(\Lambda_{j_2})), & \text{if } \ x_0 = 1 \end{cases}, \end{aligned}$$

Table 3.2: The orbit representatives of the orbits generated by $G_5(x)$ for $x \in \mathbb{F}_2^5$

$\boldsymbol{i}$	$\boldsymbol{\Lambda_i}$	$\boldsymbol{G_5(\Lambda_i)}$
1	$\Lambda_1 = (0,0,0,0,0)$	$\{(0,0,0,0,0)\}$
2	$\Lambda_2 = (0,0,0,0,1)$	$\{(0,0,0,0,1),(0,0,0,1,0),(0,0,1,0,0),(0,1,0,0,0),(1,0,0,0,0)\}$
3	$\Lambda_3 = (0,0,0,1,1)$	$\{(0,0,0,1,1),(0,0,1,1,0),(0,1,1,0,0),(1,1,0,0,0),(1,0,0,0,1)\}$
4	$\Lambda_4 = (0,0,1,0,1)$	$\{(0,0,1,0,1),(0,1,0,1,0),(1,0,1,0,0),(0,1,0,0,1),(1,0,0,1,0)\}$
5	$\Lambda_5 = (0,0,1,1,1)$	$\{(0,0,1,1,1),(0,1,1,1,0),(1,1,1,0,0),(1,1,0,0,1),(1,0,0,1,1)\}$
6	$\Lambda_6 = (0,1,0,1,1)$	$\{(0,1,0,1,1),(1,0,1,1,0),(0,1,1,0,1),(1,1,0,1,0),(1,0,1,0,1)\}$
7	$\Lambda_7 = (0,1,1,1,1)$	$\{(0,1,1,1,1),(1,1,1,1,0),(1,1,1,0,1),(1,1,0,1,1),(1,0,1,1,1)\}$
8	$\Lambda_8 = (1,1,1,1,1)$	$\{(1,1,1,1,1)\}$

$$\begin{aligned}
\tau^4(S(x_0;\Lambda_i)) &= (f(x_0;\rho^4(\Lambda_i)),\rho^2(\Lambda_j)) \\
&\Longrightarrow \begin{cases} (f(0,\rho^4(\Lambda_i)),\rho^{p+2}(\Lambda_{j_1})), & \text{if } x_0 = 0 \\ (f(1,\rho^4(\Lambda_i)),\rho^{q+2}(\Lambda_{j_2})), & \text{if } x_0 = 1 \end{cases},
\end{aligned}$$

$$\begin{aligned}
\tau^5(S(x_0;\Lambda_i)) &= (f(x_0;\rho^5(\Lambda_i)),\rho^3(\Lambda_j)) \\
&\Longrightarrow \begin{cases} (f(0,\rho^5(\Lambda_i)),\rho^{p+3}(\Lambda_{j_1})), & \text{if } x_0 = 0 \\ (f(1,\rho^5(\Lambda_i)),\rho^{q+3}(\Lambda_{j_2})), & \text{if } x_0 = 1 \end{cases}.
\end{aligned}$$

Consequently, the elements of the orbit of $G_5(\Lambda_i)$ match with the elements of the orbit of $G_5(\Lambda_{j_1})$ if $x_0 = 0$. For the other case, they match with the elements of the orbit of $G_5(\Lambda_{j_2})$. This means that if $\rho^p(\Lambda_{j_1}) = \rho^q(\Lambda_{j_2})$, or if they are the elements of the same orbit, both of these elements generate the same orbit, separately. Hence, the function f is equal to 0 for one of these orbits, and it is equal to 1 for the other orbit.

The orbit representatives of $G_5(x)$ for all x, i.e. Λ_i's for $i = 1,2,...,8$, are listed in Tab.3.2. As stated above, the elements which determine the outputs of the S-box S are the orbit representatives. Therefore, S can be described by the outputs of the orbit representatives:

$$S = [S(0;\Lambda_1), S(0;\Lambda_2), ..., S(0;\Lambda_8), S(1;\Lambda_1), S(1;\Lambda_2), ..., S(1;\Lambda_8)],$$

and also the concatenation F can be represented by

$$F = [S_1(\Lambda_1), S_1(\Lambda_2), ..., S_1(\Lambda_8), S_2(\Lambda_1), S_2(\Lambda_2), ..., S_2(\Lambda_8)].$$

Here, $S_1(\Lambda_1)$ can only be matched with Λ_1 or Λ_8 because of $|G_5(\Lambda_1)| = |G_5(\Lambda_8)|$. Similarly, $S_1(\Lambda_8)$ can only be matched with Λ_1 or Λ_8. If $S_1(\Lambda_1) = S_1(\Lambda_8)$, then $S_2(\Lambda_1) = S_2(\Lambda_8)$ and they are equal to the complement of the output of $S_1(\Lambda_1)$ (The complement operation is to add all-one vector to the input. Here, Λ_1 and Λ_8 are complements of each other). Otherwise, the condition of $S_2(\Lambda_1) = \Lambda_1$ or Λ_8 arises. In accordance with the result, $S_2(\Lambda_8)$ is determined. All these choices are made in 6 different ways since

$$(S_1(\Lambda_1), S_1(\Lambda_8), S_2(\Lambda_1), S_2(\Lambda_8)) \in \mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8),$$

and $|\mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)| = \frac{4!}{2!2!} = 6$. In other words,

$$(F(0; \Lambda_1), F(0; \Lambda_8), F(1; \Lambda_1), F(1; \Lambda_8)) \in \mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8).$$

For the match-ups of the remaining 12 orbits of the set of inputs with the double output orbits of Λ_j's for $j = 2, 3, ..., 7$, four different cases are taken into consideration. These cases take form with respect to the conditions that the output of S_1 keeps one pair of the double orbits, two or three pairs of the double orbits or no pair of double orbits. That is, the input orbits of S_1 can be matched with any of the below permutations of the output orbits represented by orbit representatives:

- $\mathcal{P}(\Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_4}, \Lambda_{j_5}, \Lambda_{j_6})$,
- $\mathcal{P}(\Lambda_{j_1}, \Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_4}, \Lambda_{j_5})$,
- $\mathcal{P}(\Lambda_{j_1}, \Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_4})$,
- $\mathcal{P}(\Lambda_{j_1}, \Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_3})$,

where each of Λ_{j_m}'s for $m = 1, 2, ..., 6$ corresponds to the different element of the set $\{\Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7\}$. After the matching of the input orbits of S_1, the ones of S_2 are automatically matched with the permutation of the remaining orbits, and this permutation is in the same structure with the permutation of input orbits of S_1. That is to say, for example, if the output of S_1 has two pairs of double orbits, then the output of S_2 should also have two pairs of double orbits. Hence, the choice of the output orbits of S_1 determines the choice of the output orbits of S_2.

Let $\mathbb{S}_0$ denote the set of orbit representatives of the 6 output orbits of S_1 and S_2 that contain no pair of double orbits. Similarly, $\mathbb{S}_1$, $\mathbb{S}_2$ and $\mathbb{S}_3$ denote the sets of orbit representatives of the output orbits that contain one, two and three pairs of double orbits, respectively. These sets are defined as

1. $\mathbb{S}_0 = \{(\Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7)\}$,
2. $\mathbb{S}_1 = \{(\Lambda_{j_1}, \Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_4}, \Lambda_{j_5}) \mid j_1, j_2, j_3, j_4, j_5 \in \{2, 3, ..., 7\}\}$,
3. $\mathbb{S}_2 = \{(\Lambda_{j_1}, \Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_4}) \mid j_1, j_2, j_3, j_4 \in \{2, 3, ..., 7\}\}$,
4. $\mathbb{S}_3 = \{(\Lambda_{j_1}, \Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_3}) \mid j_1, j_2, j_3 \in \{2, 3, ..., 7\}\}$,

where all the elements in these sets are different up to the permutation. If the output orbit representatives of S_1 appear in one of these sets, then the orbit representatives of S_2 also take part in the same set. The set of $\mathbb{S}_0$ contains only one element corresponding to output orbit representatives of S_1 and S_2 that all of the output orbits are different for both of the S-boxes. The set of $\mathbb{S}_1$ contains $\binom{6}{1}\binom{5}{4} = 30$ elements corresponding to the choices for output orbit representatives of S_1 and S_2 such that one element consists of only one pair of double orbit representatives. In a similar way, $|\mathbb{S}_2| = \binom{6}{2}\binom{4}{2} = 90$ and $|\mathbb{S}_3| = \binom{6}{3} = 20$.

After the match-up of input orbits of S_1 and S_2 with the output orbits, the numbers of rotations of the output orbit representatives corresponding to the input orbit representatives are determined. Since the sizes of the orbits to which the outputs of $S_1(\Lambda_1)$, $S_1(\Lambda_8)$, $S_2(\Lambda_1)$, and $S_2(\Lambda_8)$ belong is definite, there is no rotation for them. Let the output orbit representatives of S_1 and S_2, except the outputs of all-zero and all-one vectors, be

$$(\Lambda_{j_1}, \Lambda_{j_2}, \Lambda_{j_3}, \Lambda_{j_4}, \Lambda_{j_5}, \Lambda_{j_6}) \text{ and } (\Lambda_{k_1}, \Lambda_{k_2}, \Lambda_{k_3}, \Lambda_{k_4}, \Lambda_{k_5}, \Lambda_{k_6}),$$

respectively. Then, the outputs of S_1 will be

$$(S_1(\Lambda_1), \rho^{p_1}(\Lambda_{j_1}), \rho^{p_2}(\Lambda_{j_2}), \rho^{p_3}(\Lambda_{j_3}), \rho^{p_4}(\Lambda_{j_4}), \rho^{p_5}(\Lambda_{j_5}), \rho^{p_6}(\Lambda_{j_6}), S_1(\Lambda_8)),$$

and the outputs of S_2 will be

$$(S_2(\Lambda_1), \rho^{q_1}(\Lambda_{k_1}), \rho^{q_2}(\Lambda_{k_2}), \rho^{q_3}(\Lambda_{k_3}), \rho^{q_4}(\Lambda_{k_4}), \rho^{q_5}(\Lambda_{k_5}), \rho^{q_6}(\Lambda_{k_6}), S_1(\Lambda_8)),$$

where $j_m, k_m \in \{2, 3, ..., 7\}$, and $1 \leq p_m, q_m \leq 5$ for $m = 1, 2, ..., 6$.

The last part of the construction is to determine the first bits of the outputs, i.e. the outputs of the 6-variable Boolean function f which has a special structure. Primarily, to satisfy the bijectivity of S, f should be balanced. Recall that the concatenation F includes all vectors of $\mathbb{F}_2^5$ two times. Thus, f should be 0 for one of the sets of the vectors of $\mathbb{F}_2^5$, while it is 1 for the other set. According to present construction, if for some Λ_i

$$f(x_0; \Lambda_i) = e \implies f(x_0; \rho^t(\Lambda_i)) = e,$$

where $e \in \mathbb{F}_2$ for all $1 \leq t \leq 5$. This says that f is 0 for one of the double orbits generated by $G_5(\Lambda_i)$, while it is 1 for the other. Therefore, it is enough to determine the outputs of f corresponding to the 8 orbits of the concatenation. This makes 2^8 Boolean functions for any determined concatenation.

Moreover, if the output orbit representatives of S_1 and S_2 are in $\mathbb{S}_1$, $\mathbb{S}_2$ or $\mathbb{S}_3$, and

$$F(x_0; \Lambda_{i_1}) = \rho^p(\Lambda_j), F(x_0; \Lambda_{i_2}) = \rho^q(\Lambda_j) \implies f(x_0; \Lambda_{i_1}) = e, f(x_0; \Lambda_{i_2}) = e \oplus 1,$$

where $e \in \mathbb{F}_2$, $1 \leq p, q \leq 5$, and $i_1 \neq i_2 \in \{1, 2, ..., 8\}$. Otherwise, for any case

$$F(x_0; \Lambda_i) = \rho^p(\Lambda_j), F(x_0 \oplus 1; \Lambda_i) = \rho^q(\Lambda_j) \implies f(x_0; \Lambda_i) = e, f(x_0 \oplus 1; \Lambda_i) = e \oplus 1,$$

for some $i, j \in \{1, 2, ..., 8\}$. In the following example, given the output of the orbit representatives of S_1, determines the output of the orbit representatives of S_2, and both of them determine the output of the Boolean function f.

Example 3.1. Let the output of the orbit representatives of S_1 be

$$(S_1(\Lambda_1), ..., S_1(\Lambda_8)) = (\Lambda_8, \pi_1(\rho^{p_1}(\Lambda_4), \rho^{p_2}(\Lambda_4), \rho^{p_3}(\Lambda_7), \rho^{p_4}(\Lambda_7), \rho^{p_5}(\Lambda_2), \rho^{p_6}(\Lambda_3)), \Lambda_1),$$

for any permutation π_1 of given 6 orbits, and $1 \leq p_m \leq 5$ with $m = 1, 2, ..., 6$. As can be seen, the output of S_1 have two pairs of double orbits which are $G_5(\Lambda_4)$ and $G_5(\Lambda_7)$. This means that the output orbit representatives of S_1 is in the set of $\mathbb{S}_2$. Then, the output orbit representatives of S_2 will also be in the set of $\mathbb{S}_2$, and the output of the orbit representatives of S_2 will be

$$(S_2(\Lambda_1), ..., S_2(\Lambda_8)) = (\Lambda_i, \pi_2(\rho^{q_1}(\Lambda_5), \rho^{q_2}(\Lambda_5), \rho^{q_3}(\Lambda_6), \rho^{q_4}(\Lambda_6), \rho^{q_5}(\Lambda_2), \rho^{q_6}(\Lambda_3)), \Lambda_j),$$

for $\Lambda_i, \Lambda_j \in \{\Lambda_1, \Lambda_8\}$, any permutation π_2 of given 6 orbits, and $1 \leq q_m \leq 5$ with $m = 1, 2, ..., 6$. Following the construction of the concatenation of S_1 and S_2, all of the output orbits of F completes two sets of the vectors of $\mathbb{F}_2^5$.

Now, state $\Lambda_i = \Lambda_8$. Then, Λ_j will be Λ_1. Then, the output of the orbits of size 1 of F will be

$$(F(0; \Lambda_1), F(0; \Lambda_8), F(1; \Lambda_1), F(1; \Lambda_8)) = (\Lambda_8, \Lambda_1, \Lambda_8, \Lambda_1).$$

This implies that if the choice for the output of f corresponding to $f(0; \Lambda_1)$, $f(0; \Lambda_8)$ is made, then the outputs $f(1; \Lambda_1)$ and $f(1; \Lambda_8)$ are automatically stated, and this choice is made in $\binom{2}{1}\binom{2}{1} = 4$ ways such that

$$\begin{aligned}
f(0; \Lambda_1) = 0,\ f(0; \Lambda_8) = 0 \quad &\Longrightarrow \quad f(1; \Lambda_1) = 1,\ f(1; \Lambda_8) = 1, \\
f(0; \Lambda_1) = 0,\ f(0; \Lambda_8) = 1 \quad &\Longrightarrow \quad f(1; \Lambda_1) = 1,\ f(1; \Lambda_8) = 0, \\
f(0; \Lambda_1) = 1,\ f(0; \Lambda_8) = 0 \quad &\Longrightarrow \quad f(1; \Lambda_1) = 0,\ f(1; \Lambda_8) = 1, \\
f(0; \Lambda_1) = 1,\ f(0; \Lambda_8) = 1 \quad &\Longrightarrow \quad f(1; \Lambda_1) = 0,\ f(1; \Lambda_8) = 0.
\end{aligned}$$

The choices for the output of f for the input orbits of size 5 are made with respect to the two cases of the placement of the double orbits of F. One of these cases comes up when both of the outputs of S_1 and S_2 include the pair(s) of the double orbits at the same time. The choices for the output of f will be, in this case,

$$\begin{aligned}
F(0; \Lambda_{i_1}) = \rho^{p_1}(\Lambda_4),\ F(0; \Lambda_{i_2}) = \rho^{p_2}(\Lambda_4) \quad \Longrightarrow \quad & f(0; \Lambda_{i_1}) = 0,\ f(0; \Lambda_{i_2}) = 1, \\
& \text{or} \\
& f(0; \Lambda_{i_1}) = 1,\ f(0; \Lambda_{i_2}) = 0,
\end{aligned}$$

for $\Lambda_{i_1} \neq \Lambda_{i_2} \in \{\Lambda_2, \Lambda_3, ..., \Lambda_7\}$. Similarly, the choices for the output of f corresponding to the output orbits $\rho^{p_3}(\Lambda_7)$, $\rho^{p_4}(\Lambda_7)$ of S_1 and $\rho^{q_1}(\Lambda_5)$, $\rho^{q_2}(\Lambda_5)$, $\rho^{q_3}(\Lambda_6)$, $\rho^{q_3}(\Lambda_6)$ of S_2 are made as in the above arguments. The other case is to assign the values of f corresponding to single orbits of S_1 and S_2. This time, the choices for f is made as

$$\begin{aligned}
F(0; \Lambda_{i_1}) = \rho^{p_5}(\Lambda_2),\ F(1; \Lambda_{j_1}) = \rho^{q_5}(\Lambda_2) \quad \Longrightarrow \quad & f(0; \Lambda_{i_1}) = 0,\ f(1; \Lambda_{j_1}) = 1, \\
& \text{or} \\
& f(0; \Lambda_{i_1}) = 1,\ f(1; \Lambda_{j_1}) = 0,
\end{aligned}$$

$$F(0;\Lambda_{i_2}) = \rho^{p_6}(\Lambda_3),\ F(1;\Lambda_{j_2}) = \rho^{q_6}(\Lambda_3) \quad \Longrightarrow \quad \begin{array}{c} f(0;\Lambda_{i_2}) = 0,\ f(1;\Lambda_{j_2}) = 1, \\ \text{or} \\ f(0;\Lambda_{i_2}) = 1,\ f(1;\Lambda_{j_2}) = 0, \end{array}$$

for $\Lambda_{i_1} \neq \Lambda_{i_2}, \Lambda_{j_1} \neq \Lambda_{j_2} \in \{\Lambda_2, \Lambda_3, ..., \Lambda_7\}$.

Eventually, for all of the orbit representatives of the inputs of S_1 and S_2, the values of f are assigned. Consequently, for the rotations of them, f takes the same value as the first bits of the output of S. Hence, the output of f for all of the inputs are determined, and all of the above choices makes 2^8 different f.

CHAPTER 4

SEARCH STRATEGY FOR 6×6 BIJECTIVE S-BOXES

In the former chapter, all needed information to construct 6×6 bijective S-boxes that are symmetric under the permutation τ was given. These S-boxes are in the form $S = (f, S_1||S_2)$, and the number of such S-boxes is $2^{61.28}$. In this section, all 6×6 bijective S-boxes having nonlinearity ≥ 24 are enumerated by using an efficient exhaustive search algorithm. It is the fact that for a desirable S-box, high nonlinearity is the primary requirement to be used in the applications of cryptography. According to [6], the best known nonlinearity is 24 among all 6×6 S-boxes. Hence, in the search space of size $2^{61.28}$ there exist $2^{37.56}$ S-boxes with nonlinearity 24 under this construction.

To obtain efficiency from the cost of the search space, the search space can be divided into 4 parts with respect to the sets $\mathbb{S}_0$, $\mathbb{S}_1$, $\mathbb{S}_2$ and $\mathbb{S}_3$ in the former section. For each of these constructions, call the sets of S-boxes as Set-k for $k = 0, 1, 2, 3$. Then, each of the Set-k is obtained using an algorithm given below.

In the algorithm, the construction of the Set-k is made as per above. First of all, the outputs of $S_1(\Lambda_1)$, $S_1(\Lambda_8)$, $S_2(\Lambda_1)$ and $S_2(\Lambda_8)$ are determined from the permutation set of $\mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)$. Then, the other output orbit representatives of S_1 are chosen from the set $\mathbb{S}_k$, and any permutation $\mathcal{P}(S_1(\Lambda_2), S_1(\Lambda_3), ..., S_1(\Lambda_7))$ is taken. This choice determines the output orbit representatives of S_2 which also belong to the set $\mathbb{S}_k$, and any permutation of them is also taken. For both of these orbit representatives, any rotation tuple, which specifies how many times each of the orbit representatives is rotated, is selected. At this stage, all elements of the concatenation F are stated. After that, in accordance with the rules mentioned in the former chapter, the output of the 6-variable Boolean function f is determined. Hence, with the addition of f to F, an S-box S, which is situated in Set-k, has been constructed.

Observe that $|\mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)| = 6$, and $|\mathbb{S}_0| = 1$, $|\mathbb{S}_1| = 30$, $|\mathbb{S}_2| = 90$, and $|\mathbb{S}_3| = 20$. Additionally, the number of the permutations of the six output orbit representatives of S_1 which belong to the set $\mathbb{S}_0$ is equal to $6! = 720$. Similarly, the numbers of permutations for the sets $\mathbb{S}_1$, $\mathbb{S}_2$ and $\mathbb{S}_3$ are $\frac{6!}{2!} = 360$, $\frac{6!}{2!2!} = 180$ and $\frac{6!}{2!2!2!} = 90$, respectively. As can be seen from the fifth and sixth loops of the algorithm, the number of all rotations of the orbit representatives is equal to 5^{12} for each Set-k. Ultimately, $|\mathcal{F}|$=2^8. Hence, the number of S-boxes, for example, in Set-1 is computed as $6 \times 30 \times 360^2 \times 5^{12} \times 2^8 \approx 2^{60.34}$. Similarly, the numbers of S-boxes in Set-0, Set-2, and Set-3 are found to be $2^{57.43}$, $2^{59.92}$, and $2^{55.75}$, respectively.

```
Input: $\mathbb{S}_k$
Output: Set-$k$
Set-$k$ is empty;
for each $(S_1(\Lambda_1), S_1(\Lambda_8), S_2(\Lambda_1), S_2(\Lambda_8)) \in \mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)$ do
    for each $(S_1(\Lambda_2), ..., S_1(\Lambda_7)) \in \mathbb{S}_k$ do
        for each $(S_1(\Lambda_2), ..., S_1(\Lambda_7)) \in \mathcal{P}(S_1(\Lambda_2), ..., S_1(\Lambda_7))$ do
            Determine the output orbit representatives of $S_2$ from $S_1$;
            for each $(S_2(\Lambda_2), ..., S_2(\Lambda_7)) \in \mathcal{P}(S_2(\Lambda_2), ..., S_2(\Lambda_7))$ do
                for each $(p_1, ..., p_6) \in \{1, ..., 5\}^6$ do
                    $S_1 = (S_1(\Lambda_1), \rho^{p_1}(S_1(\Lambda_2)), ..., \rho^{p_6}(S_1(\Lambda_7)), S_1(\Lambda_8))$;
                    for each $(q_1, ..., q_6) \in \{1, ..., 5\}^6$ do
                        $S_2 = (S_2(\Lambda_1), \rho^{q_1}(S_2(\Lambda_2)), ..., \rho^{q_6}(S_2(\Lambda_7)), S_2(\Lambda_8))$;
                        $F = S_1 || S_2$;
                        $\mathcal{F} = \{f : \mathbb{F}_2^6 \to \mathbb{F}_2 | f(\tau^t(x)) = f(\tau^t(x')) \oplus 1,$
                        for all two distinct $x, x' \in \mathbb{F}_2^5$ s.t. $F(x) = F(x')\}$;
                        for each $f \in \mathcal{F}$ do
                            Add $S = (f, F)$ to the Set-$k$;
                        end
                    end
                end
            end
        end
    end
end
```

Algorithm 1: Forming Set-k from the orbit representatives in $\mathbb{S}_k$.

Now, the search strategy is applied to each of the Set-k to find all 6×6 S-boxes having nonlinearity ≥ 24. This strategy can be considered as three-step process. The first step is to sieve affine-equivalent concatenations because affine-equivalent S-boxes have cryptographically same properties with each other. The second step is to sieve rotation-symmetric S-boxes S_1 and S_2 which will never meet the requirement of nonlinearity condition, i.e. the ones having nonlinearity < 8 and the others for which the addition of Walsh spectra of the component functions of S_1 and S_2 will never be ≥ 24. The last step is to sieve the concatenations having nonlinearity < 24.

4.1 Sieving Affine Equivalent Concatenations

All four sets formed by the choices of the output orbit representatives reserve all possible S-boxes under the construction of $S = (f, S_1||S_2)$ including the affine equivalent ones. In this search, all S-boxes are classified up to the affine equivalence, and the ones which are not affine equivalent are examined. The reason for that the nonlinearity is invariant under the affine transformations. Thus, affine equivalent S-boxes are eliminated from the search space at this step. The following proposition, which is extended form of Prop.3 of [9], gives three affine transformations among the S-boxes that are symmetric under τ.

Proposition 4.1. *Let $S : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ be a symmetric S-box under the permutation $\tau(x) = (x_0, x_2, ..., x_n, x_1)$, where $x = (x_0, x_1, ..., x_n) \in \mathbb{F}_2^{n+1}$. Then each of the following S-boxes, denoted by $T(x)$, is affine equivalent to S and symmetric under τ:*

1. *(complement) $T(x) = S^c(x)$,*
2. *(reverse) $T(x) = S(x^c)$,*
3. *(rotation) $T(x) = \tau^t(S(x))$,*

where $1 \leq t \leq n$. Moreover, the nonlinearity is invariant under these transformations.

Proof. It is clear that all three operations are affine, as $T(x) = S^c(x) = S(x) \oplus \mathbf{1}$, $T(x) = S(x^c) = S(x \oplus \mathbf{1})$, and $T(x) = \tau^t(S(x)) = S(x) \cdot A$, where A corresponds to the permutation matrix of τ and $\mathbf{1}$ denotes all-one vector. The following statements show that T is symmetric under τ:

1. $T(\tau(x)) = S^c(\tau(x)) = S(\tau(x)) \oplus \mathbf{1} = \tau(S(x)) \oplus \mathbf{1} = \tau(S^c(x)) = \tau(T(x))$,
2. $T(\tau(x)) = S(\tau^c(x)) = S(\tau(x) \oplus \mathbf{1}) = \tau(S(x \oplus \mathbf{1})) = \tau(S(x^c)) = \tau(T(x))$,
3. $T(\tau(x)) = \tau^t(S(\tau(x))) = \tau^t(\tau(S(x))) = \tau(\tau^t(S(x))) = \tau(T(x))$.

For the rest of the proof, let $\tilde{f}(x) = c \cdot S(x)$ be the component function of S corresponding to the non-zero coefficient vector $c \in \mathbb{F}_2^{n+1}$. Then, the component functions of T of 1 and 2 will be $\tilde{g}(x) = \tilde{f}(x) \oplus 1$ and $\tilde{h}(x) = \tilde{f}(x \oplus \mathbf{1})$, respectively. If the Walsh transform of $\tilde{f}$ is

$$W_{\tilde{f}}(w) = \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\tilde{f}(x)} \cdot (-1)^{w \cdot x}, \text{ where } w \in \mathbb{F}_2^{n+1},$$

then the Walsh transform of $\tilde{g}(x) = \tilde{f}(x) \oplus 1$ will be

$$\begin{aligned} W_{\tilde{g}}(w) &= \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\tilde{g}(x)} \cdot (-1)^{w \cdot x} = \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\tilde{f}(x) \oplus 1} \cdot (-1)^{w \cdot x} \\ &= -\sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\tilde{f}(x)} \cdot (-1)^{w \cdot x} = -W_{\tilde{f}}(w). \end{aligned}$$

Similarly, the Walsh spectrum of $\tilde{h}(x) = \tilde{f}(x \oplus \mathbf{1})$ will be

$$\begin{aligned} W_{\tilde{h}}(w) &= \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\tilde{h}(x)} \cdot (-1)^{w \cdot x} = \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\tilde{f}(x \oplus \mathbf{1})} \cdot (-1)^{w \cdot x} \\ &= \sum_{y \in \mathbb{F}_2^{n+1}} (-1)^{\tilde{f}(y)} \cdot (-1)^{w \cdot (y \oplus \mathbf{1})} = \begin{cases} W_{\tilde{f}}(w), & \text{if } w_H(w) \text{ is even,} \\ -W_{\tilde{f}}(w), & \text{if } w_H(w) \text{ is odd.} \end{cases} \end{aligned}$$

Thus, for all component functions $\tilde{f}$, $\tilde{g}$ and $\tilde{h}$ of S and T's of 1 and 2,

$$\max_w \{|W_{\tilde{f}}(w)|\} = \max_w \{|W_{\tilde{g}}(w)|\} = \max_w \{|W_{\tilde{h}}(w)|\}.$$

This leads to the fact that the nonlinearities of S and T's of 1 and 2 are equal. For the last transformation, observe that the rotation under τ only change the places of the coordinate functions. Therefore, the Walsh spectra of the component functions under different coefficient vector will remain the same. This implies that the nonlinearity of $T(x) = \tau^t(S(x))$ is equal to the nonlinearity of $S(x)$. □

As can be seen from Prop.4.1, the half of the search space of symmetric S-boxes under the permutation τ can be eliminated using the affine transformation $T(x) = S^c(x)$ or $T(x) = S(x^c)$. Note that these two transformations eliminate the different sets of the S-boxes that each set corresponds to the half of the search space. Moreover, sieving the S-boxes under the third affine transformation $T(x) = \tau^t(S(x))$ can also reduce the search space by the fraction of $1/n$, where $1 \leq t \leq n$.

In this study, it is aimed to enumerate and classify 6×6 bijective symmetric S-boxes under the permutation τ with nonlinearity ≥ 24. For this reason, all S-boxes are generated using improved version of Alg.1 that provides efficiency in the exhaustive search. One of the techniques that provides efficiency is to eliminate the choices of the output orbit representatives of the concatenation that leads to affine equivalence of the S-boxes. That is to say, when generating S-boxes the choices of the affine equivalence relation are skipped. This reduces the complexity of the algorithm. The other techniques used in the efficient exhaustive search algorithm will be mentioned in the following sections. Now, the next proposition defines some affine transformations among the concatenations of two rotation-symmetric S-boxes.

The circulant matrix $C^i(a)$ used in the 6th transformation of below proposition is formerly defined in [9] to determine affine equivalences among the $n \times n$ rotation-symmetric S-boxes. This matrix is formed by taking $a = (a_1, a_2, ..., a_n) \in \mathbb{F}_2^n$ as the first row and rotating each row i-bit to the left relative to the preceding row, where $1 \leq i \leq n$:

$$C^i(a) = \begin{bmatrix} a \\ \rho^i(a) \\ \vdots \\ \rho^{(n-1)i}(a) \end{bmatrix}.$$

Proposition 4.2. *Let $F = (S_1||S_2)$ be a concatenation of two $n \times n$ RSSBs S_1 and S_2. Then each of the following functions, denoted by G, is also a concatenation of two $n \times n$ RSSBs and affine equivalent to F:*

1. *(complement) $G(x_0; x) = F(x_0; x) \oplus \mathbf{1}$,*
2. *(reverse) $G(x_0; x) = F((x_0; x) \oplus \mathbf{1})$,*
3. *(left partial reverse) $G(x_0; x) = S_1(x \oplus \mathbf{1})||S_2(x)$,*

4. *(right partial reverse)* $G(x_0;x) = S_1(x)||S_2(x \oplus \mathbf{1})$,
5. *(transposition)* $G(x_0;x) = S_2(x)||S_1(x)$,
6. *(circulant matrix multiplication)* $G(x_0;x) = F((x_0;x)D^q(a))C^p(b)$,

where p and q are co-primes to n such that $pq \equiv 1\ (mod\, n)$, $D^q(a)$= $\left[\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline 0 & \\ \vdots & C^q(a) \\ 0 & \end{array}\right]$,

$a, b \in \mathbb{F}_2^n$, $(x_0;x) \in \mathbb{F}_2^{n+1}$, and $C^q(a)$, $C^p(b)$ are nonsingular circulant matrices over $\mathbb{F}_2$.

Proof. The concatenation F can be defined as $F(x_0;x) = (x_0 \oplus 1)S_1(x) + x_0 S_2(x)$ for $(x_0;x) = (x_0, x_1, ..., x_n) \in \mathbb{F}_2^{n+1}$, where $S_1$and S_2 are $n \times n$ RSSBs. By using this definition, it can be shown that each of the concatenation G is affine equivalent to F. For 1, 2 and 6, affine relation is clear.

-
$$\begin{aligned} G(x_0;x) &= S_1(x \oplus \mathbf{1})||S_2(x) = (x_0 \oplus 1)S_1(x \oplus \mathbf{1}) + x_0 S_2(x) \\ &= F(x_0, x \oplus ((x_0 \oplus 1) \cdot \mathbf{1})) \\ &= F(x_0, x_0 \oplus 1 \oplus x_1, ..., x_0 \oplus 1 \oplus x_n) \\ &= F(A \cdot x \oplus (0,1,...,1)) \text{ where } A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}. \end{aligned}$$

-
$$\begin{aligned} G(x_0;x) &= S_1(x)||S_2(x \oplus \mathbf{1}) = (x_0 \oplus 1)S_1(x) + x_0 S_2(x \oplus \mathbf{1}) \\ &= F(x_0, x \oplus (x_0 \cdot \mathbf{1})) \\ &= F(x_0, x_0 \oplus x_1, ..., x_0 \oplus x_n) \\ &= F(A \cdot x) \text{ where } A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}. \end{aligned}$$

-
$$\begin{aligned} G(x_0;x) &= S_2(x)||S_1(x) = (x_0 \oplus 1)S_2(x) + x_0 S_1(x) = F(x_0 \oplus 1; x) \\ &= F((x_0;x) \oplus (1,0,...,0)). \end{aligned}$$

□

To check the nonlinearities of these transformations, let

$$\tilde{f}_1(x) = c \cdot S_1(x) \text{ and } \tilde{f}_2(x) = c \cdot S_2(x)$$

be the component functions of S_1 and S_2, where $c \neq \mathbf{0} \in \mathbb{F}_2^{n+1}$ and $x \in \mathbb{F}_2^n$. Then, the component function $\tilde{f}$ of F will be the concatenation of these component functions for every c. If $W_{\tilde{f}_1}$ and $W_{\tilde{f}_2}$ denote the Walsh spectra of $\tilde{f}_1$ and $\tilde{f}_2$, then the Walsh spectrum of $\tilde{f} = \tilde{f}_1 || \tilde{f}_2$ will be

$$W_{\tilde{f}} = [W_{\tilde{f}_1} + W_{\tilde{f}_2}, W_{\tilde{f}_1} - W_{\tilde{f}_2}].$$

Thus, the maximum of the absolute of the Walsh spectrum of $\tilde{f}$ is

$$\max_w \{|W_{\tilde{f}_1}(w)| + |W_{\tilde{f}_2}(w)|\}.$$

As can be seen from Prop.4.1, the component functions of $S_1^c(x)$, $S_2^c(x)$, $S_1(x^c)$ and $S_2(x^c)$ are $\tilde{f}_1(x) \oplus \mathbf{1}$, $\tilde{f}_2(x) \oplus \mathbf{1}$, $\tilde{f}_1(x \oplus \mathbf{1})$ and $\tilde{f}_2(x \oplus \mathbf{1})$, and their Walsh spectra are $-W_{\tilde{f}_1}$, $-W_{\tilde{f}_2}$, $\mp W_{\tilde{f}_1}$ and $\mp W_{\tilde{f}_2}$, respectively. Hence, the maximum of the absolute of the Walsh spectra of the concatenations

$$\tilde{f}_1(x) \oplus \mathbf{1} || \tilde{f}_2(x) \oplus \mathbf{1},\ \tilde{f}_1(x \oplus \mathbf{1}) || \tilde{f}_2(x \oplus \mathbf{1}),\ \tilde{f}_1(x \oplus \mathbf{1}) || \tilde{f}_2(x),\ \tilde{f}_1(x) || \tilde{f}_2(x \oplus \mathbf{1}),$$

and $\tilde{f}_2(x) || \tilde{f}_1(x)$ will remain the same as of $\tilde{f}$. This brings out that the nonlinearities of all are equal and the minimum of the nonlinearities of the component functions does not change. In other words, the nonlinearity of F is invariant under the transformations of G.

Note that taking complement of only one RSSB in the concatenation, i.e. $G = S_1^c || S_2$ or $G = S_1 || S_2^c$, does not lead to a bijective S. To exemplify, without taking into account of the rotations and permutations, take the output orbit representatives of S_1 from the Ex.3.1. Then, the output orbit representatives of S_1 and S_2 will be

$$S_1 = (\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_7, \Lambda_7, \Lambda_2, \Lambda_3, \Lambda_1) \text{ and } S_2 = (\Lambda_8, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_2, \Lambda_3, \Lambda_1).$$

If the complement of S_1 is taken under the transformation of $G = S_1^c || S_2$, then the output orbit representatives of S_1 will be

$$S_1^c = (\Lambda_1, \Lambda_6, \Lambda_6, \Lambda_2, \Lambda_2, \Lambda_7, \Lambda_5, \Lambda_8),$$

since $\Lambda_1^c = \Lambda_8$, $\Lambda_2^c = \Lambda_7$, $\Lambda_3^c = \Lambda_5$ and $\Lambda_4^c = \Lambda_8$. Clearly, the concatenation $G = S_1^c || S_2$ does not contain all orbit representatives two times, even it does not have the orbit representative Λ_4. Hence, the S-box S constructed by G can not be bijective. Similarly, taking the complement of only S_2 also fails the bijectivity of S. For this reason, these transformations are not considered in Prop.4.2.

Using these transformations (or their compositions) the aforementioned choices for the output orbit representatives, which generate affine equivalent S-boxes as shown by the next proposition, are sieved.

Proposition 4.3. *Let $S = (f, F)$ be an $(n+1) \times (n+1)$ symmetric S-box under the permutation $\tau(\bar{x}) = (x_0, x_2, ..., x_n, x_1)$, where $\bar{x} = (x_0, x_1, ..., x_n) \in \mathbb{F}_2^{n+1}$, f is an $(n+1)$-variable Boolean function, and F is a concatenation of two $n \times n$ RSSBs. Assume that G, also a concatenation of two $n \times n$ RSSBs, is obtained by the affine transformations given by Prop.4.2. Then, there exists an $(n+1)$-variable Boolean function g such that $T = (g, G)$ is symmetric under τ and affine equivalent to S.*

Proof. It is easy to prove for the first five affine transformations in Prop.4.2. Let us consider the last one, i.e., circulant matrix multiplication. Then, we have

$$\begin{aligned} T(\bar{x}) &= (g(\bar{x}), G(\bar{x})) \\ &= (f(\bar{x}D^q(a)), F(\bar{x}D^q(a))C^p(b)) \\ &= (f(\bar{x}D^q(a)), F(\bar{x}D^q(a)))D^p(b) \\ &= S(\bar{x}D^q(a))D^p(b), \end{aligned}$$

where $g(\bar{x}) = f(\bar{x}D^q(a))\ \forall \bar{x} \in \mathbb{F}_2^{n+1}$, which shows that S and T are affine equivalent. Next, we get the following:

$$\begin{aligned} T(\tau(\bar{x})) &= S(\tau(\bar{x})D^q(a))D^p(b) \\ &= (f(\tau(\bar{x})D^q(a)), F(\tau(\bar{x})D^q(a))C^p(b)) \\ &= (f(x_0, \rho(x)C^q(a)), F(x_0, \rho(x)C^q(a))C^p(b)) \\ &= (f(x_0, \rho^{n-q}(xC^q(a))), F(x_0, \rho^{n-q}(xC^q(a)))C^p(b)) \\ &= (f(\tau^{n-q}(x_0, xC^q(a))), \rho^{n-q}(F(x_0, xC^q(a)))C^p(b)) \\ &= (f(x_0, xC^q(a)), \rho^{(n-q)(n-p)}(F(x_0, xC^q(a))C^p(b))) \\ &= (f(x_0, xC^q(a)), \rho(F(x_0, xC^q(a))C^p(b))) \\ &= (f(\bar{x}D^q(a)), \rho(F(\bar{x}D^q(a))C^p(b))) \\ &= \tau(S(\bar{x}D^q(a))D^p(b)) \\ &= \tau(T(\bar{x})), \end{aligned}$$

which follows from the fact that $\rho(x)C^q(a) = \rho^{n-q}(xC^q(a))$, where ρ is the cyclic shift operator. Hence, T is also symmetric under τ. □

As said before, when generating S-boxes, the choices of the output orbit representatives of S_1 and S_2 that lead to affine equivalent S-boxes are eliminated. Without taken into consideration of rotation of any orbit representative or permutations of them, the intermediate orbit representatives of S_1 determine the ones of S_2. Since $\mathbb{S}_0 = 1$ and $|\mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)| = 6$, which is the permutation set of output orbit representatives of size 1, there are 6 choices for the output orbit representatives of F. Similarly, there are 180, 540 and 120 choices if the orbit representatives of size 5 of S_1 in $\mathbb{S}_1$, $\mathbb{S}_2$ and $\mathbb{S}_3$, respectively. After sieving those yielding affine equivalent concatenations, these numbers are reduced to 2, 8, 21, and 9, respectively. In Tab.4.1, the remaining orbit representative choices for each $\mathbb{S}_k$ after the elimination are given along with the number of S-boxes they generate under the affine transformations given by Prop.4.2.

In addition, it is clear that any S-box obtained by rotating all of the outputs of an RSSB by the same number of positions is also an RSSB and this operation is an affine transformation (This relation is presented by [9] in Prop.3 and it corresponds to third item of Prop.4.1 in this construction). Hence, to remove such transformations the first one of the output orbit representative of size 5 of S_1, i.e. $S_1(\Lambda_2) = F(0; \Lambda_2)$, can be fixed by an orbit representative. The fifth loop of the Alg.1, includes all of the rotations of each orbit representatives of size 5. To fix the first one makes 5^{11} rotations in the concatenation. As a result, the search space is reduced by a factor of $\frac{1}{5}$.

At the end of this step, the number of S-boxes in Set-k for $k = 0, 1, 2, 3$ reduces from $2^{57.43}$, $2^{60.34}$, $2^{59.92}$, and $2^{55.75}$ to $2^{53.52}$, $2^{53.52}$, $2^{52.92}$, and $2^{49.69}$, respectively. Hence, the total search space reduces from $2^{61.28}$ to $2^{54.97}$.

4.2 Sieving Rotation-symmetric S-boxes S_1 and S_2

In the set of Boolean functions, bent functions have the highest nonlinearity. However, they are not balanced. Thus, using them for an S-box is not convenient since they do not help to bijectivity, and so they do not serve the purpose. Instead, the Boolean functions that are balanced, and the nonlinearity of which is relatively close to the nonlinearity of bent functions are preferably used. In [25], it is stated that for even number of input variables n the maximum nonlinearity of a bent function is $2^{n-1} - 2^{\frac{n}{2}-1}$. In this case, this corresponds to 28. Hence, the nonlinearity of balanced Boolean functions that are used in this construction, should be maximum and less than 28. Moreover, according to [6], the maximum nonlinearity among the 6-variable balanced Boolean functions is 24. For this reason, the search space of 6×6 bijective S-boxes is restricted with the ones having nonlinearity ≥ 24.

To determine the boundary of the nonlinearities of the rotation-symmetric S-boxes S_1 and S_2, check out the Prop.2.6. In the event of the nonlinearity of $S \geq 24$, the maximum value of the absolute of the Walsh spectrum of f will be ≤ 16, and the maximum value of the absolute of the Walsh spectra of all coordinate functions that are composed to obtain the concatenation $F = S_1||S_2$ and their component functions will also be ≤ 16. Then, the addition of the maximum of the absolute of the Walsh spectra of S_1 and S_2 will be ≤ 16. Thus, the nonlinearities of S_1 and S_2 will be ≥ 8. On the other hand, $\beta_F = 16$ implies that $\mathcal{N}_{S_1}$ and $\mathcal{N}_{S_2} \geq 8$, by Prop.2.6. Therefore, when generating rotation-symmetric S-boxes S_1 and S_2, the nonlinearities of both of them are checked and sieved the ones having nonlinearity < 8.

By examining the output orbit representatives in Tab.4.1, one can find out that for some choices of the output orbit representatives there is no rotation-symmetric S-box with nonlinearity ≥ 8 generated by them. Specifically, for the sets of $\mathbb{S}_2$ and $\mathbb{S}_3$, 6 out of the 21 choices for $\mathbb{S}_2$, 3 out of the 9 choices for $\mathbb{S}_3$ in Tab.4.1 generate neither S_1 nor S_2 with nonlinearity ≥ 8, and hence they are removed from the search space. These eliminated choices are N_5, N_7, N_{11}, N_{13}, N_{18}, N_{20} for $\mathbb{S}_2$ and N_3, N_6, N_9 for $\mathbb{S}_3$. Thus, after this pre-processing, the search space slightly reduces from $2^{54.97}$ to $2^{54.86}$.

Table 4.1: The representative choices after the first step and the number (N_i) of affine equivalent choices to the concatenation $S_1||S_2$ for $\mathbb{S}_k$, $k = 0, 1, 2, 3$

	$\boldsymbol{i}$	$\boldsymbol{S_1}$	$\boldsymbol{S_2}$	$\boldsymbol{N_i}$
$\mathbb{S}_\mathbf{0}$	**1**	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)}$	$\boldsymbol{(\Lambda_8, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)}$	**2**
	2	$(\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)$	4
$\mathbb{S}_\mathbf{1}$	**1**	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_1)}$	$\boldsymbol{(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)}$	**6**
	2	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8)$	24
	3	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)}$	$\boldsymbol{(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)}$	**12**
	4	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	6
	5	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)$	12
	6	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	24
	7	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_7, \Lambda_8)}$	$\boldsymbol{(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)}$	**48**
	8	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)$	48
$\mathbb{S}_\mathbf{2}$	1	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	12
	2	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	12
	3	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8)$	24
	4	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8)$	24
	5	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	12
	6	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_7, \Lambda_1)}$	$\boldsymbol{(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8)}$	**12**
	7	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	6
	8	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_8)$	12
	9	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_8)$	$(\Lambda_1, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	12
	10	$\boldsymbol{(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_7, \Lambda_8)}$	$\boldsymbol{(\Lambda_1, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)}$	**24**
	11	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	12
	12	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_7, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)$	12
	13	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	6
	14	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_8)}$	$\boldsymbol{(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)}$	**48**
	15	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_8)}$	$\boldsymbol{(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)}$	**24**
	16	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)$	96
	17	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_8)}$	$\boldsymbol{(\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)}$	**48**
	18	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	48
	19	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)$	48
	20	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	24
	21	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_7, \Lambda_8)}$	$\boldsymbol{(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_1)}$	**24**
$\mathbb{S}_\mathbf{3}$	1	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_1)$	$(\Lambda_8, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	6
	2	$\boldsymbol{(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_1)}$	$\boldsymbol{(\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)}$	**12**
	3	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_7, \Lambda_7, \Lambda_8)$	2
	4	$\boldsymbol{(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_8)}$	$\boldsymbol{(\Lambda_1, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)}$	**6**
	5	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_8)$	$(\Lambda_1, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	12
	6	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_7, \Lambda_7, \Lambda_1)$	2
	7	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_8)$	$(\Lambda_8, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	24
	8	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_8)$	$(\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	48
	9	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_7, \Lambda_7, \Lambda_1)$	8

In addition, each of the Walsh spectra of the component functions of S_1 and S_2 are analyzed since even if both of S_1 and S_2 have nonlinearity ≥ 8, their concatenation F may not have the nonlinearity ≥ 24. If this is the case, the nonlinearity of S never be ≥ 24. For this reason, for each of the generated concatenation the following condition should be checked. Since $\beta_F = 16$,

$$\begin{aligned}
\max_{u\in\mathbb{F}_2^5}\{|W_g(u)| + |W_h(u)|\} \leq 16 \implies W_g(u) &\leq 0 \qquad \text{and} \qquad W_h(u) \leq 16,\\
W_g(u) &\leq 2 \qquad \text{and} \qquad W_h(u) \leq 14,\\
&\ \ \vdots\\
W_g(u) &\leq 16 \qquad \text{and} \qquad W_h(u) \leq 0,
\end{aligned}$$

where g and h are component functions of S_1 and S_2. This leads to 9 restrictions where if the maximum value of the absolute of the Walsh spectra of g is less than or equal to w, then the maximum value of the absolute of the Walsh spectra of h will be less than or equal to $16 - w$ for $w \in \{0, 2, ..., 16\}$. Under these conditions the nonlinearities of each S_1 and S_2 are checked.

While checking the nonlinearities, an efficient sieving method can be applied to reduce the number of choices for the output orbit representatives of S_1 and S_2. This method can be summarized below:

1. Let the sets Ω_1 and Ω_2 contain all the S_1's and S_2's generated from one of the remaining choices after the above elimination, respectively.

2. Let the subset $\Omega_1^{[w,(u,c)]}$ of Ω_1 denote the S_1's for which the absolute value of the Walsh spectrum of a component function $c \cdot S_1$ at a position $u \in \mathbb{F}_2^5$ is equal to w, i.e. $|W_{S_1}(u, c)| = w$, where $c \in \mathbb{F}_2^{5*}$ and $w \in \{0, 2, ..., 16\}$.

3. For any given the triplet $[w, (u, c)]$, constitute the subsets $\Omega_2^{[0,(u,c)]}$, $\Omega_2^{[2,(u,c)]}$,..., $\Omega_2^{[16-w,(u,c)]}$ of Ω_2, successively.

   As can be seen, the S_1's in $\Omega_1^{[u,(w,c)]}$ can be concatenated only with the S_2's in $\cup_{i\in\{0,2,...,16-w\}}\Omega_2^{[i,(u,c)]}$, since otherwise the nonlinearity of the concatenation F can not reach to or exceed 24, leading to the fact that the nonlinearity of S is less than 24.

4. If there is no S_2 in $\cup_{i\in\{0,2,...,16-w\}}\Omega_2^{[i,(u,c)]}$, then update Ω_1 by $\Omega_1 \setminus \Omega_1^{[w,(u,c)]}$.

Note that the set Ω_2 can also be updated similarly considering the concatenations formed by the S_2's in $\Omega_2^{[w,(u,c)]}$ and S_1's in $\cup_{i\in\{0,2,...,16-w\}}\Omega_1^{[i,(u,c)]}$. In this way, all 9 restrictions above are checked efficiently by reducing the search space.

There is also a reduction in the coefficient vectors of S_1 and S_2. Recall from [9] that the component functions of which their coefficients belongs to the same orbit are affine equivalent. That is, their absolute Walsh distributions are equal. Thus, it is sufficient to apply this procedure only for the coefficient vectors that are equal to orbit representatives. In this structure, for S_1 and S_2 there are 7 coefficient vectors (out of 31) to compute the Walsh spectra of the seven different component functions. This makes a reduction in the number of computations.

Hence, the above method is performed for all the triplets $[w, (u, c)]$, where the c's are coefficient vectors, and it is found that the updated sets Ω_1 and Ω_2 are empty for some of the remaining choices in Tab.4.1. More specifically, these choices are N_1 for $\mathbb{S}_0$, N_2, N_4, N_5, N_6, N_8 for $\mathbb{S}_1$, N_1, N_2, N_3, N_4, N_8, N_9, N_{12}, N_{16}, N_{19} for $\mathbb{S}_2$, and N_1, N_5, N_7, N_8 for $\mathbb{S}_3$. Thus, the search space reduces from $2^{54.86}$ to $2^{53.63}$. In Tab.4.1, the choices left after the first two steps of the search strategy are shown by bold font.

In the algorithm below, the set Ω_1 of S_1's after the elimination of the ones having non-linearity < 8, are updated by the procedure given above. The updated set of Ω_1 is denoted by $\overline{\Omega_1}$. Similarly, this algorithm is applied to the set Ω_2 of S_2's to check the Walsh value restrictions for S_2.

```
Input: $\Omega_1$ and $\Omega_2$
Output: $\overline{\Omega_1}$
for each $w \in \{0, 2, ..., 16\}$ do
    for each coefficient vector $c \in \{\Lambda_1, \Lambda_2, ..., \Lambda_8\}$ do
        for each position $u$ of the Walsh spectrum $W_{S_1}$ of $S_1$ do
            for each $S_1 \in \Omega_1$ do
                Compute $W_{S_1}(u, c)$;
                if $W_{S_1}(u, c) = w$ then
                    Record $S_1$ into $\Omega_1^{[w,(u,c)]}$;
                end
            end
            for each $S_2 \in \Omega_2$ do
                Compute $W_{S_2}(u, c)$;
                for each $i \in \{0, 2, ..., 16 - w\}$ do
                    if $W_{S_2}(u, c) = i$ then
                        Record $S_2$ into $\Omega_2^{[i,(u,c)]}$;
                        Break;
                    end
                end
            end
            if $\Omega_2^{[0,(u,c)]} \cup \Omega_2^{[2,(u,c)]} \cup ... \cup \Omega_2^{[16-w,(u,c)]} = \emptyset$ then
                Update $\Omega_1$ by $\Omega_1 \setminus \Omega_1^{[w,(u,c)]}$;
            end
        end
    end
end
$\overline{\Omega_1} = \Omega_1$;
```

Algorithm 2: Sieving S_1's that can not be concatenated with any $S_2 \in \Omega_2$.

4.3 Sieving Concatenations with Nonlinearity < 24

This section is divided to mention the last step of the process of the search algorithm. Until this stage, the rotation-symmetric S-boxes S_1's and S_2's were generated according to the output orbit representatives which remain after the elimination of the ones leading to the affine equivalent concatenations and the ones making the nonlinearity of both S_1 and S_2 less than 8. Denoting these sets by Ω_1 and Ω_2, a nonlinearity check was done for all component functions of each possible concatenation of S_1 in Ω_1 and S_2 in Ω_2. Some of the S_1's for which there is no S_2 to be concatenated with under the nonlinearity condition were eliminated from Ω_1 by an efficient sieving method. Similarly, S_2's were also eliminated from Ω_2. Now, at this stage all possible concatenations of the updated sets of Ω_1 and Ω_2 are extracted. Then, the nonlinearity check similar to the one in the previous section is done for all constructed $S_1||S_2$'s and the concatenations with nonlinearity less than 24 are eliminated. Consequently, all possible 6-variable coordinate functions f's with nonlinearity ≥ 24, which also make S bijective, are added to these concatenations. This constructs the S-boxes S's having nonlinearity at least 24.

Recall that the sets $\overline{\Omega_1}$ and $\overline{\Omega_2}$ denote the sets of S_1's and S_2's after the elimination in the previous step, respectively. Having all S_1's and S_2's that help to the construction, the steps required to generate all 6×6 bijective S-boxes including the last sieving method for the concatenations can be summarized below:

1. For any given triplet $[w, (u, c)]$, constitute the subsets $\overline{\Omega_1}^{[w,(u,c)]}$ and $\cup_{i \in \{0,2,\dots,16-w\}} \overline{\Omega_2}^{[i,(u,c)]}$ of $\overline{\Omega_1}$ and $\overline{\Omega_2}$, respectively.
2. For each of the S_1's in the former subset and each of the S_2's in the latter one, constitute the concatenation $F = S_1||S_2$.
3. If the nonlinearity of $F \geq 24$ for some S_1 and S_2, then add each possible coordinate function f to F to form the S-box $S = (f, S_1||S_2)$.
4. If the nonlinearity of S is ≥ 24, then record S into a file.

   Note that as in the preceding step, the S_1's in $\overline{\Omega_1}^{[w,(u,c)]}$ can not be concatenated with any S_2 in $\overline{\Omega_2}$ except those in $\cup_{i \in \{0,2,\dots,16-w\}} \overline{\Omega_2}^{[i,(u,c)]}$.
5. After the nonlinearity check for all S constructed by S_1's in $\overline{\Omega_1}^{[w,(u,c)]}$ and S_2's in $\cup_{i \in \{0,2,\dots,16-w\}} \overline{\Omega_2}^{[i,(u,c)]}$, update $\overline{\Omega_1}$ by $\overline{\Omega_1} \setminus \overline{\Omega_1}^{[w,(u,c)]}$.

   Note also that when eliminating S_1's in $\overline{\Omega_1}^{[w,(u,c)]}$, the ones belonging to the other subsets of Ω_1 are also eliminated. This provides efficiency in the process by reducing the search space.

Furthermore, there is also a reduction in the coordinate functions. Recall that according to the structure of the concatenation $F = S_1||S_2$, there can be 2^8 6-variable Boolean functions to be added as the first coordinate function of S. This number comes from the number of output orbit representatives of S_1 and S_2. Since all orbits are double, it is enough to determine f values for the one of these double orbits, and since f takes the same value for all elements of the same orbit, there are 2^8 different f to be used as the first coordinate function of S. Moreover, the nonlinearities of $S = (f, F)$ and $T = (f^c, F)$ are the same, where f^c is the complement of f. If $f(\mathbf{0}) = 0$ is fixed, the complements of 2^7 coordinate functions are eliminated. This reduces the search space by half.

Finally, by performing this procedure for all the triplets $[w, (u, c)]$, the search space is reduced to $2^{48.47}$. This means that all 6×6 bijective symmetric S-boxes under the permutation τ with nonlinearity ≥ 24 are generated efficiently by a non-negligible reduction in the search space. The algorithm for the last step is presented below:

```
Input: $\overline{\Omega_1}$ and $\overline{\Omega_2}$
Output: The set of $S$'s
for each $w \in \{0, 2, ..., 16\}$ do
    for each coefficient vector $c \in \{\Lambda_1, \Lambda_2, ..., \Lambda_8\}$ do
        for each position $u$ of the Walsh spectrum $W_{S_1}$ of $S_1$ do
            for each $S_1 \in \overline{\Omega_1}$ do
                Compute $W_{S_1}(u, c)$;
                if $W_{S_1}(u, c) = w$ then
                    Record $S_1$ into $\overline{\Omega_1}^{[w,(u,c)]}$;
                end
            end
            for each $S_2 \in \overline{\Omega_2}$ do
                Compute $W_{S_2}(u, c)$;
                for each $i \in \{0, 2, ..., 16 - w\}$ do
                    if $W_{S_2}(u, c) = i$ then
                        Record $S_2$ into $\overline{\Omega_2}^{[i,(u,c)]}$;
                        Break;
                    end
                end
            end
            for each $S_1 \in \overline{\Omega_1}^{[w,(u,c)]}$ do
                for each $S_2 \in \overline{\Omega_2}^{[0,(u,c)]} \cup ... \cup \Omega_2^{[16-w,(u,c)]}$ do
                    Construct $F = S_1||S_2$;
                    if the nonlinearity of $F \geq 24$ then
                        Construct all elements of $\mathcal{F}$ according to the output of $F$;
                        for each $f \in \mathcal{F}$ do
                            Add $f$ as the first coordinate function to $S$ and
                            construct $S = (f, S_1||S_2)$;
                            if the nonlinearity of $S \geq 24$ then
                                Record $S$ into the file;
                            end
                        end
                    end
                end
            end
            Update $\overline{\Omega_1}$ by $\overline{\Omega_1} \setminus \overline{\Omega_1}^{[w,(u,c)]}$;
        end
    end
end
```

Algorithm 3: Sieving F with nonlinearity < 24 and constructing all 6×6 bijective S-boxes with nonlinearity ≥ 24.

CHAPTER 5

RESULTS

In consequence of the three-step procedure, in the class of 6×6 bijective S-boxes that are symmetric under the permutation τ, there are $2^{37.56}$ S-boxes with nonlinearity 24 and there is no S-box exceeding this nonlinearity. Further, among these S-boxes, the best differential uniformity is 4 and the number of differentially 4-uniform S-boxes is $2^{33.99}$. In [9], the S-boxes with the same cryptographic properties are enumerated in the class of bijective RSSBs for which the search space is of size $2^{47.90}$. In this class, it has been found that there are $2^{28.25}$ S-boxes with nonlinearity 24 and among them the number of those that are differentially 4-uniform is $2^{24.74}$. Compared to these results, this search identifies a much larger set of S-boxes achieving the same cryptographic properties than those found in [9].

For the classification of S-boxes in terms of transparency order (TO), the statements about the TO of the affine equivalent S-boxes are followed in the literature. One of these statements proposes [7] that if S is an $n \times n$ S-box and γ_S is its transparency order, then the transparency order γ_T of $T(x) = S(xA \oplus d) \oplus e$ is equal to γ_S, where A is a nonsingular binary matrix and $d, e \in \mathbb{F}_2^n$. The other proposes [10] that the transparency order of $T(x) = S(x) \cdot B$ is invariant under the column permutation of B, where B is a nonsingular binary matrix. However, the TOs of affine equivalent S-boxes obtained by the circulant matrix multiplication are not invariant under this transformation. Starting from this point of view, after the search is completed, the S-boxes which are affine equivalent under the transformation of the 6th item of Prop.4.2 are generated since they can have different TOs. Recall that in the search strategy all affine equivalent S-boxes under the transformations of Prop.4.2 were eliminated, i.e. at the stage of generation, the choices for the orbit representatives that lead to affine equivalent concatenations were skipped. For this reason, the transformation of the generated S-boxes by the circulant matrix multiplications are also generated and their TOs are classified.

The classification of the $2^{33.99}$ differentially 4-uniform S-boxes with respect to the absolute indicator (AI), algebraic degrees ($d_{\min}$ and $d_{\max}$) and transparency order (TO) is presented in Tab.5.1. Recall that $d_{\min}$ is the minimum algebraic degree among the component functions of the S-boxes and $d_{\max}$ is the maximum algebraic degree among the coordinate functions of the S-boxes. The classification results for the partitioned sets of the search space, i.e. Set-k for $k = 0, 1, 2, 3$, are also tabled in Tab.5.2, Tab.5.3, Tab.5.4, and Tab.5.5. As can be seen, the numbers of differentially 4-uniform S-boxes with nonlinearity 24 belonging to the Set-0, Set-1, Set-2 and Set-3 are $2^{29.91}$, $2^{32.87}$, $2^{32.82}$, and $2^{29.09}$, respectively. Moreover, by looking through the Tab.5.1, it is observed that the minimum transparency order the S-boxes have in this classification is 5.270. This value is attained from the Set-2 and Set-3 in the tables Tab.5.4 and Tab.5.5 (shown by bold font).

One of the 6×6 bijective S-boxes having the best value of TO (5.270), the best nonlinearity 24, the best differential uniformity 4 among the generated S-boxes in the consequence of this efficient exhaustive search algorithm is presented below in decimal form:

$$\begin{aligned} S = \quad & (0,1,2,35,4,26,38,34,8,22,21,3,44,12,36,54,16,49,13,33,11,17,\\ & 6,43,56,48,24,53,40,58,45,32,63,42,52,62,41,28,61,60,50,7,25,\\ & 18,59,10,57,29,37,47,14,46,19,9,5,30,55,39,20,15,51,23,27,31). \end{aligned}$$

The absolute indicator of this S-box is 64, the algebraic degrees $d_{\min}$ and $d_{\max}$ are 2 and 4.

In the tables, the numbers of the S-boxes are the multiples of 10. This comes from the search strategy due to the reduction of 5 rotations of each concatenation of F and the reduction of the complements of the coordinate functions f's for each S-box $S = (f, F)$. Recall that using the third item of Prop.4.1, $F(0; \Lambda_2)$ was fixed in the first step of the search algorithm to eliminate the affine equivalent concatenations. This reduced the search space by a factor of $\frac{1}{5}$. In the final step, the half of the 2^8 coordinate functions f's were eliminated by fixing the $f(\mathbf{0}) = 0$. This also reduced the search space by a factor of $\frac{1}{2}$.

As a remark, the search algorithm is performed on a workstation with 2 CPUs of Intel Xeon Processor E5-2620v3 (15M Cache, 2.40 GHz, 6 cores) and 16 GB RAM under Windows 8.1 Professional 64-bit operating system. It takes around 10 days (236 hours) exploiting all the cores.

Table 5.1: The classification of the 6×6 bijective differentially 4-uniform S-boxes with nonlinearity 24 which are constructed by the concatenation of RSSBs

AI	$d_{\min}$	$d_{\max}$	**TO**	**Number of S-boxes**
24	3	4	$\geq 5.619, \leq 5.786$	10368×10
24	4	4	$\geq 5.413, \leq 5.889$	42695424×10
32	3	4	$\geq 5.548, \leq 5.849$	165888×10
32	4	4	$\geq 5.349, \leq 5.905$	629213184×10
32	4	5	$\geq 5.607, \leq 5.813$	10368×10
40	4	4	$\geq 5.421, \leq 5.905$	97096320×10
48	4	4	$\geq 5.480, \leq 5.889$	3400704×10
64	2	2	$\geq 5.714, \leq 5.714$	5184×10
64	2	3	$\geq 5.381, \leq 5.873$	730944×10
64	2	4	$\geq \mathbf{5.270}, \leq 5.905$	176613696×10
64	3	3	$\geq 5.500, \leq 5.905$	383616×10
64	3	4	$\geq 5.341, \leq 5.905$	753769152×10
64	3	5	$\geq 5.655, \leq 5.817$	10368×10
64	4	4	$\geq 5.607, \leq 5.770$	10368×10

Table 5.2: The classification of the 6×6 bijective differentially 4-uniform S-boxes with nonlinearity 24 which are constructed by the concatenation of RSSBs in the Set-0

AI	$d_{\min}$	$d_{\max}$	**TO**	**Number of S-boxes**
24	3	4	$\geq 5.619, \leq 5.730$	288×40
24	4	4	$\geq 5.440, \leq 5.889$	438336×40
32	3	4	$\geq 5.655, \leq 5.734$	288×40
32	4	4	$\geq 5.421, \leq 5.905$	9214560×40
32	4	5	$\geq 5.675, \leq 5.738$	288×40
40	4	4	$\geq 5.448, \leq 5.905$	1978848×40
48	4	4	$\geq 5.500, \leq 5.845$	126144×40
64	2	2	$\geq 5.714, \leq 5.714$	288×40
64	2	3	$\geq 5.381, \leq 5.873$	26496×40
64	2	4	$\geq 5.302, \leq 5.885$	2320704×40
64	3	3	$\geq 5.540, \leq 5.905$	25632×40
64	3	4	$\geq 5.341, \leq 5.905$	11161440×40
64	4	4	$\geq 5.607, \leq 5.770$	288×40

Table 5.3: The classification of the 6×6 bijective differentially 4-uniform S-boxes with nonlinearity 24 which are constructed by the concatenation of RSSBs in the Set-1

AI	$d_{\min}$	$d_{\max}$	TO	Number of S-boxes
24	3	4	$\geq 5.619, \leq 5.778$	3456×10
24	4	4	$\geq 5.417, \leq 5.889$	20560896×10
32	3	4	$\geq 5.556, \leq 5.849$	91008×10
32	4	4	$\geq 5.349, \leq 5.905$	290878848×10
32	4	5	$\geq 5.667, \leq 5.813$	3456×10
40	4	4	$\geq 5.429, \leq 5.905$	43205760×10
48	4	4	$\geq 5.480, \leq 5.889$	1359360×10
64	2	2	$\geq 5.714, \leq 5.714$	1152×10
64	2	3	$\geq 5.381, \leq 5.873$	271872×10
64	2	4	$\geq 5.341, \leq 5.905$	80786304×10
64	3	3	$\geq 5.500, \leq 5.905$	118656×10
64	3	4	$\geq 5.361, \leq 5.905$	350350848×10
64	3	5	$\geq 5.655, \leq 5.817$	4608×10
64	4	4	$\geq 5.607, \leq 5.770$	3456×10

Table 5.4: The classification of the 6×6 bijective differentially 4-uniform S-boxes with nonlinearity 24 which are constructed by the concatenation of RSSBs in the Set-2

AI	$d_{\min}$	$d_{\max}$	TO	Number of S-boxes
24	3	4	$\geq 5.619, \leq 5.786$	5760×10
24	4	4	$\geq 5.413, \leq 5.889$	19401984×10
32	3	4	$\geq 5.548, \leq 5.849$	71424×10
32	4	4	$\geq 5.349, \leq 5.905$	280242432×10
32	4	5	$\geq 5.607, \leq 5.813$	5760×10
40	4	4	$\geq 5.421, \leq 5.905$	41551488×10
48	4	4	$\geq 5.480, \leq 5.889$	1299456×10
64	2	2	$\geq 5.714, \leq 5.714$	2304×10
64	2	3	$\geq 5.381, \leq 5.873$	313344×10
64	2	4	$\geq \mathbf{5.270}, \leq 5.905$	81669888×10
64	3	3	$\geq 5.500, \leq 5.905$	110592×10
64	3	4	$\geq 5.361, \leq 5.905$	333317376×10
64	3	5	$\geq 5.655, \leq 5.817$	5760×10
64	4	4	$\geq 5.607, \leq 5.770$	5760×10

Table 5.5: The classification of the 6×6 bijective differentially 4-uniform S-boxes with nonlinearity 24 which are constructed by the concatenation of RSSBs in the Set-3

AI	$\boldsymbol{d_{\min}}$	$\boldsymbol{d_{\max}}$	**TO**	**Number of S-boxes**
24	4	4	$\geq 5.468, \leq 5.873$	979200×10
32	3	4	$\geq 5.599, \leq 5.746$	2304×10
32	4	4	$\geq 5.417, \leq 5.873$	21233664×10
40	4	4	$\geq 5.460, \leq 5.865$	4423680×10
48	4	4	$\geq 5.516, \leq 5.837$	237312×10
64	2	2	$\geq 5.714, \leq 5.714$	576×10
64	2	3	$\geq 5.500, \leq 5.794$	39744×10
64	2	4	$\geq \mathbf{5.270}, \leq 5.873$	4874688×10
64	3	3	$\geq 5.540, \leq 5.778$	51840×10
64	3	4	$\geq 5.341, \leq 5.873$	25455168×10

CHAPTER 6

CONCLUSION

From ancient times till the present, the ciphers of symmetric cryptography have been a path holding the secrets of mankind, providing the people to securely communicate in the existence of the adversaries. Due to the practical reasons in the implementations they present, the ciphers of that kind are still widely used in the areas of security, and so studied. One of the classes of this cryptography, the one mostly preferred, are block ciphers, and the most important part of the block ciphers are the S-boxes since the security of these ciphers mainly relies on them. In essence, the S-boxes are mathematical structures transforming a tuple of input in certain size to another tuple of output in that size such that the output should look like random. Thus, their design is based on combinatorial properties which gives the best randomness.

In this thesis, a construction method for the 6×6 bijective S-boxes, which relies on the concatenation of 5×5 rotation-symmetric S-boxes, is introduced. Carrying the properties of rotation-symmetric S-boxes and taking the computational advantages of the concatenations in terms of nonlinearity, the concatenation method presents a larger and richer class of S-boxes than the class of 6×6 rotation-symmetric S-boxes with regard to the best known nonlinearity 24. This mentioned class corresponds to the S-boxes that are symmetric under the permutation $\tau(x) = (x_0, x_2, x_3, x_4, x_5, x_1)$, where $x = (x_0, x_1, ..., x_5) \in \mathbb{F}_2^6$.

Additionally, to enumerate these S-boxes, the ones with the nonlinearity ≥ 24, an efficient exhaustive search algorithm is proposed. This algorithm, which includes the sieving methods to eliminate the components of these S-boxes that lead to affine equivalent S-boxes and that violate the nonlinearity condition, reduces the search space from $2^{61.28}$ to $2^{48.47}$. Carrying out the search algorithm, among the generated S-boxes under this construction, differentially 4-uniform ones are classified in terms of absolute indicator, algebraic degree and transparency order.

As a result of this search, a large pool of 6×6 bijective S-boxes, which have desirable cryptographic properties with respect to high nonlinearity and low differential uniformity, is generated. The size of this pool is about $2^{33.99}$ and these cryptographically robust S-boxes can be used in any application that requires small-size S-boxes.

In the background of this research, the concatenation of S-boxes, the concatenation of RSSBs and the structure of this construction are studied. To eliminate affine equivalent

S-boxes, affine transformations of the symmetric S-boxes under the permutation τ are also studied. Hence, these materials and this search strategy can be used to generate another constructions. Furthermore, this concatenation method can also be applied to the S-boxes in higher dimensions.

REFERENCES

[1] E. Biham and A. Shamir, Differential cryptanalysis of des-like cryptosystems, Journal of CRYPTOLOGY, 4(1), pp. 3–72, 1991.

[2] A. Biryukov, C. De Canniere, A. Braeken, and B. Preneel, A toolbox for cryptanalysis: Linear and affine equivalence algorithms, in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 33–50, Springer, 2003.

[3] A. Canteaut and M. Videau, Symmetric boolean functions, IEEE Transactions on information theory, 51(8), pp. 2791–2811, 2005.

[4] C. Carlet, Vectorial boolean functions for cryptography, Boolean models and methods in mathematics, computer science, and engineering, 134, pp. 398–469, 2010.

[5] K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff, Redefining the transparency order, in *WCC2015-9th International Workshop on Coding and Cryptography 2015*, 2015.

[6] H. Dobbertin, Almost perfect nonlinear power functions on gf (2 n): the welch case, IEEE Transactions on Information Theory, 45(4), pp. 1271–1275, 1999.

[7] M. A. Evci and S. Kavut, Dpa resilience of rotation-symmetric s-boxes, in *International Workshop on Security*, pp. 146–157, Springer, 2014.

[8] H. M. Heys, A tutorial on linear and differential cryptanalysis, Cryptologia, 26(3), pp. 189–221, 2002.

[9] S. Kavut, Results on rotation-symmetric s-boxes, Information Sciences, 201, pp. 93–113, 2012.

[10] S. Kavut, Dpa resistivity of small size s-boxes, in *ISDFS 2015*, pp. 64–69, Proceedings of the 3rd International Symposium on Digital Forensics and Security, 2015.

[11] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, Springer New York, 1994, ISBN 9780387942933.

[12] P. Kocher, J. Jaffe, and B. Jun, Differential power analysis, in *Annual International Cryptology Conference*, pp. 388–397, Springer, 1999.

[13] P. C. Kocher, Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems, in *Annual International Cryptology Conference*, pp. 104–113, Springer, 1996.

[14] X. Lai, Higher order derivatives and differential cryptanalysis, in *Communications and Cryptography*, pp. 227–233, Springer, 1994.

[15] M. Matsui, Linear cryptanalysis method for des cipher, in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 386–397, Springer, 1993.

[16] B. Mazumdar and D. Mukhopadhyay, Construction of rssbs with high nonlinearity and improved dpa resistivity from balanced rsbfs, IEEE Transactions on Computers, PP(99), pp. 1–1, 2016.

[17] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, Constrained search for a class of good bijective s-boxes with improved dpa resistivity, IEEE Transactions on Information Forensics and Security, 8(12), pp. 2154–2163, 2013.

[18] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, Design and implementation of rotation symmetric s-boxes with high nonlinearity and high dpa resilience, in *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, pp. 87–92, IEEE, 2013.

[19] K. Nyberg, Differentially uniform mappings for cryptography, in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 55–64, Springer, 1993.

[20] S. Picek, B. Ege, L. Batina, D. Jakobovic, Ł. Chmielewski, and M. Golub, On using genetic algorithms for intrinsic side-channel resistance: the case of aes s-box, in *Proceedings of the First Workshop on Cryptography and Security in Computing Systems*, pp. 13–18, ACM, 2014.

[21] S. Picek, B. Ege, K. Papagiannopoulos, L. Batina, and D. Jakobovic, Optimality and beyond: The case of 4x4 s-boxes, in *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, pp. 80–83, IEEE, 2014.

[22] B. Preneel, *Analysis and design of cryptographic hash functions*, Ph.D. thesis, Citeseer, 1993.

[23] E. Prouff, Dpa attacks and s-boxes, in *International Workshop on Fast Software Encryption*, pp. 424–441, Springer, 2005.

[24] J.-J. Quisquater and D. Samyde, Electromagnetic analysis (ema): Measures and counter-measures for smart cards, in *Smart Card Programming and Security*, pp. 200–210, Springer, 2001.

[25] J. Seberry, X.-M. Zhang, and Y. Zheng, Nonlinearity and propagation characteristics of balanced boolean functions, 1994.

[26] C. Shannon, Communication theory of secrecy systems.

[27] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.), IEEE Transactions on Information theory, 30(5), pp. 776–780, 1984.

[28] P. Stănică and S. Maitra, Rotation symmetric boolean functions—count and cryptographic properties, Discrete Applied Mathematics, 156(10), pp. 1567–1580, 2008.

[29] D. R. Stinson, *Cryptography: theory and practice*, CRC press, 2005.

[30] X.-M. Zhang and Y. Zheng, Gac—the criterion for global avalanche characteristics of cryptographic functions, in *J. UCS The Journal of Universal Computer Science*, pp. 320–337, Springer, 1996.