S-Boxes construction over Galois fields of order 256

Dawood Shah

Supervised

By

Prof Dr. Tariq Shah

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTER OF PHILOSOPHY
AT
DEPARTMENT OF MATHEMATICS
QUAID-I-AZAM UNIVERSITY ISLAMAD, PAKISTAN
MARCH 2018

DEPARTMENT OF MATHEMATICS

Dated: March 2018

External Examiner: _____

Research Supervisor: _____
Prof Dr. Tariq Shah

Examing Committee: _____

_____

To my parents

Table of Contents

Preface

Although over the last 40 years, cryptography is weighed up as a developed branch of science nonetheless it is a new field of study compare to other subjects and every day brings so many expansion. Symmetric cryptography is one of the significant branch by which two parties share secret information and keys by encryption and decryption procedures. Symmetric cryptography splits into two main branches; Block cipher and Stream cipher. S-box is the important component of block cipher algorithm, used in many famous cipher system such as data encryption standard (DES), International data encryption algorithm (IDEA), advanced encryption standard (AES) [1,2]. S-box is one of the nonlinear components of the block cipher, hence the security strength of block cipher depends on the quality of an S-box. As a result of this many researchers have shown their interest to design new and powerful S-boxes. Owing to their strong cryptographic features, S-boxes that are created on algebraic systems have much attention and which are robust against linear and differential cryptanalysis. Thus a secure communication based on different types of S-boxes are always encouraged. Like AES S-box, the affine power affine (APA) S-box is proposed which upsurges the algebraic complexityalgebraic complexity though possession the anticipat available encryption properties [3]. The action of the symmetric group S_8 on the original S-box used in AES, the $S8$ AES S-box is offered in [4]. On applying additional transform based on binary Gray codes on the original S-box of AES. The Gray S-box is

obtained [5]. The Gray S-box has a 255-term polynomial as compare to 8-term polynomial which carries all the properties and rises the security for AES. Similarly, Xyi S-box, Residue Prime S-box and Skipjack S-box are normally used S-boxes in the encryption and decryption techniques [6, 7]. Typically the algebraic strength of an S-box is measured by Nonlinearity Nonlinearity, strict avalanche criterion strict avalanche criterion (SAC), bit independence criterion bit independence criterion(BIC), linear approximation probability linear approximation probability (LP) and Differential approximation probability Differential approximation probability (DP) [8]. It is evident by the study of novelty in algorithms for S-box construction that the alteration of the model and the selection of Boolean functions give small to the performance indices of an S-box. In this research, we suggest that the performance of an S-box is momentously link with the contextual Galois field. The finite fields of the same order are isomorphic but the scaling effect of a nonlinear Boolean function apply on two or more different fields of the same order may diverge. An S-box is a significant component in a block cipher used to produce confusion in the data; it is valued take in that the confusion making ability is allied with the optimal of the irreducible polynomial used to form the contextual Galois field. The main aim of this research is to understand the basic concept of cryptography, but mainly focused on the construction of S-boxes based on the group action of projective general linear group on the Galois field $GF(2^8)$. The algebraic analysis such as nonlinearity, strict avalanche criteria, linear approximation probability, bit independence criteria and differential approximation probability on the newly generated S-box is performed to determine the strength of the S-boxes.

Chapter 1

Cryptology and Algebra

1.1 Introduction

People always want to keep their sensitive information secret from others. There are a lot of examples we have seen in history, where peoples tried to keep their information secret. Nowadays world intelligence agencies and other secret agencies used to communicate with each other in basic cryptography method. It is because to keep their information secret. Headway in a society increased the more refine methods for protecting data. As the world becomes further connected, the demand for information and electronic services is growing and with accumulated demand comes accumulated dependency on electronic systems. Already the exchange of sensitive information like Master Card numbers over the open network is a common paractice. protecting info and electronic systems unit important to our manner of living. The world **Cryptography** has been derived from the Greek word **krypto** that means **hidden**. It is the science of hiding info so that unlawful users are unable to understand this information. It is the science of information security. The skills needed to protect data belong to the field of cryptography.

The work of cryptography is the converting of readable and understandable data

into unreadable data to protects the data. It is used for protecting private data from being stolen. Even it will receive your messages that they will able to understand. When cryptography protects data it implemented other security necessities for data together with authentication, repudiation, confidentiality, and integrity. Cryptography is, where security engineering come across Mathematics. It is an interdisciplinary study of basically three fields.

1. Mathematics
2. Computer Science
3. Electrical Engineering

The main purpose of cryptography is securing communication over a non-secure channel between two parties in such a way that their hosting cannot understand what is supposed to say the channel may be a telephone line or computer network. The field of cryptography direct link with the field of cryptanalysis.The key purpose of this introductory chapter, is about its definitions and basic concepts to afford background to the material that is presented in the upcoming chapters. We have divided this chapter into six sections. In these six sections we briefly described, what is cryptography, what are the needs of cryptography, what are the objectives of cryptography, what are the constituents of cryptography, types of cryptography and in the last section, we have discussed basic concepts including binary number, rings, fields, polynomial ring and finite fields etc.

1.1.1 Cryptology

Cryptology is the study of secure communication over non-secure channels and related problems [9].

1.1.2 Cryptography

The process of designing systems for secure communication over non-secure channels belongs to the field of Cryptography. It is the study of Mathematical technique that is linked to the aspects of information security.

1.1.3 Cryptanalysis

The discipline of examining and breaking cryptographic system is called Cryptanalysis [9].

1.2 Cryptography Components

The main components of cryptography are given in the following subsections [10].

1.2.1 Plain text

A type of data that can understand and readable without usual process.

1.2.2 Encryption

It is a process in which manifest data is converted into hidden data to secure data.

1.2.3 Secret key

It is an input to the encryption algorithm. For securing information a numerical value (secret key) is used by an algorithm modify information and make the information

secure. But only to those who have the corresponding key to recover the information.

1.2.4 Cipher text

A type of data that cannot understand and unreadable without any usual process.

1.2.5 Decryption

It is a process in which encrypted data is converted into original plaintext. .

1.3 Types of Cryptography

In [10] there are two main types of cryptography.

1.3.1 Asymmetric key Cryptography

The asymmetric key algorithm was adapted in the 1970s and modernized Cryptography. The Asymmetric key cryptography is also called public key cryptography. public key cryptography consist of two keys, one key is a public key which is used for encryption and another private key is used for the decryption.

The public key can be shared freely without any compromise with the security of a private key. A private key must be kept secret. If someone has a public key he can encrypt info but can not decrypt it, only that person who has the private key can decrypt the information.

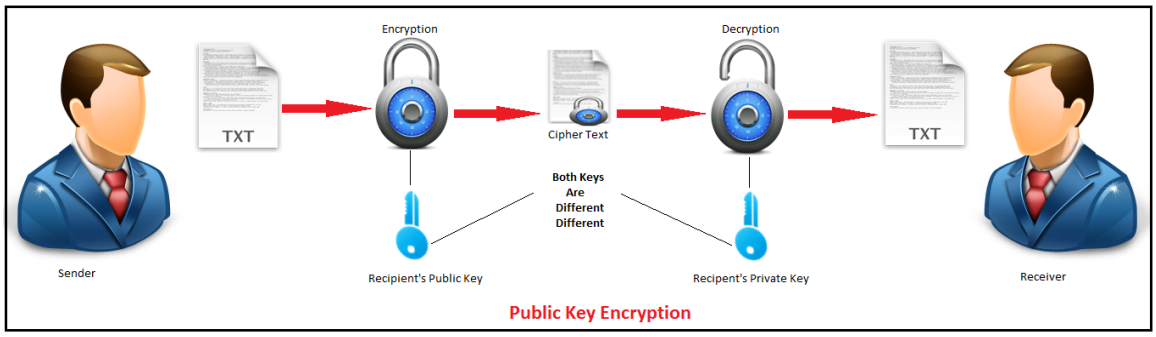


Figure 1.1: Public key

1.3.2 Symmetric key Cryptography

Symmetric key cryptography is also known as private key cryptography. Symmetric-key cryptography is that type of cryptography in which the encryption and decryption are same in many cases and also known to both sender and receiver. Such as like key are used for encryption and decryption.

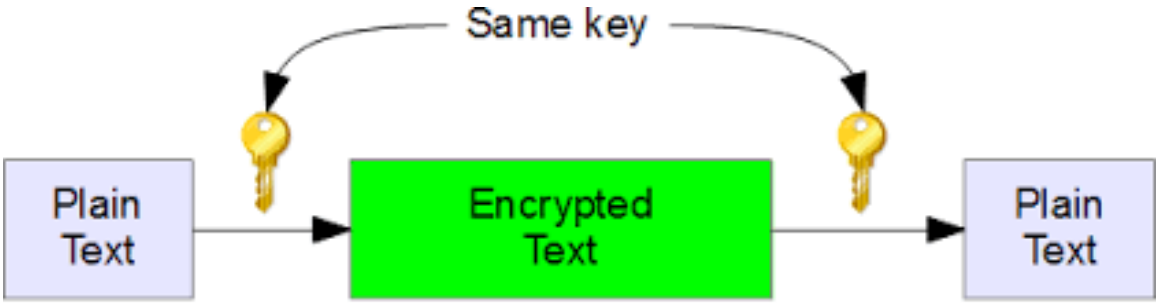


Figure 1.2: Private key

Example 1.3.1. *AES (Advance encryption standard), AES and DES (Data encryption standard), are the example of private key cryptography.*

1.4 Algebraic structures

Let G be a non empty set, let $G \times G$ denote the set of all order pairs (x, y) such that $x \in G$ and $y \in G$. Then the mapping from $G \times G$, into G is called binary operation

on G. In this definition its required that the image of $(x, y) \in G \times G$, must be in G, which is the closure property of an operation. By an algebraic structure, its mean a set together with one or more binary operation on G [5].

1.4.1 Group

Definition 1.4.1. *A group is a nonempty set G together with binary operation $*$ on G, such that for all $\alpha', \alpha'', \alpha''' \in G$ the following axioms hold.*

1. $\alpha' * (\alpha'' * \alpha''') = (\alpha' * \alpha'') * \alpha'''$.
2. *There exist* $e \in G$, *such that for all* $\alpha' \in G$, $\alpha' * e = \alpha' = e * \alpha'$.
3. *For all* $\alpha' \in G$, *there exist* $\alpha'^{-1} \in G$, *such that* $\alpha' * \alpha'^{-1} = e = \alpha'^{-1} * \alpha'$.

Thus a mathematical system $(G, *)$, satisfying axioms 1 to 3 is said to be a group.

Example 1.4.2. *The set of Real number, $(\mathbb{Z}, *)$, is a group where $*$ represent the usual operation of multiplication.*

Definition 1.4.3. *(Subgroup) Let G be a group, $H \subseteq G$ is a subset of G which is a group under the same binary operation. We call H is a subgroup of G and denoted by $H \leq G$.*

Example 1.4.4. *$(\mathbb{Z}, +)$, is a subgroup of $(\mathbb{R}, +)$, where $\mathbb{R}$, is the set of real numbers, $\mathbb{Z}$, is the set of integers and $+$, is the usual operation addition.*

Remark 1.4.5. *A nonempty subset $H \subseteq G$ is a subgroup if and only if a,b $\in H$, $\Rightarrow$ $ab^{-1} \in H$.*

1.4.2 Ring

Definition 1.4.6 (Ring)**.** *A ring $(R, *, +)$, is a non empty set R together with two binary operations multiplication $'*'$ and addition $'+'$, such that the following axioms hold [11].*

1. *R is an abelian group with respect to addition $'+'$.*
2. *R is semigroup with respect to multiplication $'*'$.*
3. *Distribute laws of multiplication over addition hold.That is*
   $\alpha' * (\alpha'' + \alpha''') = (\alpha' * \alpha'') + (\alpha' * \alpha'''), \forall\ \alpha', \alpha'', \alpha''' \in R.$
   $(\alpha' + \alpha'') * \alpha''' = (\alpha' * \alpha''') + (\alpha'' * \alpha'''), \forall\ \alpha', \alpha'', \alpha''' \in R.$

Definition 1.4.7 (Commutative ring)**.** *A Ring R, is said to be commutative ring, if*

$$\alpha' * \alpha'' = \alpha'' * \alpha', \forall \alpha', \alpha'' \in R.$$

Example 1.4.8. *The set of integers $(\mathbb{Z}, +, *)$, is a ring with respect to addition $'+'$ and usual multiplication $'*'$.*

1.4.3 Field

Definition 1.4.9. *A field is a nonempty set F, together with binary operations addition $'+'$ and $'*'$ usual operation multiplication, $(F, *, +)$, if the following axioms hold [11].*

1. *F is an abelian group with respect to addition '+'.*
2. *F is an abelian group with respect multiplication '*'.*
3. *Distribute laws of multiplication over addition hold. That is*
   $\alpha' * (\alpha'' + \alpha''') = (\alpha' * \alpha'') + (\alpha' * \alpha'''), \forall\ \alpha', \alpha'', \alpha''' \in F$
   $(\alpha' + \alpha'') * \alpha''' = (\alpha' * \alpha''') + (\alpha'' * \alpha'''), \forall\ \alpha', \alpha'', \alpha''' \in F.$

1.4.4 Polynomial ring

Let R be a commutative ring. Then the indeterminant x is an expression of the from $g(x) = a_m x^1 + ... + a_2 x^2 + a_1 x^1 + a_0 x^0$, is a polynomial $g(x)$ over the ring R. where each $a_i \in R$ and $n \geq 0$. The coefficient of x^i is an element a_i in $g(x)$. The degree of $g(x)$, for which $a_m \neq 0$ is the largest m, denoted by $degf(x)$, and the leading coefficient is a^m [11].

Remark 1.4.10. *If $f(x) = a_0$, and $a_0 \neq 0$, then $degf(x) = 0$. If all coefficients of the polynomial $f(x)$, are 0 then it is called 0 polynomial. And if the leading coefficient of a polynomial $f(x)$, is 1 then the polynomial is called monic polynomial.*

Definition 1.4.11. *Let R be a commutative ring. Then the set of all polynomials whose coefficients from the ring R is a polynomial ring denoted by $R[x]$. polynomial addition and multiplication are the two standard operations.*

Example 1.4.12. *Let $f(x) = x^4 + x$, and $g(x) = x^2 + x + 1$, be the element of $\mathbb{Z}_2[x]$. working in $\mathbb{Z}_2[x]$, $f(x) + g(x) = x^4 + 1$, and $f(x) * g(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x$.*

Definition 1.4.13. *Let F be arbitrary field . A polynomial $p(x) \in \mathbb{F}[x]$ of degree at least 1, is said to be an irreducible polynomial over $\mathbb{F}$ if $p(x)$, cannot be written as the product of two polynomials having a positive degree in $\mathbb{F}[x]$.*

Example 1.4.14. *$x^8 + x^4 + x^3 + x^2 + 1$, is reducible over $\mathbb{Z}_2[x]$.*

Definition 1.4.15. *Let $p(x)$, be a polynomial of degree less than n in $\mathbb{F}[x]$. Then the set $\frac{\mathbb{F}[x]}{<p(x)>}$, denote the equivalence classes of polynomial of degree less n. Addition and multiplication are performed modulo $p(x)$.*

Proposition 1.4.16. *Let $f(x)$, be any polynomial in $\mathbb{F}[x]$. Then $\frac{F[x]}{<f(x)>}$ is a commutative ring.*

Proposition 1.4.17. *If $p(x) \in \mathbb{F}[x]$ be an irreducible polynomial over $\mathbb{F}$. Then $\frac{\mathbb{F}[x]}{<p(x)>}$, is a field.*

1.4.5 Finite field of the from $GF(p^n)$

In this section, we have defined a finite field as a finite set, that obeys all of the axioms of fields and gave some example of a finite field [11]. Finite fields are the particular interest in the context of cryptography. In many cryptographic algorithms, finite field plays a circular role. For a positive integer n, the order of finite field must be a power of prime number p^n and generally can be written as $GF(p^n)$.

Definition 1.4.18. *A field having finite order is called finite field or Galois field and denoted by $GF(q)$, where q is prime or power of a prime number.*

Remark 1.4.19. *Existence and uniqueness of finite field.*

- *A Galois field contains q elements. where q is prime or power of a prime number.*
- *For any prime number p then power order p^n, there exist a unique Galois field of order p^n.*

Remark 1.4.20. *Let $\mathbb{F}_q$ be a finite field of order q, where $q = p^n$, p is any prime number, the $\mathbf{F}_q$, contain $\mathbb{Z}_p$, another word $\mathbb{Z}_p$ is a subfield of $\mathbb{F}_q$. And $\mathbb{F}_q$ is also called the extension field of $\mathbb{Z}_p$.*

1.4.6 Construction of Galois field:

General procedure to construct a finite field $GF(p^n)$, of order p^n, for prime number p and positive integer $n \geq 1$. Let $\mathbb{Z}_p$ be the set of integer mod p.

1. The set of polynomials $\mathbb{Z}_p[x]$, with coefficient mod p is a commutative ring.

2. Chose an irreducible polynomial $p(x) \in \mathbb{Z}_p[x]$ of degree n mod p.

   Then $< p(x) >$ are the maximal ideal contain in $\mathbb{Z}_p[x]$.

3. Then $GF(p^n) = \frac{\mathbb{Z}_p[x]}{<p(x)>}$ are the finite Galois field.

1.4.7 Linear group

In this section, we have discussed general linear groups, Special linear group and projective general linear groups over a field $\mathbb{F}$ [12]. Let $\mathbb{F}$ be a field and n be positive integer then the set of all $n \times n$, matrices with entries from $\mathbb{F}$ is denoted by $M_n(\mathbb{F})$.

Definition 1.4.21 (General Linear Group)**.** *[12] The set of all $n \times n$ matrices with entries from a field $\mathbb{F}$ is called general linear group, denoted by $GL(n, \mathbb{F})$, and define by*

$$GL(n, \mathbb{F}) = \{A \in M_n(\mathbb{F}) : det(A) \neq 0\}.$$

Remark 1.4.22. *The set $GL(n, \mathbb{F})$ from a group under metrics multiplication.*

Definition 1.4.23 (Special linear group)**.** *[12] Special linear over a field $\mathbb{F}$ is denoted by $SL(n, \mathbb{F})$, defined as*

$$SL(n, \mathbb{F}) = \{A \in GL(n, \mathbb{F}) : det(A) = 1\}.$$

Remark 1.4.24. *Special linear group $SL(n, \mathbb{F})$ is a normal subgroup of special linear group $GL(n, \mathbb{F})$.*

Definition 1.4.25 (Center for general linear group)**.** *The center of general linear group $GL(n, \mathbb{F})$ is the set*

$$Z = \{\lambda I_n : \lambda \in \mathbb{F}^*\}.$$

Definition 1.4.26. *Let $\mathbb{F}$ be a field and Z be the center of general linear group $GF(n,\mathbb{F})$. Then projective general linear group over a field $\mathbb{F}$ is denoted by $PGL(n,\mathbb{F})$, and defined as*

$$PGL(n,\mathbb{F}) = \frac{GL(n,\mathbb{F})}{Z}.$$

1.4.8 Group action

Let G be a group and Ω be a nonempty set. By an action of G on Ω we mean a function $\mu' : \Omega \times G \to \Omega$ such that for all $\omega' \in \Omega$ and $g', h' \in G$.

$$\mu'(\mu'(\omega', g'), h') = \mu'(\omega', g'h').$$

$$\mu'(\omega', 1) = \omega', \ \textit{where } 1 \ \in G \textit{ is the identity of } G.$$

Then we can say G act on set Ω.

Example 1.4.27. *Let x be a nonempty set and $G \leq sym(x)$. Then G act on a set x defined as $\mu(\omega, g) = (\omega)g$ for $g \in G$ and $\omega \in x$. here we defined $\mu(\omega, g) = \omega^g$.*

$$(\omega^g)^h = ((\omega)g)^h = ((\omega)g)h = (\omega)gh = (\omega)^{gh}.$$

$$\omega^1 = \omega 1 = \omega.$$

This action is called natural action.

1.5 Boolean algebra

Let B be a nonempty set, then the set $(B, \vee, \wedge, \sim)$, where $\vee$, $\wedge$ are the binary operations, and $\sim$ is a unary operation, is said to be a Boolean algebra, if for all $a', b', c' \in B$ satisfy the following axioms.

(B_1) $a' \vee b' = a' \vee b'$, *and* $a' \wedge b' = a' \wedge b'$.

(B_2) $a' \vee (b' \wedge c') = (a' \vee b') \wedge (a' \vee c')$, *and* $a' \wedge (b' \vee c') = (a' \wedge b')$.

(B_3) There exist $0, 1 \in B$ with $0 \neq 1$ such that $0 \vee a' = a' = a' \vee 0$ and $1 \wedge a' = a' = a' \wedge 1$.

(B_4) $a' \wedge (\sim a') = 0$ and $a' \vee (\sim a') = 1$.

The binary operation $\vee$ and $\wedge$ are called OR and AND respectively and the unary operation $\sim$ is called negation.

1.5.1 Boolean function

Let $\mathbb{Z}_2^n$ be the n-dimensional vector space then Boolean function $B(x)$ is a mapping $B : \mathbb{Z}_2^n \to \mathbb{Z}_2$ where $x = (x_n, x_{n-1}, ...x_1, x_0)$, and $\mathbb{Z}_2^n$ represent a Galois field of order 2^n, the total number of distinct Boolean functions of n variable are 2^{2^n} [13].

1.5.2 Some logic operations

AND operation

Let $x = \{0, 1\}$, then the AND operation on a set x, for any two input values $u', v' \in B$, the output value AND operation of u', v' is denoted by $u' \wedge v'$, and will be equal to 0 whenever one of the input value is 0 or both input values are 0, if both input values are 1 then output value will be equal to 1. The truth table of AND operation are given below

u'	v'	$u' \wedge v'$
0	0	0
1	0	0
0	1	0
1	1	1

OR operation

Let $x = \{0, 1\}$, the OR operation on a set x, for any two input value $u', v' \in B$, then the output value of OR operation of u', v' is denoted by $u' \vee v'$, and will be equal to 1 if whenever one value of them is 1 or both values are 1, if both values are 0 then the output value will be equal to 0. The truth table of OR operation are given below

u'	v'	$u' \vee v'$
0	0	1
1	0	1
0	1	1
1	1	0

XOR operation

Let $x = \{0, 1\}$, then the XOR operation on a set x, for any two input value $u', v' \in B$, then the output XOR operation of u, v is denoted by $u \oplus v$, and will be equal to 1 whenever one the input value are 1, if both the input values are 0 or both input values is 1 then output value will be equal to 0. The truth table of XOR operation are given below

u'	v'	$u' \oplus v'$
0	0	0
1	0	1
0	1	1
1	1	0

Chapter 2

Block Ciphers and S-Boxes

2.1 Introduction

This chapter consist of three sections, in the first section we have discussed ciphers, properties of ciphers and types of ciphers. And the second section is to illustrate the principle of symmetric key algorithm *Advanced Encryption Standard (AES)*. And third is the literature review of some standard S-boxes.

2.2 Cipher

Definition 2.2.1. *Cipher or (Cryptographic system) consists of five-tuple* (P, C, K, E, D) *satisfying the following conditions.*

1. *Let* P *denote the finite set of all plaintexts.*

2. *Let C denote the finite set of all ciphertexts.*

3. *Let K denote the finite set of all possible keys is called keyspace.*

4. *For any $k \in K$ their exit rule of encryption $e_k \in K$ such that $e_k : P \to C$ and rule of decryption $d_k \in D$ such that $d_k : C \to P$ is a function and for every $y \in P$ and $d_k(e_k(y)) = y$*

2.2.1 Properties of good Ciphers

In [14] Claude Elwood Shanan identifies the two properties Confusion and for the secure Ciphers.

Definition 2.2.2 (Confusion)**.** *Confusion refers that in simple key and ciphertext does not relate. In particularly every bit of ciphertext depend on several bits of the key.*

Definition 2.2.3 (Diffusion)**.** *Diffusion refers that change the plaintext by the single character should change several characters of ciphertext. Similarly, change the ciphertext by the single character should change several characters in plain text. If we change a single bit of the plaintext it can change several bits of the ciphertext.*

Stream Cipher The encryption process in which encrypts a digital data stream one bit or one byte is stream cipher. Which means that change the plain text by one letter can change one letter in the ciphertext. In a modern cryptographic system, this process cannot be used. Because by using frequency analysis frequency analysis,

it is easy to find encryption key.

Block Cipher The encryption process in which encrypts a digital data stream blocks of bits or bytes at a time is called block cipher. By encrypting blocks of several numbers or latter simultaneously the frequency analysis is more difficult. In block cipher almost all the characters of the ciphertext block change if we change one the character in the plaintext Block.

2.3 Advanced Encryption Standard

In 2001 the National Institute of Standard and Technology (NIST) published Advanced encryption standard *AES* and replaced Data encryption standard *(DES)* by the Advanced Encryption Standard. As compared to other cryptographic Algorithm AES is more complex and cannot be explained easily, their operation is performed on 8-bit Bytes.

2.3.1 Structure of AES

AES advanced encryption standard is a reversible encryption algorithm, iterated symmetric block ciphers. To complete encryption and decryption in reverse order the same number of steps performed, some steps repeat multiple time, operate on a fixed number of bytes . AES is a secret encryption algorithm, the key is expanded into individual subkeys, for each operation round one subkey, this process is called key expansion

The operation used in AES can be broken down into the following 4 functions.

1. Add round key
2. Bytes Substitution
3. Shift Row
4. Mix Colum

An iteration of the above 4 steps is called round, the number of rounds of the algorithm depends on the key size, i.e 10 rounds algorithm for 10 bytes key, 12 rounds algorithm 24 bytes key and 14 rounds for 32 bytes key. The last consist of 3 step because add round key performed at the start of the algorithm as round 0. Similarly in the last round of decryption Mix column round do not perform.

Add Round Key: In the add round key given ciphertext is XORed with subkey generated in the keys expansion process. For each round there exist a subkey which can never use again in the next round, in the next round the add round key function expended are used.

Byte Substitution: In byte substitution, each value of the state is replaced with the corresponding S-box value during the encryption, in the reverse process each value of the state replaced with the corresponding inverse of the S-box.

Shift Row: In this step of round arranges the state of data in a matrix form and then performed a circular shift for each row. The shift is not bitwise it is byte-wise, in circular shift each byte move one space over and there are a different number of the shift in each row. The following example is the shift row process.

$$\begin{bmatrix} 1 & 5 & 9 & 13 \\ 2 & 5 & 10 & 14 \\ 3 & 7 & 11 & 15 \\ 4 & 8 & 12 & 16 \end{bmatrix} \; Shiftrow \; \begin{bmatrix} 1 & 5 & 9 & 13 \\ 6 & 10 & 14 & 2 \\ 11 & 15 & 3 & 7 \\ 16 & 4 & 8 & 12 \end{bmatrix}$$

Mix Column: The Mix column is perhaps hardest step of the round to understand and explain both, there are two parts of this step. The first part will explain which part of the state are multiple against which part of the matrix. Here the matrix is

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

In the second part explain how this multiplication performed over a Galois field. The multiplication is performed one column at a time (4 bytes), the multiplication is performed as matrix multiplication for example

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 2 & 1 & 1 \end{bmatrix} * \begin{bmatrix} b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ b_4 & b_8 & b_{12} & b_{16} \end{bmatrix}$$

The first byte of is calculated by multiplying the first row 4 value of the state column with the first row 4 value of the matrix. The result of each multiplication is then Xored to produced one byte i.e

$$c_1 = (b_1 * 2) \oplus (b_2 * 3) \oplus (b_3 * 1) \oplus (b_4 * 1)$$

$$c_2 = (b_5 * 2) \oplus (b_6 * 3) \oplus (b_7 * 1) \oplus (b_8 * 1)$$

2.4 S-box Theory

In this section, we have discussed the area of substitution box (S-box) and also discuss construction method and analysis of some standards-boxes.

2.4.1 S-box

As $m \times n$ substitution box (S-box) is a mapping from m input bits to n output bits $S : \mathbb{Z}^m \to \mathbb{Z}^n$ or in a simple way to combine the set of output Boolean functions in fixed order is an S-Box, the possibility of input and output bits are 2^m and 2^n. if we consider S to be $m \times n$ S-box then their representation is to be $2^m \times n$ matrix.

If $m \times n$ S-box with $m < n$ number of output bits less then input bits then entries of S-box must be repeated. The S-box is said to be surjective if all possible output bits are present in S-box.

If $m \times n$ S-box for $m = n$ i.e the number of output bits is equal to the number of input bits, each input entries mapped to a distinct S-box entry. Then S-box may either contain repeat entries or either distinct S-box entries and maybe the multiple inputs entries mapped to the same output entries, all possible output bits are not present in the S-box. An S-box is said to be injective if distinct input entries mapped to the distinct output entries, S-box is said to bijective S-box if S-box is both surjective and injective, bijective s-boxes are always reversible I,e there exist a reverse map output entries to input and only exist if $m = n$. In $m \times n$ S-box is said to be regular which contain all of it possible 2^{2^n} output, an equal number of times appearing in the S-box . Thus the possibility of each output bits appear in the S-box is 2^{m-n}, if $m \geq n$ then S-box are balanced S-box. An $(m \times n)$ is said to be bent if $n \geq 2m$ and n are even if it can be written as linear combination of components Boolean function is bent.

2.4.2 Cryptographic properties of S-box

In the next chapter, we have discussed cryptographic properties of S-box.

2.4.3 Literature survey on some standard S-boxes

Rijindael S-box

In 2001 Vincent Rijmen, Joan Daemen in [1] presented Rijindael S-box. The designing procedure of Rijindael S-box is the combination of two power function take multiplicative inverse of an element x modulo irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ belong to Galois field and then using affine transformation matrix'

$$g(x) = \begin{cases} x^{-1},\ if\ x \neq 0 \\ 0,\ if\ x = 0 \end{cases}$$

$$l(x) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

where x_i are coefficient of x and the S-box denoted by

$$S(x) = log$$

APA S-box

In (2006) Lingguo Cui and Yuanda Cao, [3] proposed a new method to construct 8×8 named Affine power Affine (APA) S-box, improved the AES s-box with APA structure and can be written as

$$S(x) = logol$$

where g is the inverse function and l is Affine transformation function and x is any element in the Galois field $GF(2^8)$

Gray S-box

In 2008. Tran et al [5] for the advanced encryption standard present a Gray S-box. The construction procedure of Gray S-box is add a binary Gray code transformation with original AES S-box to increase the complexity of and security against algebraic attacks. Cryptographic properties of AES S-box like Non-linearity, stick avalanche criterion, and differential uniformity also achieves Gray S-box.

SKIPJACK S-box

Skipjack was introduced by U.S National security (NSA). US government used Skipjack as the encryption algorithm. This algorithm was constructed to be used in fast phones. It is a fasital network with 32 rounds and used 80 bits key which was also known by Crypto variable to encrypt and decrypt 64 -bits blocks data. Every round of Skipjack is characterized by different operation and S-box is the most notable operation of each round, S-box is the notable operation of each round. In [6], Skipjack S-box construction is given. Further I.Hussain and T.Shah analyzed Skipjack S-box with different analysis i,e nonlinearity, SAC, BIC, LP,DP [15].

Chapter 3

Construction of S-boxes

3.1 Introduction

In this chapter, we have offered a novel technique to design 16 different robust 8×8 S-boxes over the elements these 16 Galois fields. Accordingly, on these different Galois fields we define 16 linear fractional transformations as: $z \longrightarrow \frac{az+b}{cz+d}$ where z is an arbitrary element in any of these Galois fields and from any permanent Galois field the parameters a, b, c, d are throughout fixed elements. Accordingly, for fixed parameters a, b, c, d, we obtained 16 distinct S-boxes. The algebraic analysis such as nonlinearity, strict avalanche criteria, linear approximation probability, bit independence criteria and differential approximation probability on the newly generated S-box is performed

to determine the strength of the S-box.

This chapter is organized as follows. Some basic concepts regarding Galois fields are given in section 2. In section 3, the algebraic algorithm for the design of new S-boxes is introduced. Section 4 contains the methods used to analyze the proposed S-boxes and the methods include Nonlinearity, SAC, BIC, LP, and DP. Section 5. Contain performance index. Section seven contain statical analysis of proposed S-boxes to know about the security strength S-boxes in image encryption applications..

3.2 Construction of Galois Filed of order 256

The set of all polynomials whose coefficients from the field $\mathbb{Z}_2$ is a polynomial ring denoted by $\mathbb{Z}_2[x]$. A polynomial $p(x)$ is said to be irreducible in $\mathbb{Z}_2[x]$. If $p(x)$ cannot be a factor into a product of lower-degree polynomials in $\mathbb{Z}_2[x]$. If $p(x)$ is an irreducible polynomial over $\mathbb{Z}_2$, then ideal generated by $p(x)$ is a maximal ideal of the ring $\mathbb{Z}_2[x]$ and it is denoted and can be written as:

$$< p(x) >= \{a(x) : a(x) = p(x).h(x) \ for \ some \ h(x) \in \mathbb{Z}_2[x]\}$$

Now if $p(x)$ is irreducible polynomial in $\mathbb{Z}_2[x]$, then the quotient ring $\frac{\mathbb{Z}_p[x]}{<p(x)>}$ is a finite field, known as Galois field $GF(2^m)$ having order 2^m where m is the degree of primitive irreducible polynomial $p(x)$. More explicitly the elements of $\frac{\mathbb{Z}_2[x]}{<p(x)>}$ are the polynomials over $\mathbb{Z}_2$, whose degrees are strictly less than the degree of $p(x)$. The addition and subtraction are those of polynomials over $\mathbb{Z}_2$. The product of two elements are the remainder of the Euclidean division of the product in $\mathbb{Z}_p[x]$. The multiplicative inverse of non-zero element may be computed with the extended

Euclidean algorithm. Essentially in this study, the order 2^8 Galois field $GF(2^8)$ are of specific interest. For the of Galois field $GF(2^8)$, we choose a degree-8 primitive irreducible polynomial that generates the maximal ideal of the principle ideal domain $\mathbb{Z}_2[x]$. Subsequent $GF(2^8) - 0$ is the multiplicative cyclic Galois group of the result field $GF(2^8)$ and hence each nonzero element of the field $GF(2^8)$ can be expressed as a power of the primitive element α. where α is the root of the irreducible polynomial, in study we consider the $\{p_i(x) \in \mathbb{Z}_2[x];\}$ $p_i(x)$ is irreducible and $1 \leq i \leq 16$ of 16 primitive irreducible polynomials of degree 8, to construct corresponding sixteen Galois Fields $\frac{\mathbb{Z}_p[x]}{<p_i(x)}, 1 \leq i \leq 16$. Where the case of primitive irreducible polynomial is already taken in [18]. in the next section, we use the Galois fields to develop the S-boxes.The rest of 8-degree primitive irreducible polynomials and their related Galois fields are given in Table 3.1.

Table 3.1: Primitive irreducible polynomials and their corresponding Galois fields

Primitive Polynomials $p_i(x)$	Galois Field $GF(2^8)$	Primitive Polynomials $p_i(x)$	Galois Field $GF(2^8)$
$p_1(x) = x^8 + x^4 + x^3 + x^2 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_1(x)>}$	$p_2(x) = x^8 + x^7 + x^3 + x^2 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_2(x)>}$
$p_3(x) = x^8 + x^5 + x^2 + 1$	$\frac{\mathbb{Z}_3[x]}{<p_3(x)>}$	$p_4(x) = x^8 + x^7 + x^5 + x^3 + 1$	$\frac{\mathbb{Z}_4[x]}{<p_4(x)>}$
$p_5(x) = x^8 + x^6 + x^4 + x^3 + x^2 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_5(x)>}$	$p_6(x) = x^8 + x^6 + ^5 + x^1 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_6(x)>}$
$p_7(x) = x^8 + ^6 + x^5 + ^2 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_7(x)>}$	$p_8(x) = x^8 + x^6 + x^5 + x^3 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_8(x)>}$
$p_9(x) = x^8 + x^7 + x^3 + x^2 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_9(x)>}$	$p_{10}(x) = x^7 + x^5 + x^3 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_{10}(x)>}$
$p_{11}(x) = x^8 + x^7 + x^2 + x + 1$	$\frac{\mathbb{Z}_2[x]}{<p_{11}(x)>}$	$p_{12}(x) = x^8 + x^7 + x^6 + x + 1$	$\frac{\mathbb{Z}_2[x]}{<p_{12}(x)>}$
$p_{13}(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$	$\frac{\mathbb{Z}_2[x]}{<p_{13}(x)>}$	$p_{14}(x) = x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$	$\frac{\mathbb{Z}_2[x]}{<p_{14}(x)>}$
$p_{15}(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_{15}(x)>}$	$p_{16}(x) = x^8 + x^6 + x^5 + x^4 + 1$	$\frac{\mathbb{Z}_2[x]}{<p_{16}(x)>}$

3.3 Algorithm for construction of S-boxes

The designing procedure of the new S-boxes is based on the algebraic action of projective general linear group in $PGL(2, \frac{\mathbb{Z}_2[x]}{<p_i(x)>})$ on a Galois field $\frac{\mathbb{Z}_2[x]}{<p_i(x)>}$by linear fractional transformation. Accordingly, the linear fractional transformation used in the construction of S-boxes, which is given as;

$$g_i : PGL(2, \frac{\mathbb{Z}_2[x]}{< p_i(x) >}) \times \frac{\mathbb{Z}_2[x]}{< p_i(x) >} \longrightarrow \frac{\mathbb{Z}_2[x]}{< p_i(x) >}$$

,

$$g_i(\alpha_i^{m_j}) = \begin{cases} \frac{\alpha_i^{m_1}(\alpha_i^{m_j})+\alpha_i^{m_2}}{\alpha_i^{m_3}(\alpha_i^{m_j})+\alpha_i^{m_4}}, & if \;\; \alpha_i^{m_3}(\alpha_i^{m_j}) + \alpha_i^{m_4} \neq 0 \\ \alpha_i^{m_k}, & if \quad \alpha_i^{m_3}(\alpha_i^{m_j}) + \alpha_i^{m_4} = 0 \end{cases} \tag{3.3.1}$$

where $\alpha_i^{m_1}, \alpha_i^{m_2}, \alpha_i^{m_3}, \alpha_i^{m_4} \in \frac{\mathbb{Z}_2[x]}{<p_i(x)>}$ for any fixed (i) [16]. From this action we can construct 16776960 the justification is given in [12]. For the construction of new S-boxes, the algorithm begins with the action of $PGL(2, \frac{\mathbb{Z}_2[x]}{<p_i(x)>})$ on $\frac{\mathbb{Z}_2[x]}{<p_i(x)>}$ for any fixed i. Further details of the last step of the algorithm are shown in Table 3.1. In Table 3.1, column 1 denotes the elements of $\frac{\mathbb{Z}_2[x]}{<p_i(x)>}$ ranging from 0 to 255. Column 2 represents the analytical details of the linear fractional transformation and the results from the evaluation of $g_i(z)$ are listed. The numbers in $g_i(z)$ are substituted with their binary value equivalent, represented as some power of α_i where α_i the primitive element is defined as the root of the primitive irreducible polynomial $p_i(x)$. The resulting values from $\frac{\mathbb{Z}_2[x]}{<p_i(x)>}$ are then converted to the eight-bit binary values to be used in S-box. The final column displays the elements of the proposed S-box. In this study we fixed parameters (a,b,c,d)=$(\alpha_i^8, \alpha_i^{75}, \alpha_i^3, \alpha_i^{223})$ as taken in [18]. Thus the S-box design algorithm will be as under:

$$g_i : PGL(2, \frac{\mathbb{Z}_2[x]}{< p_i(x) >}) \times \frac{\mathbb{Z}_2[x]}{< p_i(x) >} \longrightarrow \frac{\mathbb{Z}_2[x]}{< p_i(x) >}$$

$$g_i(\alpha_i^m) = \begin{cases} \frac{\alpha_i^8(\alpha_i^m)+\alpha_i^{75}}{\alpha_i^3(\alpha_i^m)+\alpha_i^{223}}, & if \ \ \alpha_i^m \neq \alpha_i^{145} \\ \alpha_i^5, & if \quad \alpha_i^m = \alpha_i^{145} \end{cases} \tag{3.3.2}$$

where $\alpha_i^8, \alpha_i^{75}, \alpha_i^3, \alpha_i^{223} \in \frac{\mathbb{Z}_2[x]}{<p_i(x)>}$ for any fixed i. The new S-boxes, created through the proposed algorithm are listed just below the Table 3.2. These are the 16×16 lookup tables. Construction of S-box based on linear fractional transformation by choosing irreducible polynomial $p_1(x) = x^8 + x^4 + x^3 + x^2 + 1$ with corresponding Galois field.

Table 3.2: S-box Construction algorithm against one the 15 Galois fields of order 256

$GF(2^8) = \frac{\mathbb{Z}_2[x]}{<p_1(x)>}$	$g_1(\alpha^m) = \frac{\alpha_1^8(\alpha^m)+\alpha_1^{75}}{\alpha_1^3(\alpha^m)+\alpha_1^{223}}$	Element of S-box 1
0 =0	$\frac{\alpha_1^8(0)+\alpha_1^{75}}{\alpha_1^3(0)+\alpha_1^{223}}=\frac{\alpha^{75}}{\alpha^{223}} = \alpha^{107}$	$\alpha_1^{107} = 104$
$1=\alpha_1^0$	$\frac{\alpha_1^8(\alpha_1^0)+\alpha_1^{75}}{\alpha_1^3(\alpha_1^0)+\alpha_1^{223}}=\frac{\alpha_1^{224}}{\alpha_1^0} = \alpha^{224}$	$\alpha_1^{224} = 18$
$2=\alpha_1^1$	$\frac{\alpha_1^8(\alpha_1^1)+\alpha_1^{75}}{\alpha_1^3(\alpha_1^1)+\alpha_1^{223}}=\frac{\alpha_1^{39}}{\alpha_1^{193}} = \alpha_1^{101}$	$\alpha_1^{101} = 34$
$3 = \alpha_1^{25}$	$\frac{\alpha_1^8(\alpha_1^{25})+\alpha_1^{75}}{\alpha_1^3(\alpha_1^{25})+\alpha_1^{223}}=\frac{\alpha^{53}}{\alpha^{100}}=\alpha_1^{208}$	$\alpha_1^{208} = 81$
$4 = \alpha_1^2$	$\frac{\alpha_1^8(\alpha_1^2)+\alpha_1^{75}}{\alpha_1^3(\alpha_1^2)+\alpha_1^{223}}=\frac{\alpha^{172}}{\alpha^{147}} = \alpha_1^{25}$	$\alpha_1^{25} = 3$
.	.	.
.	.	.
.	.	.
$251 = \alpha_1^{234}$	$\frac{\alpha^8(\alpha_1^{253})+\alpha^{75}}{\alpha^3(\alpha_1^{253})+\alpha^{223}} = \frac{\alpha_1^{162}}{\alpha_1^{192}} = \alpha_1^{225}$	$\alpha_1^{225} = 36$
$252 = \alpha_1^{168}$	$\frac{\alpha^8(\alpha_1^{168})+\alpha^{75}}{\alpha^3(\alpha_1^{168})+\alpha^{223}} = \frac{\alpha_1^{122}}{\alpha_1^{57}} = \alpha_1^{65}$	$\alpha_1^{65} = 190$
$253 = \alpha_1^{80}$	$\frac{\alpha^8(\alpha_1^{80})+\alpha^{75}}{\alpha^3(\alpha_1^{80})+\alpha^{223}} = \frac{\alpha_1^{174}}{\alpha_1^{211}} = \alpha_1^{218}$	$\alpha_1^{218} = 43$
$254 = \alpha_1^{88}$	$\frac{\alpha^8(\alpha_1^{88})+\alpha^{75}}{\alpha^3(\alpha_1^{88})+\alpha^{223}} = \frac{\alpha_1^{85}}{\alpha_1^{151}} = \alpha_1^{189}$	$\alpha_1^{189} = 87$
$255 = \alpha_1^{175}$	$\frac{\alpha^8(\alpha_1^{175})+\alpha^{75}}{\alpha^3(\alpha_1^{175})+\alpha^{223}} = \frac{\alpha_1^{236}}{\alpha_1^{209}} = \alpha^{27_1}$	$\alpha_1^{27} = 12$

3.4 The List of all S-boxes 1-15

Table 3.3: Proposed S-box 1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
104	18	34	81	03	125	74	167	149	40	54	120	111	165	171	49
27	243	70	16	242	124	250	240	147	132	99	07	253	58	203	148
10	22	162	94	222	205	50	130	42	129	123	139	181	208	174	46
196	83	112	109	209	229	225	90	178	160	200	226	118	38	180	69
15	169	09	213	182	24	197	146	188	202	224	71	93	100	249	06
233	238	168	108	47	215	80	89	227	207	13	217	161	184	211	210
127	107	221	60	79	220	231	121	61	185	44	234	198	186	183	212
48	144	55	02	68	194	154	51	117	110	20	85	155	64	152	157
115	214	79	204	01	206	172	29	101	82	195	151	78	08	255	136
30	11	28	35	201	106	66	156	246	105	173	96	159	84	141	65
230	95	163	216	133	41	164	113	119	53	177	59	32	97	142	31
239	228	92	88	67	103	145	39	98	37	134	254	252	131	170	251
232	73	00	14	75	77	138	72	248	179	158	199	241	19	26	56
62	192	175	45	63	219	187	122	17	247	126	114	218	143	05	150
223	191	245	128	140	21	25	237	193	04	116	57	23	33	52	150
153	137	86	236	135	235	91	166	102	244	176	36	190	43	87	12

Table 3.4: Proposed S-box 2

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
98	18	135	95	03	128	180	17	19	139	240	200	176	204	149	164
247	178	173	112	181	255	127	146	74	245	197	113	158	163	21	32
224	111	131	145	83	134	107	155	199	43	00	51	26	196	206	48
62	254	34	152	138	104	198	82	08	102	133	225	60	80	02	116
22	231	75	06	37	04	69	44	115	47	57	126	110	227	31	35
191	161	141	186	105	118	94	45	96	185	91	154	114	124	68	156
135	33	142	30	248	54	42	157	130	166	250	122	25	253	230	243
214	249	90	77	218	05	172	183	66	58	61	50	56	53	87	78
07	215	137	15	159	150	144	10	217	244	117	86	97	187	251	84
23	212	226	210	147	169	106	189	20	92	120	93	100	16	99	175
89	242	234	72	188	236	81	184	76	167	237	171	88	238	221	235
101	121	211	64	216	165	246	136	222	40	192	208	190	241	109	46
233	28	119	24	179	160	49	170	148	193	12	14	205	229	55	59
67	73	209	201	71	239	123	36	125	232	228	63	213	143	70	52
85	194	29	168	223	203	140	132	129	220	79	202	65	252	38	13
103	174	39	11	09	151	27	207	182	219	41	108	177	01	195	162

Table 3.5: Proposed S-box 3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
229	18	26	142	03	99	111	100	126	164	189	156	132	210	213	206
167	94	98	97	117	102	07	65	46	16	198	202	40	24	107	35
243	193	251	174	14	158	00	36	09	161	58	80	118	149	114	159
109	166	130	136	146	25	196	59	128	199	08	81	113	124	230	153
231	233	108	11	236	212	72	56	173	227	237	147	105	31	228	15
103	76	44	242	78	90	143	50	89	29	96	60	66	215	141	254
95	216	57	162	49	17	86	182	75	155	148	183	140	222	87	21
28	13	52	192	05	204	30	70	163	232	240	53	48	208	69	160
02	255	82	181	67	177	01	101	123	138	12	32	74	38	178	22
85	246	92	37	207	234	154	135	214	223	04	125	201	209	83	250
220	39	226	137	133	151	238	68	217	55	187	20	43	139	169	45
244	221	224	219	152	176	64	175	194	06	121	34	200	180	122	172
157	239	171	106	225	119	179	110	42	170	253	184	290	247	168	191
54	144	79	165	23	71	37	19	185	88	104	129	145	93	77	131
115	252	127	249	62	235	197	33	211	10	120	218	186	27	41	241
112	63	205	188	245	116	84	248	61	91	195	203	150	134	51	47

Table 3.6: Proposed S-box 4

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
166	18	240	186	03	67	123	53	124	178	99	214	26	138	45	29
41	188	85	25	13	243	101	114	249	24	226	219	245	75	153	72
06	115	39	79	43	198	157	70	133	221	21	208	01	97	151	194
100	71	148	126	116	227	103	55	122	113	19	73	255	59	27	200
204	44	159	246	191	222	05	20	23	189	209	95	82	87	69	143
207	16	177	14	118	74	187	254	212	61	89	196	171	50	66	251
248	136	215	28	150	228	04	129	231	253	195	168	244	140	230	203
241	90	250	252	88	63	142	161	235	35	80	83	51	78	00	236
211	190	33	220	197	81	149	174	247	155	32	08	141	135	152	170
242	210	180	15	234	184	34	144	65	128	199	07	31	10	09	127
46	147	47	163	120	84	201	232	109	205	40	225	119	93	42	169
110	86	38	182	30	22	02	237	213	154	52	54	62	132	58	176
49	134	37	217	238	17	216	239	96	57	121	223	204	206	229	68
91	218	179	165	106	12	202	145	98	107	233	183	139	175	193	137
160	112	192	56	117	173	131	181	156	108	167	11	48	94	172	146
162	130	111	162	92	185	76	158	125	60	36	102	105	104	64	77

Table 3.7: Proposed S-box 5

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
122	18	213	150	03	154	171	180	227	36	43	69	28	134	164	32
217	246	19	209	146	206	214	189	181	85	255	51	128	102	88	22
236	167	241	25	229	176	141	77	73	182	37	38	23	244	194	192
83	237	45	175	198	190	108	243	220	110	121	89	76	239	149	61
132	53	145	203	57	162	100	158	124	27	70	90	169	58	92	101
187	82	68	06	74	59	151	219	55	96	35	112	142	202	130	147
00	106	160	10	47	165	177	62	228	64	163	52	56	31	78	139
12	157	103	156	39	135	42	71	240	238	98	94	16	166	46	104
168	33	97	07	235	81	242	216	230	254	247	223	13	212	140	17
233	05	50	188	199	152	153	186	185	197	26	93	215	205	129	87
161	178	60	207	159	172	109	80	250	41	144	04	222	86	72	191
183	156	11	211	48	224	34	24	01	208	66	107	118	65	63	195
105	111	99	232	199	15	75	95	125	179	137	127	120	02	123	251
113	201	49	234	193	174	252	345	08	210	115	204	114	138	21	133
131	226	54	20	44	30	170	91	84	248	136	173	116	200	40	253
70	09	14	218	196	67	184	225	117	231	155	29	249	221	148	143

Table 3.8: Proposed S-box 6

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
88	18	186	250	03	63	188	27	106	103	66	138	246	23	56	223
68	211	31	232	36	234	76	213	28	21	65	203	46	179	227	247
82	39	73	97	93	44	119	218	91	167	240	22	215	176	209	168
58	177	200	219	238	160	89	100	00	249	17	144	16	253	199	146
113	15	11	125	53	189	77	124	96	40	47	114	101	120	207	152
158	155	109	185	255	33	251	41	111	14	148	24	139	187	122	149
04	20	169	237	241	173	102	74	174	161	172	72	235	166	178	06
105	49	62	52	233	245	170	217	194	129	01	126	90	151	198	153
212	110	29	10	104	222	206	30	210	130	38	55	175	230	163	80
116	86	85	118	75	34	228	07	59	224	121	117	196	242	184	236
243	136	162	205	140	231	45	37	08	150	69	156	64	180	204	60
84	95	87	226	42	132	143	09	131	135	191	13	137	94	154	57
164	32	171	83	252	190	19	192	26	127	157	133	108	115	71	134
165	221	239	201	248	254	197	02	220	70	67	214	159	61	12	195
208	99	78	229	05	145	81	43	225	98	216	142	141	147	112	35
183	128	51	79	48	181	50	54	107	25	182	193	202	123	244	92

Table 3.9: Proposed S-box 7

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
192	18	119	214	03	161	165	222	04	88	74	91	216	08	80	240
132	07	101	236	198	211	110	184	107	109	254	205	178	249	162	92
120	139	175	227	106	247	77	167	103	163	86	141	104	67	248	170
246	62	00	111	181	224	27	60	29	134	35	239	133	228	06	85
202	253	230	44	196	68	229	140	54	204	189	96	193	25	82	127
152	255	59	52	185	145	215	99	128	144	183	244	78	89	169	143
39	79	117	187	105	218	223	243	194	63	83	93	188	40	200	164
47	21	182	186	69	61	126	72	02	43	94	179	157	31	159	57
180	66	34	168	203	41	241	58	251	199	135	207	208	245	250	53
124	38	10	50	225	95	129	05	42	17	56	195	172	149	24	115
206	98	49	14	12	81	151	166	75	233	26	148	130	191	197	48
137	173	70	237	37	201	220	28	232	16	190	234	1118	153	136	252
217	97	36	32	131	114	87	33	154	123	102	142	147	55	15	160
30	112	65	76	46	171	108	176	177	100	156	121	138	210	150	212
231	155	20	209	242	221	116	235	19	113	13	238	45	64	09	71
11	226	122	90	22	23	146	01	213	73	174	125	158	51	219	84

Table 3.10: Proposed S-box 8

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
142	18	55	73	03	56	48	154	168	229	219	115	158	175	24	11
245	201	215	242	221	38	109	70	184	90	234	217	117	15	216	189
00	41	120	235	87	132	126	101	06	94	183	220	29	121	188	226
203	195	202	118	149	91	104	07	45	36	52	233	252	193	176	05
105	71	163	82	12	160	27	23	53	225	51	42	140	107	218	64
33	249	159	97	34	185	72	232	231	139	170	147	204	39	13	16
119	17	08	31	40	65	68	162	174	171	254	186	155	164	100	192
223	141	113	129	75	108	125	122	62	161	130	128	236	116	43	25
182	09	77	250	138	248	44	178	181	124	10	26	19	106	200	78
99	224	228	112	137	69	165	237	212	145	251	206	54	136	04	47
239	209	177	60	93	30	89	247	190	207	59	246	114	156	21	211
144	98	76	180	46	143	152	135	210	49	58	191	244	238	88	173
35	194	28	187	205	172	131	208	146	157	199	127	57	198	150	123
85	227	01	32	222	151	74	103	134	240	61	253	197	166	111	110
83	79	243	80	66	96	92	148	14	22	169	133	86	20	153	67
255	213	84	95	214	37	167	241	230	179	102	196	02	50	63	81

Table 3.11: Proposed S-box 9

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
166	18	240	186	03	67	123	53	124	178	99	214	26	138	45	29
41	188	85	25	13	243	101	114	249	24	226	219	245	75	153	72
06	115	39	79	43	198	157	70	133	221	21	208	01	97	151	194
100	71	148	126	116	227	103	55	122	113	19	73	255	59	27	200
204	44	159	246	191	222	05	20	23	18	209	95	82	87	69	143
207	16	177	14	118	74	187	254	212	61	89	196	171	50	66	251
248	136	215	28	150	228	04	129	231	253	195	168	244	140	230	203
241	90	250	252	88	63	142	161	235	35	80	83	51	78	00	236
211	190	33	220	197	81	149	174	247	155	32	08	141	135	152	‘70
242	210	180	15	234	184	34	144	65	128	199	07	31	10	09	127
46	147	47	163	120	84	201	232	109	205	40	225	119	93	42	169
110	86	38	182	30	22	02	237	213	154	52	54	62	132	58	176
49	134	37	217	238	17	216	239	96	57	121	223	224	206	229	68
91	218	179	165	106	12	202	145	98	107	233	183	139	175	193	137
160	112	192	56	117	173	131	181	156	108	167	11	48	94	172	146
164	130	111	162	92	185	76	158	125	60	36	102	105	104	64	77

Table 3.12: Proposed S-box 10

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
84	18	73	117	03	103	199	149	54	197	191	218	221	07	21	51
200	208	106	223	167	19	122	239	186	183	161	147	92	203	198	67
55	170	82	100	104	123	182	91	156	165	227	88	137	168	39	29
49	228	231	179	226	252	237	232	52	193	30	224	95	74	225	43
77	80	94	209	41	205	68	105	24	26	254	86	136	119	37	98
36	126	13	112	70	31	116	42	99	87	125	107	185	110	154	250
240	207	102	59	189	229	34	06	23	220	14	178	206	08	28	138
174	194	48	225	20	109	78	204	166	173	40	175	247	44	251	38
157	143	214	22	244	02	151	69	148	234	202	15	76	241	253	01
130	61	144	81	25	201	53	46	160	127	90	150	235	11	32	212
58	155	128	213	60	04	133	96	135	79	16	140	192	243	17	62
180	211	245	45	153	142	113	10	139	05	56	163	196	141	242	145
85	190	162	216	215	195	124	120	236	131	184	249	159	50	158	66
177	219	115	111	83	210	33	89	188	93	47	132	97	75	187	35
222	246	238	64	27	217	164	230	121	57	114	71	118	181	108	63
169	248	134	152	176	09	72	00	65	12	171	101	129	233	172	146

Table 3.13: Proposed S-box 11

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
181	18	201	254	03	227	211	11	195	49	177	28	111	45	41	13
188	82	199	165	60	171	72	158	185	57	40	247	42	63	47	38
173	65	196	142	112	170	104	44	169	134	90	124	236	237	240	43
167	239	10	245	242	130	218	159	115	69	67	08	161	64	151	194
37	172	49	244	01	80	94	232	73	154	23	81	97	27	113	226
145	114	35	77	200	88	255	95	126	86	54	136	166	26	246	214
253	32	87	07	210	178	241	157	233	59	212	228	225	128	107	83
203	61	76	164	193	100	96	106	217	33	50	21	53	59	110	102
224	252	251	78	248	17	30	118	137	215	58	116	146	179	123	66
138	132	174	208	31	00	163	152	99	148	91	235	119	02	150	135
141	183	89	109	55	180	36	190	108	231	175	182	98	105	204	191
143	229	249	144	120	74	93	70	34	117	79	16	46	234	12	153
133	84	197	92	14	25	162	24	15	250	198	243	206	127	09	05
68	122	51	192	186	39	139	56	04	06	140	156	62	202	85	71
184	160	147	121	129	103	20	222	207	219	238	221	205	230	223	125
131	52	19	187	189	48	101	155	216	22	168	75	176	213	220	29

Table 3.14: Proposed S-box 12

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
241	18	231	146	03	164	248	232	48	78	68	124	127	115	46	125
116	136	179	01	101	204	15	244	109	14	86	236	251	206	209	66
119	253	221	153	181	224	44	95	196	159	41	20	154	139	38	149
13	217	47	200	88	12	29	107	193	94	76	96	57	155	167	79
252	05	161	214	85	31	208	182	11	199	246	151	30	170	176	26
58	180	99	114	237	56	147	87	100	45	173	226	81	69	177	212
245	103	233	211	207	213	240	168	192	34	93	148	92	52	90	135
16	255	158	49	27	111	222	142	171	210	163	24	98	104	133	113
50	67	219	118	54	70	190	197	33	61	91	63	230	126	227	138
152	89	123	07	223	17	28	62	184	132	144	239	110	121	84	56
77	06	157	106	183	105	198	35	250	243	32	128	249	194	205	02
23	37	10	247	25	178	80	165	175	160	131	134	04	254	09	08
53	150	166	112	229	187	117	201	59	186	189	185	75	36	65	43
82	215	238	162	202	228	141	64	42	195	72	174	21	129	203	119
172	225	40	242	102	71	00	234	143	145	218	220	216	60	130	39
51	83	188	235	169	55	97	120	191	137	140	22	73	122	108	74

Table 3.15: Proposed S-box 13

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
212	18	60	99	03	202	95	120	253	131	50	169	249	88	123	101
172	170	14	10	70	69	113	208	81	48	162	72	106	153	142	53
160	230	86	33	204	241	17	164	96	198	143	156	35	79	197	59
130	49	152	58	223	175	13	216	42	103	06	244	23	213	08	144
191	189	185	110	181	157	161	173	179	87	43	16	176	252	177	54
183	209	07	235	68	214	98	114	250	105	20	224	182	225	196	47
45	206	37	92	62	134	119	64	236	195	154	155	180	219	135	36
126	85	248	193	71	26	159	148	22	40	108	52	97	34	218	239
231	83	78	166	122	19	151	61	55	246	255	117	76	90	111	129
141	217	242	167	254	28	200	75	168	88	82	237	44	139	127	178
233	89	112	107	128	67	184	211	80	104	01	124	93	146	247	12
24	150	48	39	228	165	133	229	31	234	102	29	09	125	220	115
192	232	32	251	238	138	121	190	02	11	222	194	118	243	21	149
210	51	221	140	147	66	158	30	05	136	187	201	145	109	174	00
215	186	116	240	63	171	205	137	27	65	25	132	74	100	73	38
91	46	245	57	41	15	163	203	77	207	56	226	199	94	04	227

Table 3.16: Proposed S-box 14

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
133	18	181	107	3	53	216	144	118	47	244	222	71	163	138	23
241	239	49	96	245	58	223	252	130	242	160	173	199	108	89	05
200	63	249	213	195	153	193	40	80	148	2	75	30	197	29	13
198	212	77	172	104	217	151	136	33	119	243	238	208	227	69	159
45	182	117	176	190	225	232	186	254	214	94	174	12	134	158	146
231	141	115	164	54	166	106	97	86	36	27	161	41	8	83	162
229	55	22	168	73	10	44	253	180	19	99	78	87	210	25	235
52	204	211	46	64	226	90	170	120	39	218	171	192	109	67	88
95	16	76	24	178	246	143	124	152	248	66	59	26	209	230	179
167	126	220	237	20	127	183	82	0	98	112	116	57	157	7	1
219	60	233	81	11	145	155	111	215	103	34	142	129	14	206	37
84	85	137	189	70	205	187	114	17	56	101	175	251	154	15	147
74	188	156	21	221	61	51	79	165	131	236	150	185	194	62	9
224	149	132	177	247	31	35	4	32	68	196	43	121	92	110	240
250	50	123	28	122	125	225	207	202	169	91	72	42	184	65	128
38	113	234	135	93	100	140	228	203	6	48	201	139	102	191	105

Table 3.17: Proposed S-box 15

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

Table 3.18: Proposed S-box 16

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

3.5 Algebraic analysis

In this section, we have presented some valuable analysis of S-box followed by [16].

3.5.1 Nonlinearity

The distance among the Boolean function f and the set of all affine linear functions is said to be nonlinearity of f. Basically the nonlinearity of a Boolean function f characterizes the number of bits which transformed in the truth table of f to reach the neighboring affine function.The upper bound of nonlinearity is $N = 2^{n-1} - 2^{\frac{n}{2}-1}$ [19] so that for $n = 8$ the extreme value of nonlinearity is 120. It can be seen from the Performance Indexes of S-boxes that average nonlinearity of all proposed S-boxes is almost 112, hence an optimal value is achieved. In figure 3.1, we have the nonlinearity analysis of proposed S-boxes with some standard S-boxes, which we have already discussed in section 2.4.2, literature review of S-boxes, to know about the security strength of proposed S-boxes as compare to other S-boxes. It can be seen in the performance indexes of proposed S-boxes 1-16 that the nonlinearity of each proposed S-box measure is 112. In figure 3.1 when we compare the values of nonlinearity of proposed S-boxes with some of the standard S-boxes, we absorbed that the result of proposed S-boxes are same as the result of analysis of the top S-boxes, i,e Gray, APA and AES S-box, and batter then other S-boxes such as Skipjack , Xyi and Residue prime S-box.

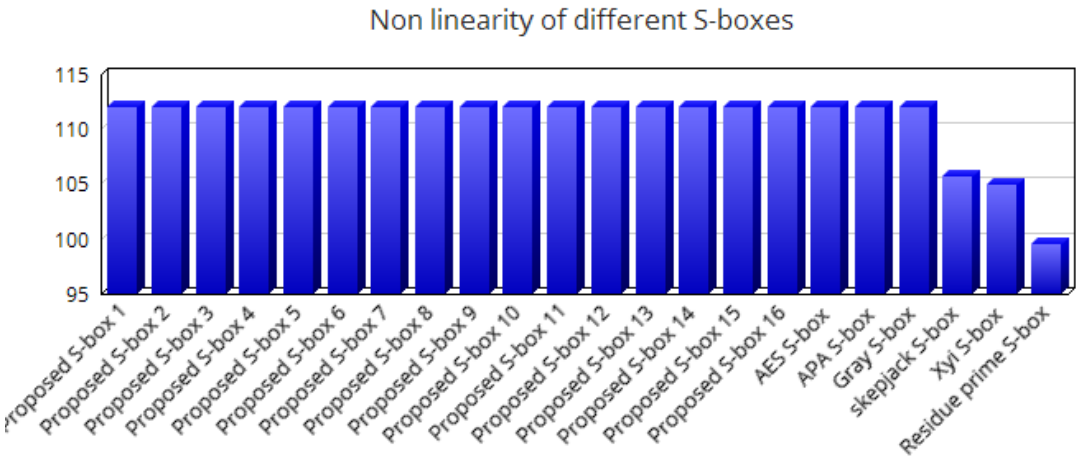


Figure 3.1: Comparison of nonlinearity analysis of different S-boxes

3.5.2 Strict avalanche criteria

The SAC was first introduced in 1895 by Webster and Tavares [20]. The SAC constructs on the notions of completeness and avalanche. It is satisfied if, whenever a single bit of input changed, each of the output bits changes with a 0.5 probability that is, when one bit of input is changed, half of its corresponding output bits will changes. We can observe from the performance Indexes of S-boxes that the proposed S-box successfully satisfied SAC. The result of the strict avalanche criterion (SAC) analysis of all proposed S-box are different and closed to 0.5, and in figure 3.2 the comparison of SAC analysis of all proposed S-boxes with standard S-boxes are presented, it can be seen that the SAC analysis result of all 16 proposed S-boxes is approximately equal to 0.5 which is comparatively best.

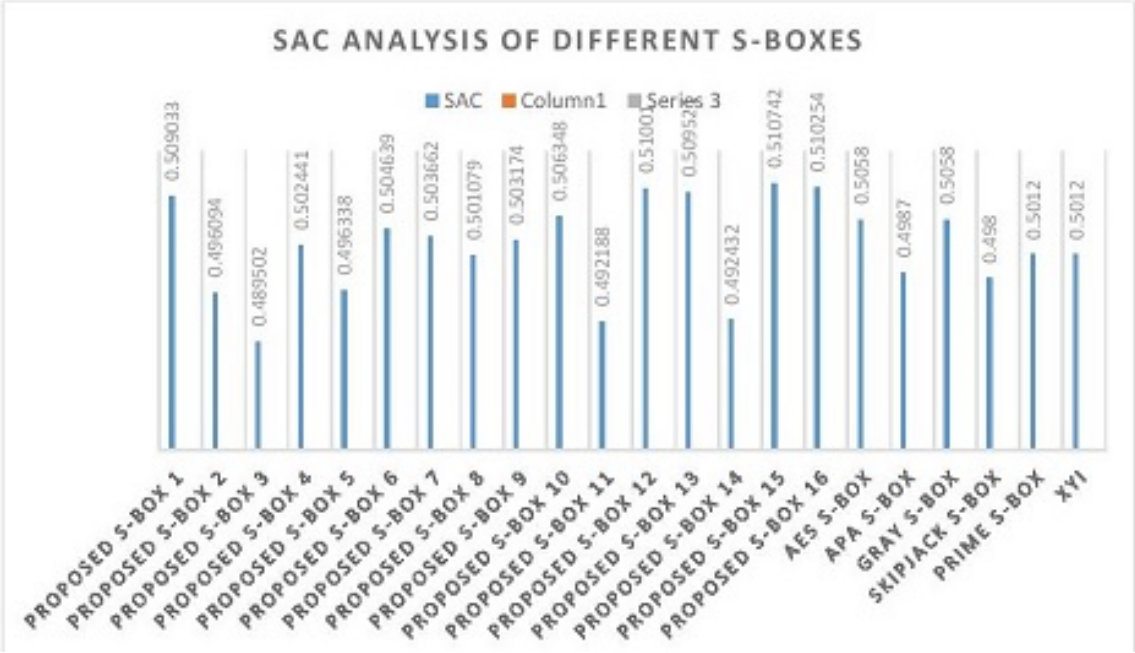


Figure 3.2: Comparison of SAC analysis of different S-boxes

3.5.3 Bit independent criterion

The BIC was also first introduced by Webster and Tavares [20] which is another required property for any cryptographic methods. Table 2, shows the results of BIC analysis of proposed S-box and in the sense of encryption strength, the BIC of the proposed S-box is acceptable. Performance Indexes of S-boxes show that the rank of our proposed S-box is comparable with S-boxes from literature and we observed that the proposed S-boxes satisfied BIC close to the best possible value. In Bit independence criterion variables are pairwise compared to analyze independence between these variables. Performance indexes of all proposed S-box show that the result of the

nonlinearity of bit independent criterion analysis is equal. Moreover, BIC analysis of all S-boxes has minimum value 112 and average value 112 respectively. In the figure showing the comparison of the result of the BIC analysis of all Proposed S-boxes with Standard S-boxes, it can be seen that BIC analysis result of proposed S-boxes is same as the result of BIC analysis of AES, APA and Gray S-box and much batter then Xyi, Skipjack, and Residue prime S-box.

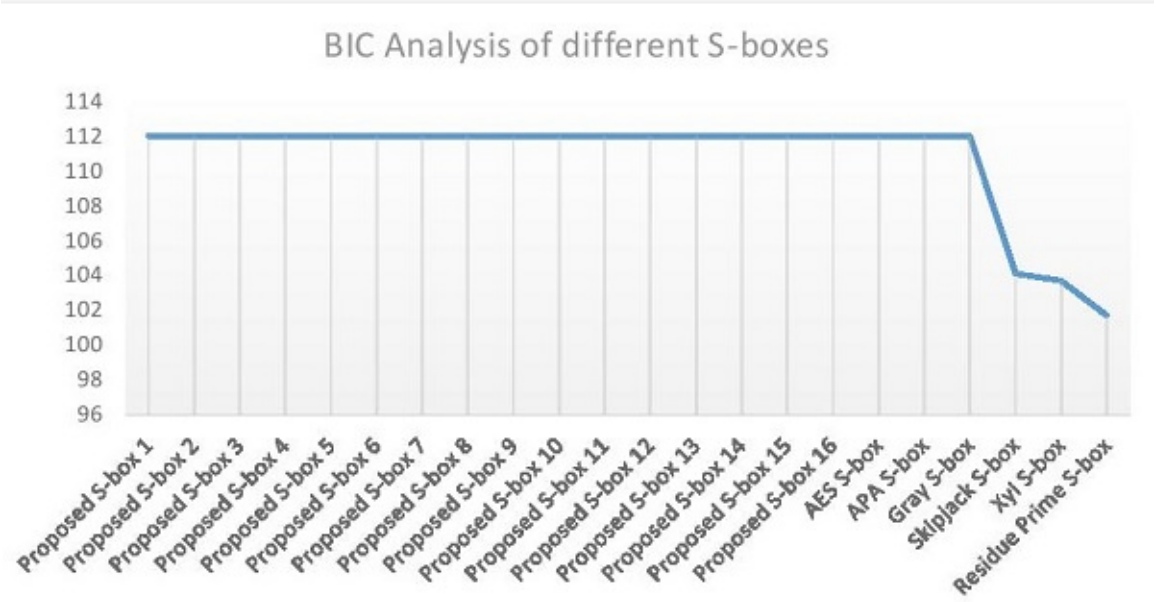


Figure 3.3: Comparison of BIC analysis of different S-boxes

3.5.4 Linear approximation probability

The maximum value of the imbalance of an event is said to be the linear approximation probability. The parity of the input bits selected by the mask G_b is equal to the parity of the output bits selected by the mask G_a According to Matsui s original definition

[20], linear approximation probability of a given S-box is defined as

$$LP = \max_{G_a, G_b \neq 0} |\frac{\sharp\{a \in x | a.G_a = S(a).G_b\}}{2^n}| - \frac{1}{2}|$$

Where G_a and G_b are input and output masks, respectively, x the set of all possible inputs; and 2^n is the number of elements of x. From Performance Indexes of S-boxes, we see that the average value of LP of the proposed S-boxes are 0.0625 which is appropriate against linear attacks. It can be seen in the figure 3.2 that the result of linear approximation analysis of all 16 proposed S-boxes are much better than the result of linear approximation probability analysis of Skipjack, Xyi, and Residue prime S-box.

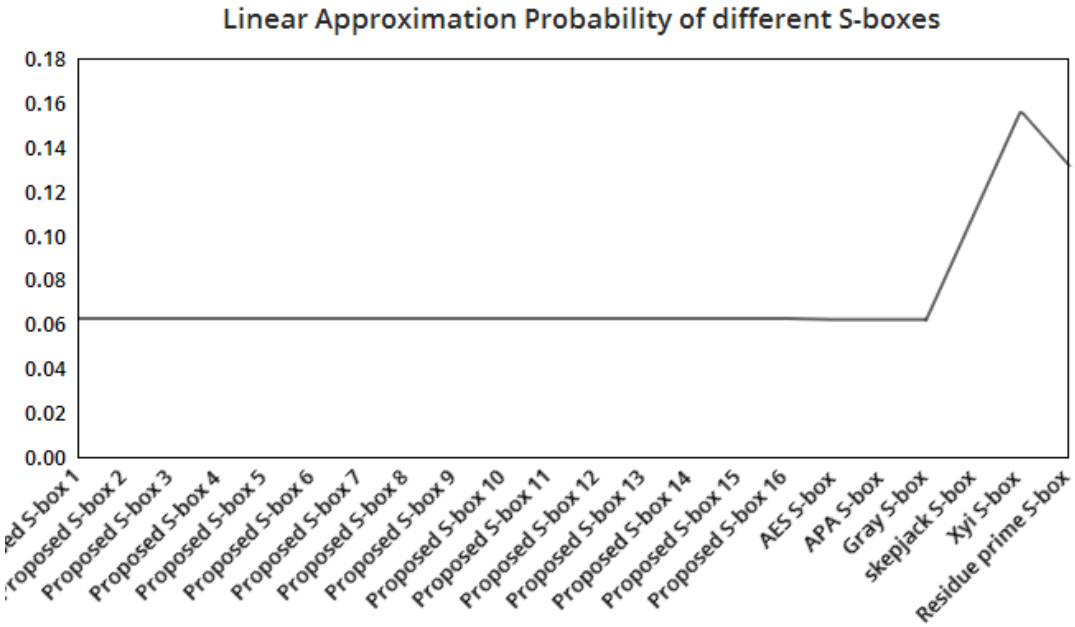


Figure 3.4: Comparison of LP analysis of different S-boxes

3.5.5 Differential approximation probability

The differential approximation probability (DP) of S-box is a measure for differential uniformity and is defined as

$$DP^s(\Delta a \rightarrow \Delta b) = [\frac{\sharp\{a \in x | S(a) = S(a \pm \Delta a = \Delta b)\}}{2^m}]$$

This means an input differential Δa_i should uniquely map to an output differential Δb_i so that ensuring a uniform mapping probability for each i. The average value of differential approximation probability for proposed S-boxes are 0.015625 (Performance Indexes of S-boxes) and Table 3 shows the comparison of differential approximation probability of different S-boxes.

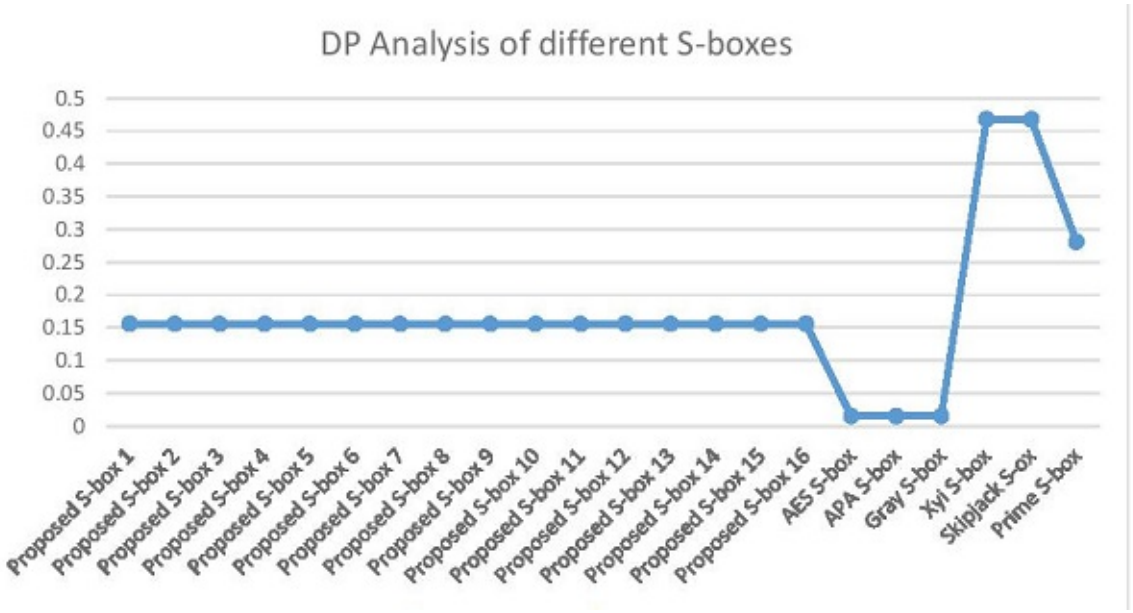


Figure 3.5: Comparison of DP analysis of different S-boxes

Performance indexes of S-box 1						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.546875	0.4375	0.509033	0.0141386		
BIC		112	112	0		
BIC-SAC		0.474609	0.501256	0.0129051		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 2						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.4375	00.496094	0.017304		
BIC		112	112	0		
BIC-SAC		0.472656	0.504883	0.0104725		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 3						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.4375	00.489502	0.0167477		
BIC	112	112	0			
BIC-SAC		0.46875	0.497559	0.0121931		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 4						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.4375	00.502441	0.01534543		
BIC		112	112	0		
BIC-SAC		0.490234	0.501883	0.009400		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 5						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.546875	0.4375	0.4956338	0.0160869		
BIC		112	112	0		
BIC-SAC		0.490234	0.501883	0.009400		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 6						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.546875	0.4375	0.506639	0.0160869		
BIC		112	112	0		
BIC-SAC		0.480469	0.054185	0.0140524		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 7						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.4375	00.503662	0.0169564		
BIC		112	112	0		
BIC-SAC		0.482422	0.501325	0.00987734		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 8						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.4375	0.501709	0.0137496		
BIC		112	112	0		
BIC-SAC		0.482422	0.505092	0.0119186		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 9						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.546875	0.453125	00.503174	0.0140285		
BIC		112	112	0		
BIC-SAC		0.488281	0.50014	0.009838244		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 10						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.453125	00.506348	0.0164989		
BIC		112	112	0		
BIC-SAC		0.476563	0.506836	0.0126308		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 11						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.546875	0.433125	0.492188	0.0.0133185		
BIC		112	112	0		
BIC-SAC		0.486328	0.498535	0.0091405		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 12						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.4375	00.51001	0.0186504		
BIC		112	112	0		
BIC-SAC		0.480469	0.501186	0.0186504		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 13						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.546875	0.4375	0.509521	0.0162014		
BIC		112	112	0		
BIC-SAC		0.482422	0.503418	0.0114676		
DP					0.015625	
LP	144					0.625

Performance indexes of S-box 14						
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.453125	0.492432	0.013879		
BIC		112	112	0		
BIC-SAC		0.476563	0.502581	0.0125502		
DP					0.015625	
LP	144					0.625

Table 3.19: Performance indexes of S-box 15

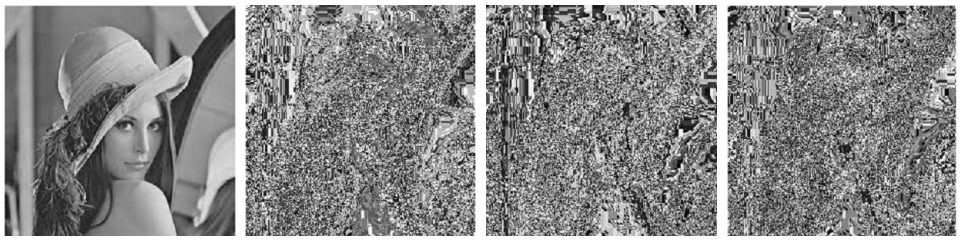
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.453125	0.510742	0.0159796		
BIC		112	112	0		
BIC-SAC		0.486328	0.50565	0.0119301		
DP					0.015625	
LP	144					0.625

Table 3.20: Performance indexes of S-box 16

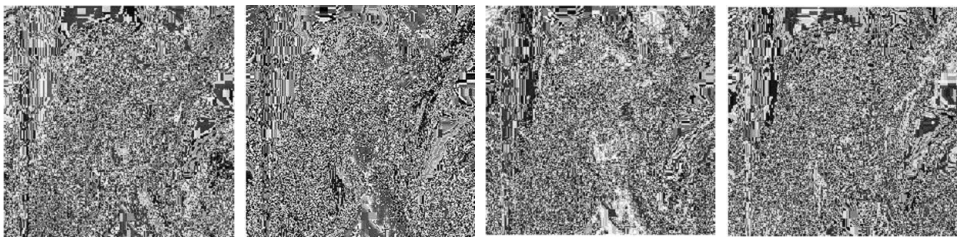
Analysis	Max	Min	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	112	112	112			
SAC	0.0.5625	0.453125	0.510742	0.0159796		
BIC		112	112	0		
BIC-SAC		0.486328	0.50565	0.0119301		
DP					0.015625	
LP	144					0.625

3.6 Statistical analysis of proposed S-boxes

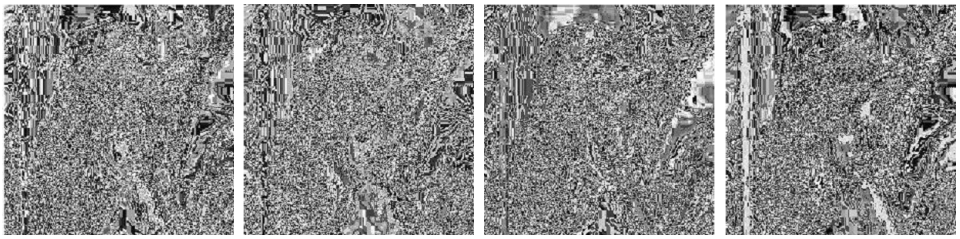
In this section, we have taken the image of Lenna and performed an image encryption experiment using proposed S-boxes, we apply MLC majority logic criterion which includes Contrast analysis, energy analysis, homogeneity analysis, correlation analysis and entropy analysis used to determine the best suitable S-box. The result of statistical analysis of proposed S-boxes and some other well known S-boxes are given in Table 3.21, it can be seen in the table that the statistical analysis result of all proposed S-boxes are almost same and batter then the result of other S-boxes.



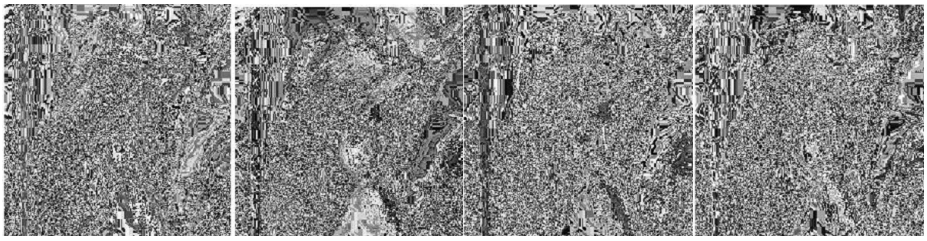
(a) Orignal (b) S-box 1. (c) S-box 2. (d) S-box 3.



(e) S-box 4. (f) S-box 5. (g) S-box 6. (h) S-box 7.



(i) S-box 8. (j) S-box 9. (k) S-box 10. (l) S-box 11.



(m) S-box 12. (n) S-box 13. (o) S-box 14. (p) S-box 15.

Figure 3.6: Encrypted Images.

3.6.1 Entropy

Entropy is the statistical analysis measure the randomness which can use in the characterize of the structure of image. The high level of randomness make complex

image detection process the Mathematically it can be written as,

$$H = \sum_{i=1}^{n} g(x_i) log_b f x_i$$

. In Table 3.21 show that the result of entropy analysis of encrypted images of different S-box. It can be seen that the entropy analysis of all proposed S-boxes are equal, and batter then the result of entropy AES, APA, Gray, Xyi, and Hussain S-box.

3.6.2 Energy

Energy analysis is used to measure the energy of encrypted image, Gray level Co-occurrence matrix (GLCM) are used for this purpose. In (GLCM) the squared component are called energy, mathematically it can be written as

$$E = \sum_{m} \sum_{n} f^2(v, u).$$

Here v and u denote the pixel of the image, and $f(v, u)$ are the number of gray-level co-occurrence. It can be seen in the table 3.18 that energy analysis of all proposed S-box is less than the energy analysis of AES S-box, APA S-box, Gray S-box, Residue Prime S-box, Xyi S-box.

3.6.3 Contrast

Contrast analysis is used to help the viewer to identify the object of an image. In image encryption process randomness is directly proportional to the contrast value, mean increasing randomness in encrypted image increasing the value of contrast. The

result of contrast analysis of all proposed S-boxes and some other S-boxes have given in table 3.21. The following mathematical formula is used to measure the contrast analysis

$$\sum_{n}\sum_{m}(m-n)^2 f(m,n).$$

3.6.4 Correlation

Correlation analysis is used to analyze the correlation of entire image pixels couple wise. There are three possible ways to select, Vertical, horizontal, and diagonal formate, for this purpose correlation analyzed the entire image with partial regions. The correlation is calculated by the following formula.

$$C = \frac{(u-\alpha u)(v-\alpha v)f(u,v)}{\sigma_u \sigma_v}.$$

where for the perfectly positive or perfectly negative images the value of correlation is 1 or -1, for the constant image the correlation is NaN, which mean it is not a number, just a data type which represented by the redefined value. The result of correlation of all proposed S-boxes are given in table 3.21.

3.6.5 Homogeneity

Homogeneity analysis is used to measure the closeness of elements which are distributed from GLCM to GLCM diagonals. It is also known as a gray tone spital dependency matrix. In tabular from, the GLCM is work to shows the statistic of arrangement gray level pixels. The process of entire form of GLCM extend this analysis.

The mathematical from of Homogeneity analysis are given below

$$H^* = \sum_u \sum_v = \frac{f(u,v)}{1-|u-v|}.$$

Table 3.21: Statistical analysis of different S-boxes

8×8 S-boxes	Contrast	Correlation	Energy	Homogeneity	Entropy
proposed S-box 1	9.5062	0.1532	0.186	0.4723	7.3021
proposed S-box 2	9.3720	0.1142	0.0190	0.4712	7.3021
proposed S-box 3	9.6826	0.1393	0.0184	0.4633	7.3021
proposed S-box 4	8.6784	0.1332	0.0193	0.4724	7.3021
proposed S-box 5	8.9918	0.1084	0.0191	0.4687	7.3021
proposed S-box 6	8.6557	0.1034	0.0186	0.4716	7.3021
proposed S-box 7	9.3562	0.1273	0.0184	0.4639	7.3021
proposed S-box 8	8.7901	0.1073	0.0193	0.4716	7.3021
proposed S-box 9	8.6826	0.1065	.0190	0.4755	7.3021
proposed S-box 10	8.7033	0.1904	0.0190	0.4838	7.3021
proposed S-box 11	8.5146	0.1105	0.0180	0.4693	7.3021
proposed S-box 12	8.3766	0.1386	0.0185	0.4761	7.3021
proposed S-box 13	9.0504	0.1160	0.0180	0.4653	7.3021
proposed S-box 14	9.8755	0.0957	0.0183	0.4600	7.3021
proposed S-box 15	9.9046	0.1252	0.0183	0.4555	7.3021
proposed S-box 16	9.5060	0.1532	0.0186	0.4723	7.3021
AES S-Box	7.5509	0.0554	0.0202	0.4662	7.2531
APA S-box	8.1195	0.1473	0.0183	0.4676	7.2264
Gray S-box	7.2301	0.0586	0.0203	0.4623	7.2301
Skipjack S-box	7.5283	7.7058	0.1025	0.0193	7.2214
Xyi S-box	8.3108	0.0417	0.0196	0.4533	7.2207
Residue prime	8.3108	0.0417	0.0202	0.4640	7.2035

Chapter 4

Conclusion

In the presented work a novel technique for the construction of 8×8 S-boxes over 16 different Galois fields is given. The method of linear fractional transformation is adopted by fixing the same parameters a, b, c, d for the design of all 16 S-boxes. The algebraic strength of these newly constructed S-boxes are measured by Nonlinearity, BIC, SAC, BIC-SAC, LP, and DP. So we observed after the comparison with well-known 8×8 S-boxes that the results are of finest value and up to the standard. In addition, it is determined that these new S-boxes are balanced, which make it strong. For the futuristic point of view; by using the linear fractional transformations, one can obtain a large class of S-boxes by varying the parameters a, b, c, d Moreover, other

construction techniques of S-boxes can also be used to generate the variety of good S-boxes.

Bibliography

[1] Daemen, J. and Rijmen, V. (2002). *The design of rijndael Aes. The Advanced Encryption Standard*.

[2] Zimmermann, R., Curiger, A., Bonnenberg, H., Kaeslin, H., Felber, N., Fichtner, W. (1994). *A 177 Mb/s VLSI implementation of the international data encryption algorithm.* IEEE Journal of Solid-State Circuits, 29(3), 303-307

[3] Cui, L and Cao, Y. (2007).*A new S-box structure named Affine-Power-Affine.* International Journal of Innovative Computing, Information and Control, 3(3), 751-759.

[4] Hussain, I., Shah, T., and Mahmood, H. (2010). *A new algorithm to construct secure keys for AES.* International Journal of Contemporary Mathematical Sciences, 5(26), 1263-1270.

[5] Tran, M. T., Bui, D. K., & Duong, A. D. (2008, December). *Gray S-box for advanced encryption standard. In Computational Intelligence and Security*, 2008.

CIS'08. International Conference (Vol. 1, pp. 253-258). IEEE.

[6] Kim, J. and Phan, R. C. W. (2009). *Advanced differential-style cryptanalysis of the NSA's skipjack block cipher*. Cryptologia, 33(3), 246-270.

[7] Yi, X., Cheng, S. X., You, X. H., and Lam, K. Y. (1997, November). *A method for obtaining cryptographically strong* 8×8 *S-boxes*. In Global Telecommunications Conference, 1997. GLOBECOM 97, IEEE (Vol. 2, pp. 689-693).

[8] Shah, T., Hussain, I., Gondal, M. A., & Mahmood, H. (2011). *Statistical analysis of S-box in image encryption applications based on majority logic criterion*. Int. J. Phys. Sci, 6(16), 4110-4127.

[9] Farwa, S., Shah, T., & Idrees, L. (2016). *A highly nonlinear S.box based on a fractional linear transformation*, Springer Plus 5:1658, DOI 10.1186/s40064.016.3298.

[10] W. Trappe, L. Washington,(2002) *Introduction to Cryptography with Coding Theoryî*, 2nd edition, Prentice Hall,.

[11] J, B, Fraleigh. (2003),*A First Course in Abstract Algebra, 7th edition*, University of Rhode Island.

[12] W. Stallings, (1999) *Cryptography and Network Security, Principles and Practice* 5th edition, Prentice Hall, 1999.

[13] Cameron, P., (January-March 2000) *Notes on Classical Groups* Queen Mary and Westfield College London E1 U.K School of Mathematical Sciences.

[14] Crama, Y; Hammer, P. L. (2011), *Boolean Functions, Cambridge University Press*

[15] Shannon, C. (1949) *"Communication theory of secrecy systems,"* Bell Syst. Tech. J. 28(4), 656–715.

[16] O.P. Verma, R. Agarwal, D. Dafouti, S. Tyagi,(2011) *Performance Analysis of Data Encryption Algorithmî, Electronics Computer Technology(ICECT)*, vol.5, 399-403.

[17] Hussain, I., Shah, T., Gondal, M. A., Wang ,Y., (2011). *Analysis of SKIPJACK S-Box*, World Applied Sciences Journal 13 (11): 2385-2388, 2011 ISSN 1818-4952

[18] Altaleb, A., Saeed M S., Hussain, I., Aslam, M. (2016) .*An algorithm for the construction of substitution box for block ciphers based on projective general linear group* AIP Advances 7, 035116 DOI 10.1063/1.4978264

[19] W. Trappe, L. Washington,(2002) .*Introduction to Cryptography with Coding Theory*, 2nd edition, Prentice Hall,

[20] Webster, A. F., and Tavares, S. E. (1985, August).*On the design of S-boxes.* In Advances in Cryptology—CRYPTO 85 Proceedings ($pp.523-534$). Springer Berlin Heidelberg

[21] W. Di e and M. Hellman,(1976) *New directions in Cryptography*, IEEE transactions in information theory, vol. 22 (1976), 644-654.

Index