بسم الله الرحمن الرحيم

In the name Of Allah, the most beneficent, the eternally merciful

Loop Based S-box Constructions and Data Hiding Implementation

By

Sadam Hussain

Department of Mathematics

Quaid-I-Azam University, Islamabad

Pakistan

2017

Loop Based S-box Constructions and Data Hiding Implementation

By

Sadam Hussain

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-I-Azam University, Islamabad

Pakistan

2017

Loop Based S-box Constructions and Data Hiding Implementation

By

Sadam Hussain

A thesis submitted in the partial fulfillment of the requirement for the degree of

MASTER OF PHILOSOPHY

in

Mathematics

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-I-Azam University, Islamabad

Pakistan

2017

Dedicated to

My

Beloved

Parents

Acknowledgement

All praises to Almighty Allah, the most Merciful and the more Beneficent, who created this universe and gave us the idea to discover it. First of all, I am highly grateful to Allah Almighty who helped and blessed me more than I deserve.

I deem it a great honor to express my deepest sense of gratitude to my honorable supervisor **Prof Dr. Tariq Shah** for his kind and able guidance, valuable comments and encouraging altitude throughout my research work.

Special thanks to **Atta Ullah (**Ph.D Scholar **)** for his help in this work.

I would like to express my appreciation to the faculty members and the administration of Mathematics department, Quaid-i-Azam University, Islamabad.

This acknowledgment would be incomplete unless I offer my humble veneration to my family especially to my brothers Sufyan Javed and Zaman Javed and Sisters for their endless love, care and supporting spiritually throughout my life and academic career.

Sincere thanks to all my friends and class mate's especially Sajjad Shoukat Jamal, Adnan Saeed Butt, Muhammad Nasir, Yasir Naseer, Muhammad Asif, Muhammad Tanveer, Mubsher Umer, Shahid Amanullah, Zeeshan Shahid and Muzammil Hanif for their necessary cooperation in the accomplishment of my dissertation

Last but not the least, I would like to thank one of my best teacher and friend **Dr. Umer Shoaib** (Assistant Professor in GCU Faisalabad), who have been a source of encouragement and motivation to complete the degree of Philosophy.

Sadam Hussain
June 2017

Preface

Cryptography is used for protection and transmitting information in such a way that only specified persons can read and process it. The basic cryptographic techniques are used for thousands of years in different areas. In history, many governments or organized groups mostly used cryptography to conceal secret messages from enemies. About 100 BC Julius Caesar made use of certain encryptions so that he may send secret messages to his army. This type of encryption is known as Caesar cipher, which is a type of substitution cipher (A cipher is an encryption or decryption algorithm and substitution means that each character of a message is replaced by another character to form the message unreadable).

Even though over the last 40 years, Modern cryptography is considered as a mature branch of science but it is still relatively new field of study compared to other subjects and every new day brings so many developments. But now a days, millions of secure and encoded transmissions occur online every day. Cryptographic standards are used to protect data, banking data, images, videos, health information and much more. In all these, the online security threats evolve so quickly, so there is a need for network security, which is the study of methods for protecting data in communication systems and computers from unauthorized authorities. Network security or data security progressed rapidly since 1975. Modern cryptography and Network security techniques are mostly based on mathematical theory and computer science practices.

For few years, finite Galois rings have great importance in cryptography and coding theory. In 1979, Priti Shankar established a relationship between BCH- codes over Galois ring $GR(p^k, m)$ and Galois field $GF(p^m)$ through a p-reduction map. In the construction of these BCH-codes, the maximal cyclic subgroup G_{p^m-1} of a group of units of Galois ring $GR(p^k, m)$ plays a pivotal role. The maximal cyclic subgroup G_{p^m-1} is isomorphic to Galois group $GF(p^k)^*$ and this provides a way to use it in cryptography. The Galois rings were firstly used in cryptography by Shah et al.

In cryptography, the substitution box (S-box) is the vital component of almost all symmetric cryptosystem. The process of encryption creates confusion and diffusion in data and the S-box plays a key role to make confusion in data because it is the only non-linear and invertible part in the encryption process. The strength of encryption technique depends on the ability of S-box in twisting the data hence, the process of finding new and powerful S-boxes is of great importance in the field of cryptography. Firstly, S-boxes are constructed only by using Galois fields. But Shah et al. give method of construction of S-boxes by using elements of Galois rings $GR(4,2)$ and $GR(4,4)$. Here Shah et al. used the maximal cyclic subgroup of the group of units of Galois ring $GR(4,4)$, which has 16 elements and so that 4×4 S-box is formed. The maximal cyclic subgroup of a group of units of commutative chain ring is also used to construct healthier S-box.

The purpose of the research is to develop a good understanding of some basic concepts of cryptography but mainly focused on the construction of S-boxes on inverse property loops of order 16 and 256. The newly constructed S-boxes are then analyzed by some algebraic analyses to determine the strength of the proposed S-boxes and by statistical analyses of their application in image encryption algorithms.

The details of the dissertation are here under:

- The first chapter consists of three section. In the first section, we discussed some basic algebraic concepts, which were necessary to understand cryptography. In the second section, we discussed some basic components of cryptography and lastly we discussed some examples of classical and modern cryptography. In the last section, we discuss some basic definitions of loop theory.
- In the second chapter, the concept of S-box is discussed. In addition, the construction techniques of S-box on a maximal cyclic subgroup of a group of Galois ring $GR(2^k, 4)$ for $1 \leq \mathrm{k} \leq 5$.
- In the third chapter, a novel technique to construct S-boxes based on inverse property loops of order 16 and order 256. Some algebraic analysis to determine the strength of these S-boxes are also given in this chapter
- In the fourth chapter, we discuss the application of these S-boxes in watermarking and image encryption.
- The last chapter consists the conclusion of this work.

Contents

Notations

S, T, X, Y, R and F…	Sets, Groups, Rings, Fields
$\varphi, f, g, \alpha, \beta$ ∨, ∧,~, ⊕ …	Functions
., +, *, ¤,⊕,⊙ …	Binary Operations
$\alpha \circ \beta$	Composition of functions
L…	Loops
a, b, c, x, y, z…	Elements of set
$s_1 \in S$ …	s_1 Belongs to set S
$\mathbb{Z}_m$…	Ring of modulo classes
$\frac{S}{R}$ …	Factor Ring
$\wp$ …	Plaintext
$\mathbb{C}$ …	Ciphertext
L_a, R_a …	Left and Right translations
(a, b) …	Commentator
(a, b, c)…	Associator
Z(L) …	Center of loop
N(L) …	Nucleus of loop
$N_\lambda(L)$ …	Left nucleus
$N_\mu(L)$ …	Middle nucleus
$N_\rho(L)$ …	Right nucleus
S-box …	Substitution boxes
R[x] …	Ring with polynomial
BIT …	Bit Independence Criterion
SAC …	Strong Avalanche Criterion
DP …	Differential approximation probability
LP …	Linear approximation probability
MLC …	Majority Logic Criterion

Chapter 01

Algebraic Preliminaries

This chapter explains the facts in the background of modern cryptography. We review some basic concept which is related to upcoming chapters. This chapter has three sections. In a section first, we define some algebraic terms, which are necessary to understand cryptography. In a section second, some cryptographic terms are defined, Examples of classical and modern cryptography are also given in this section. In the last section, we defined some terms of loop theory which is necessarily part of this dissertation.

1.1 Algebraic structures

1.1.1 Binary Operation

Let S be a non-void set and "$*$" be operation on S then $*$ is called binary operation on S if

$$for\ all\ s_1, s_2 \in S \Longrightarrow s_1 * s_2 \in S$$

Note that if "$*$" is a binary operation on S then $(S,*)$ is called groupoid.

1.1.2 Semigroup

A groupoid $(S,*)$ is called Semigroup if it is associative, that is

$$for\ all\ \ s_1, s_2, s_3 \in S, \quad (s_1 * s_2) * s_3 = s_1 * (s_2 * s_3)$$

1.1.3 Monoid

A semigroup $(S,*)$ is called monoid if there is a unique element $e \in S$ satisfying

$$e * s = s * e = s\ , \qquad for\ all\ s \in S$$

Here "e" is called identity element of set S.

1.1.4 Group

A monoid $(S,*)$ is called a group if, for each element $s_1 \in S$, there is a unique element s_2 in S which satisfying $s_1 * s_2 = s_2 * s_1 = e$.

Example 1: The sets $Z, Q, R, and\ C$ are all groups under the binary operation of " $+$ ".
$(\mathbb{Z}_m, +mod\ m)$ is also group with 0 as an identity element, here $\mathbb{Z}_m = \{0,1,2, \dots, m-1\}$.
Each $s_1 \in \mathbb{Z}_m$ has an inverse $-s_1$, for which $s_1 + (-s_1) \equiv 0\ mod(n)$. But the set $\mathbb{Z}_m$ not a group under the binary operation " $\cdot$" mod m.
Remark 1: The sets $(N,\cdot)\ and\ (\mathbb{Z},\cdot)$ are only monoids but not groups. Here operation " $\cdot$ " is a simple multiplication of numbers.

Commutative group

If the commutative law is satisfied in a group $(S,*)$ then we called it a commutative group that is.

$$s_1, s_2 \in S,\ \ s_1 * s_2 = s_2 * s_1$$

Example 2: The sets $Z\ and\ R$ are commutative groups under the binary operation " $+$ ".
$(M, +)$ is also a commutative group, where M is set of $n \times n$ matrices and binary operation " $+$ " is a usual addition of matrices. The set N of all invertible matrices is non-commutative group under the operation multiplication of matrices.
Remark 2: The Commutative group is also known as an abelian group.

1.1.5 Homomorphism

A function $\varphi: S \to T$ is called a homomorphism of group $(S,*)$ to group $(T,\cdot)$, if

$$\varphi(s_1 * s_2) = \varphi(s_1) \cdot \varphi(s_2), \qquad for\ all\ s_1, s_2 \in S$$

Endomorphism: If both S, T are the same groups, then homomorphism $\varphi : S \to T$ is called endomorphism.

Epimorphism: An onto homomorphism which is also called surjective homomorphism $\varphi : S \to T$ is called Epimorphism.

Monomorphism: A one-one homomorphism which is also called injective homomorphism $\varphi : S \to T$ is called monomorphism. That is,

$$\varphi(s_1) = \varphi(s_2) \Longrightarrow s_1 = s_2 \ \ for\ all\ s_1, s_2 \in S.$$

Isomorphism: An injective and surjective homomorphism $\varphi : S \to T$ is known as an isomorphism.

Remark 3: Two groups $M\ and\ H$ are said to be isomorphic if there is an isomorphism between $M\ and\ H$.

1.1.6 Coset

Suppose H be a subset of a group $(S,*)$ and $s \in S$ then we say that $s * H = \{s * r : r \in H\}$ $(H * s = \{q * r : r \in H\})$ is a left coset (right coset) of H in S.

Example 3: Suppose that $S = (Q_8, .)$ and $H = \{1, -1\}$, then

$$1 + H = -1 + H = \{1, -1\} = H + 1 = H + -1$$
$$i + H = -i + H = \{i, -i\} = H + i = H + -i$$
$$j + H = -j + H = \{j, -j\} = H + j = H + -j$$
$$k + H = -k + H = \{k, -k\} = H + k = H + -k$$

are the left cosets of H in S.

Normal subgroup

Let $(S,*)$ be a group then a subgroup N is called a normal subgroup of S if $\forall\ s \in S, srs^{-1} \in N$.

Remark 4: A subgroup N is called normal subgroup of a group $(S,*)$ if

$$for\ all\ s \in S, \qquad s * N = N * s$$

Example 4: In example 3, H is a normal subgroup of group S.

1.1.7 Factor group

Let $(S,*)$ be a group under binary operation " $*$ " and N be its normal subgroup, then the set of all cosets of N in S is called factor group of S mod N. It is denoted by

$$\frac{S}{N} = \{s * N : s \in S\}$$

The binary operation in $\frac{S}{N}$ is defined as $(s_1 * N) * (s_2 * N) = (s_1 * s_2) * N, for\ all\ s_1, s_2 \in S$

Example 5: Suppose that $S = (\mathbb{Z}_6, +)$ is a group and $N = \{0,3\}$ is a normal subgroup of S. Then factor group is given below.

$$\frac{S}{N} = \{N, 1 + N, 2 + N\}$$

Finite group

If the number of elements in a group S is finite, then we call it a finite group. This symbol $|S|$ indicates the number of elements in a group. In other words, a group S is finite if $|S| < \infty$.

Cyclic group

Suppose that $(S,*)$ is a group and $s \in S$. If for each $z \in S$, there exist a number $m \in \mathbb{N}$ such that the equality $z = s^m$ is held. Then we say that S is cyclic group generated by s and s is called generator of group S. It is denoted by $S =< s >$

Example 6: Suppose that $S = \{1, -1, i, -i\}$, then group $(S, .)$ is cyclic and generated by i and $-i$.

Group Action

Suppose that $(S,*)$ is a group and X is non-void set, then the action of group S on a set X from left is a mapping $\varphi: S \times X \rightarrow X$, which satisfies the following conditions.

i. $\varphi\ (e, x) = e\ \ \varphi\ h = h\ :\ for\ all\ x \in X$. Here e is an identity element in S.

ii. $\varphi\big(m_1, \varphi(m_2, x)\big) = \ \varphi(m_1 * m_2, x)\ , \forall\ s_1, s_2 \in S\ and\ x\ \in X.$

1.1.8 Ring

Suppose that R is a non-void set and $+: R \times R \rightarrow R$, $.: R \times R \rightarrow R$ are two binary operations on it. Then we say that R is Ring if following conditions hold.

- $(R, +)$ is an abelian group.
- $(R, .)$ is a semigroup.
- Distributives laws are hold. That is, for all $y_1, y_2, y_3 \in R$

$$y_1.(y_2 + y_3)\ = (y_1.y_2) + (y_1.y_3)\ and\ (y_1 + y_2).y_3\ = (y_1.y_3) + (y_2.y_3).$$

Abelian Ring

If commutative law with respect to a binary operation " $\cdot$ " is satisfied in a ring $(R, +, .)$, then R is called an abelian ring.

Example 7: the set of integer and set of real numbers are abelian rings under usual addition and multiplication.

Zero Divisor

Suppose that $(R,+,.)$ is a ring and non-zero $z \in R$. If there exist non-zero $y \in R$ such that $z \cdot y = 0$, then z is called zero divisor.

Example 8: Suppose $\mathbb{Z}_{10}$ is a ring, then $2 \cdot 5 = 10 = 0\ mod(10)$, since both 2,5 are non-zero so 2 and 5 are zero divisors.

Ring with identity

Suppose $(R,+,.)$ be a ring, if there exist an element $e \in R$ such that $y.e = e.y = y$ for all $y \in R$.then e is called identity element of R with respect to operation " $\cdot$ " and the ring $(R,+,.)$ is called ring with identity.

Unit element

Suppose that $(R,+,.)$ is a ring and non-zero element $x \in R$. If there exist non-zero element $y \in R$ such that $z.y = e$, then x is called the unit element of the ring. Here e represents the identity element of a ring with respect to binary operation " $\cdot$ " .

1.1.9 Ideal of a Ring

A subset I of a $(R,+,.)$ is called ideal if following conditions hold.

i. I is a subgroup under $+$. That is, for all $z_1, z_2 \in I \Longrightarrow z_1 - z_2 \in I$.

ii. I is closed over a ring R. That is, for all $s \in R$ and for every $z_1 \in I$ implies $sz_1 \in I$.

Prime Ideal

Suppose that P is a proper ideal of a commutative ring $(R,+,.)$. If $for\ all\ y, z \in Y, yz \in P$ implies either $y \in P$ or $z \in P$, then P is called prime ideal of R.

Principle Ideal

Let $(R,+,.)$ be a ring and I be an ideal of R. Then I is called principal ideal if it is generated by a single element of it. That is $I =< z >= \{yz : y \in R, z \in I\}$.

Remark 5: If every ideal is principal ideal in ring R. Then we say R is a principal ideal ring.

Local Ring

A ring $(R,+,.)$ is called local ring if it has only one maximal ideal.

Example 9: The rings of the form $\mathbb{Z}_{p^k}$, where k is non-zero positive integer and p is any prime number are local rings, i.e. $\mathbb{Z}_{16}$, $\mathbb{Z}_{25}$, $\mathbb{Z}_{27}$ are the examples of a local ring.

Quotient ring

Let $(R,+,.)$ be a ring and I be its ideal, then $\frac{R}{I} = \{y + I : y \in Y\}$ is Quotient ring with respect to the operations defined as

$$(y_1 + I) + (y_2 + I) = (y_1 + y_2) + I \ \ and \ (y_1 + I).(y_2 + I) = (y_1.y_2) + I$$

Polynomial Ring

Let R be a ring, then $R[x]$ is the collection of all polynomial of degree n whose coefficient are elements of R that form a ring with given binary operation interpret as:

If $g = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$ and $h = b_0 + b_1x^1 + b_2x^2 + \cdots \ + b_nx^n$, then

$g + h = (a_0 + b_0) + (a_1 + b_1)x^1 + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n$ &

$g.h = c_0 + c_1x^1 + c_2x^2 + \cdots + c_nx^n$ here $c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_0b_i$.

It is denoted by $(R[x],+,\cdot)$ and is called a polynomial ring.

Reducible Polynomial

Let $g(x)$ be a polynomial in $R[x]$. Then $g(x)$ is called reducible polynomial if it can be factorized into two or more polynomials.

Irreducible Polynomial

A polynomial $f(x)$ in $R[x]$ is called a reducible polynomial if it cannot be factorized into two or more polynomials.

Monic Polynomial

A polynomial $g(x) = c_0 + c_1x^1 + \cdots + c_nx^n$ is called a monic polynomial if $c_0 = 1$.

Primitive Polynomial

A polynomial $h(x) = c_0 + c_1x^1 + c_2x^2 + \cdots + c_nx^n$ is called a primitive polynomial if greatest common divisor of all the coefficients of $h(x)$ is 1.

Remark 6: Every monic polynomial $g(x)$ is primitive

1.1.10 Field

A non-empty set F with two binary operations " $+$ " and " $\cdot$ " is called field if it satisfies the following conditions.

- F is an abelian group under operation $+$.
- $\mathrm{F}/\{0\}$ is an abelian group under operation $\cdot$.
- Distributive laws hold, That is, for all $y_1, y_2, y_3 \in$ F.

$$y_1 \cdot (y_2 + y_3) = (y_1 \cdot y_2) + (y_1 \cdot y_3)$$

$$(y_1 + y_2) \cdot y_3 = (y_1 \cdot y_3) + (y_2 \cdot y_3)$$

Example 10: The set $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$ with usual addition and multiplication is the example of the smallest infinite field with 0,1 additive and multiplicative identities respectively. If $n = p$ then ($\mathbb{Z}_n$,$\oplus$,$\odot$) set of integers modulo n is a finite field.

Galois Field

A field F is called Galois field if it has finite order. That is order is prime or a power of the prime. For each prime p and a natural number m there exist a Galois field $G\mathrm{F}(p^m)$ of order p^m.

For each prime p and natural number m greater than 1, set of polynomials of equivalence classes is a field of order p^m, coefficients of these polynomials are the elements of $GF(p)$ and m is the degree of the irreducible polynomial over $GF(p)$. That is if $f(\xi)$ is an irreducible polynomial of degree m, Then

$\frac{GF(p)[x]}{<f(\xi)>} = GF(p^m) = \{a_0 + a_1\xi^1 + a_2\xi^2 + \cdots + a_{k-1}\xi^{k-1} : a_i \in \mathrm{GF(p)}\}$, where ξ is the primitive root of $f(x)$.

Example 11: If $p = 3$ and $g(\xi) = 1 + \xi + \xi^3$ is an irreducible polynomial of degree 3 and ξ is the primitive root of $g(x)$. Then the elements of $GF(3^2)$ are $\{0,1,\xi,\xi^2,1+\xi,1+\xi^2,\ \xi+\xi^2,1+\xi+\xi^2\}$.

1.1.11 Boolean Algebras

Suppose X be a non-void set containing $0, 1$ with binary operations AND $(\wedge)$, OR $(\vee)$ and a unary operation Negation $(\sim)$ on a set X. Then set X is called Boolean algebra if it satisfying the following axioms.

i. For all $x_1, x_2, x_3 \in X$ $x_1 \vee x_2 = x_2 \vee x_1$ and $x_1 \wedge x_2 = x_2 \wedge x_1$.

ii. $x_1 \wedge (x_2 \vee x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3)$ and $x_1 \vee (x_2 \wedge x_3) = (x_1 \vee x_2) \wedge (x_1 \vee x_3)$.

iii. $0 \vee x = x$ and $1 \wedge x = x$ for all $x \in X$.

iv. $x \wedge (\sim x) = 0$ and $x \vee (\sim x) = 1$ for all $x \in X$.

Remark 7: $x_1 \vee x_2$ and $x_1 \wedge x_2$are also denoted as $x_1 + x_2$ and $x_1 \cdot x_2$ respectively.

Example 13: Suppose that Y is a non-void set. Then the collection of all subsets of Y which is known as the power set of Y forms a Boolean algebra in which $0 = \emptyset$ and $1 = Y$ with binary operations $\cup$, $\cap$ and complement as unary operations.

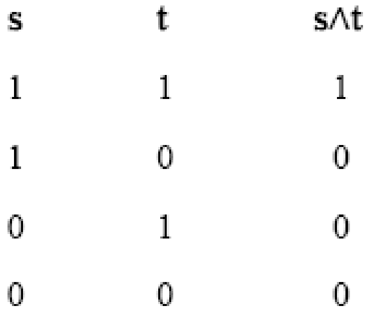
1.1.12 Boolean Function

Suppose that X is a Boolean algebra. A mapping $\phi: X^n \rightarrow X$ is called a Boolean function, here n is a non-negative integer. In cryptography, a multi-valued Boolean function is a function which defined on an $F_2{}^k$ to an $F_2{}^m$ with binary vectors of length k and m.

1.1.13 Some Logic Operations

AND Operation

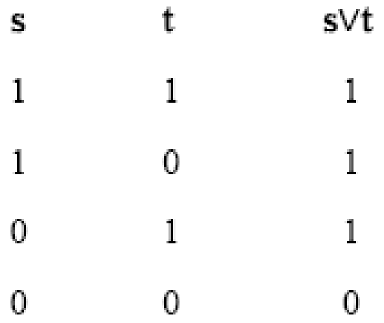
Suppose that $X = \{0,1\}$, then a mapping $\wedge : X \times X \rightarrow X$ is called AND Operation. Its output is 1 only when both inputs are 1 otherwise, its output is 0. Its truth table is given below:



s	t	s∧t
1	1	1
1	0	0
0	1	0
0	0	0

OR Operation

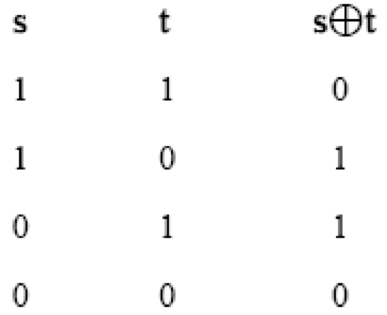
Suppose that $X = \{0,1\}$. A mapping $\vee : X \times X \to X$ is called OR Operation. Its output is 0 only when both inputs are 0, otherwise, its output is 1. Its truth table is given below:



s	t	s∨t
1	1	1
1	0	1
0	1	1
0	0	0

XOR Operation

Suppose that $X = \{0,1\}$. A mapping $\oplus : X \times X \to X$ is called XOR Operation. Its output is 1 when both inputs are different, otherwise, its output is 0. Its truth table is given below:



s	t	s⊕t
1	1	0
1	0	1
0	1	1
0	0	0

Remark 8: It is possible that inputs may be more than two in a XOR Operation, but its output is 1 only when numbers of 1's is odd in an input otherwise 0.

1.2 Basic Terminologies of Cryptography

In order to understand cryptography completely, we first talk over some basic terminologies which are given below [1, 4].

Plain Text

The text or message in understandable form is said to be a Plain text. It is English alphabets, characters, etc.

Cipher Text

When some algorithm is applied on a plain text then the resulting message or data is known as Cipher text. It may be is characters or English alphabets, etc.

Encryption Algorithm

The method in which the plain text is transformed into cipher text by using some secret key is called Encryption algorithm.

Decryption Algorithm

The method in which the cipher text is recovered to plain text by using some secret key is said to be decryption algorithm.

The encryption and decryptions secret keys always kept hidden, only sender and receiver know about it so that enemy even knows the algorithm but he could not read the data or message without the secret key.

Interceptor

The party or a person other than sender and receiver is said to be an interceptor or an attacker who try decrypt the data.

Plaintext Alphabet

The set of characters or letters which we used to write the plaintext is called Plaintext Alphabet. Generally, English alphabet, some characters like numbers and punctuation marks are used for Plaintext Alphabet

Cipher Text Alphabet

The set of characters or letters which we used to write the cipher text is called Cipher text Alphabet. It might be possible that both plaintext alphabets and cipher text alphabets are same or may be different. For example suppose $\{a, b, c, \dots, z\}$ used for plaintext alphabets but $\{A, B, C, \dots, Z\}$ or $\{1,2,3, \dots, 26\}$ are used for cipher text alphabets.

Key Size

The size of a secret key which is used in encryption or decryption algorithm to encrypt or decrypt the data is called key size. The size of key depend upon the algorithm which is used in encryption or decryption algorithm. Different key size is used in different algorithms. That is, 64 bits key is used in DES and 128, 192 and 256 bits keys are used in AES.

Cryptanalysis

A method in which the interceptor try to find a secret key used in the encryption algorithm so that he read the data or message is called cryptanalysis. He tries to find a secret key by using all possible keys, it is called as brute force attack or exhaustive key search.

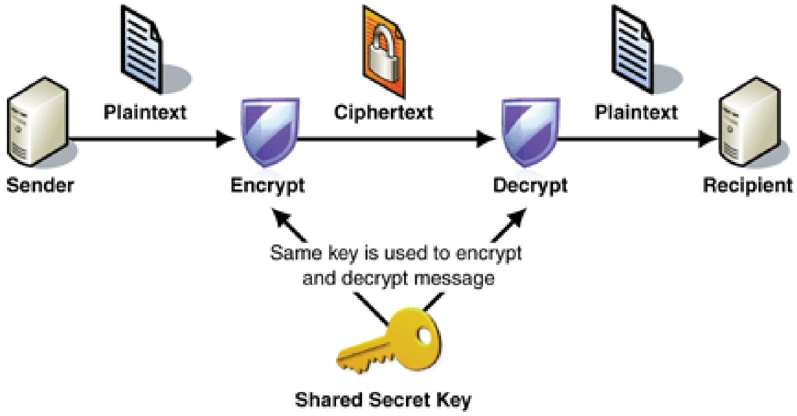
1.2.1 Classes of Cryptography

There are two main classes of cryptography on the base of key operation used,

- Same Key Cryptography (Symmetric)
- Different Key Cryptography (Asymmetric)

Same Key Cryptosystem

The Same key is used for the encryption and decryption algorithm in a symmetric key cryptography. In a symmetric key cryptosystem, the secret key is only accessible to the sender and receiver. These types of cryptosystems are also commonly called private key cryptosystems or single key cryptosystems. The most famous same key cryptosystems are AES, DES, RC4, Triple DES, Two fish etc.



There are further two branches of symmetric key cryptography.

- Stream Cipher
- Block Cipher

Stream Cipher

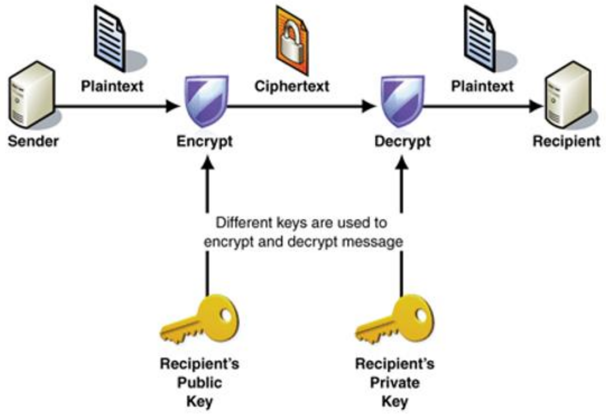
A stream cipher is an encryption algorithm which encrypts the data one bit or bytes of plain text at a time. Auto keyed vigenere is the example of classical stream cipher and ChaCha, RC4 and Fish cipher are examples of modern cryptographic stream ciphers. It remains to use an infinite stream of pseudorandom bytes as a key. A stream cipher is designed to approximate idealized cipher which is known as One paid time. The keys for stream cipher are given to both the sender and receiver through some secure medium. A stream cipher is not breakable unless one can find keystream. For daily life applications, the bit-stream generator is carried out in an algorithmic procedure and bit-stream can be established by both the sender and receiver. In this way, the bit-stream generator is used as an algorithm of key controlled and it may produce a stream bit, which is strong in cryptographic aspects. In this way, the users share only generating key and they have a knowledge of producing keystream.

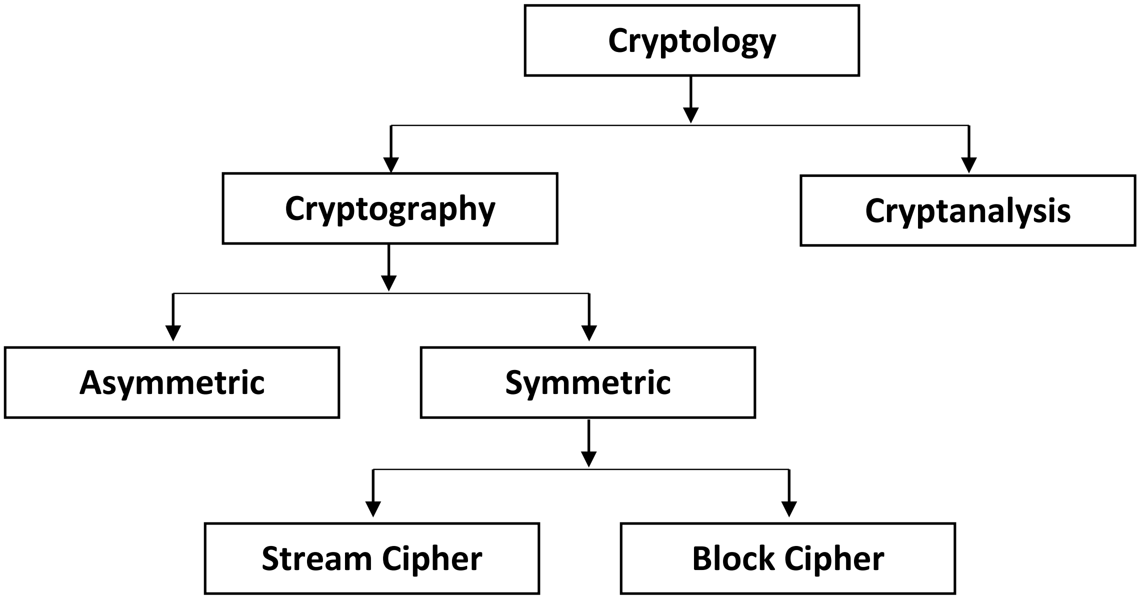
Block Cipher

The working of a block cipher is in a plain text and it fabricates same length block of cipher text. Normally the blocks used in a block cipher are 64 bits or 128 bits. These ciphers are complex and comparatively unhurried. In an immense range of applications block cipher are preferred as compared to a stream cipher. AES, DES and Triple DES have commonly used examples.

Asymmetric Key Cryptosystem

In the Asymmetric key cryptosystem, public and private key are used for the encryption and decryption of data, that’s way it is also called public key cryptography. Anyone who is interested has an access on a public key but on the other hand, only official person know the private key. RSA is the commonly used as a public-key cryptosystem. This system is used for authentication, confidentiality or both.





1.2.2 Some Classical and Modern Ciphers

1.2.2.1 Classic Ciphers

Caesar Cipher

The Caesar cipher is also called a shift cipher, which is the earliest and simplest substitution introduced by Julius Caesar. Each letter of the alphabet is substituted with a letter corresponding to a certain number of letters up to or down to letters. For example,

Plain text: ATTACK IS IMMINENT for $k = 5$ has a cipher text

Cipher text: PHHW XV DIWHU WKH MXLFH SDUWB

For the given value of k, we shift the each character of the alphabet by k times like in above example for $k = 5$ plain characters change in given below.

Plain characters: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher characters: F G H I J K L M N O P Q R S T U V W X Y Z A B C D E.

Now if we change each letter into a numerical value, then we explain the Caesar ciphering scheme as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the enciphering scheme for cipher value $\mathbb{C}$ and plain value $\wp$ is given below.

If $\mathbb{C}$ is cipher text and $\wp$ is a plain text, then encryption algorithm is defined as:

$$\mathbb{C} = \ E(\wp, 5) = (\wp + 5)mod26$$

We can choose any number from $1\ to\ 25$ for a shift in a Caesar ciphering algorithm. That is

$$\mathbb{C} = E(\wp, h) = (\wp + h)mod26$$

We can decipher the given cipher text into plain text by using deciphering scheme given below

The decryption algorithm is described as:

$$\wp = D(h, \mathbb{C}) = (\mathbb{C} - h)mod26$$

Example 14: when $k = 3$, then a plain text "ALGEBRA" becomes "DOJHEUD".

Affine Cipher

The more general form of a Caesar cipher is an affine cipher which is a one to one crosspondance between $\mathbb{Z}_n$ to a $\mathbb{Z}_n$, defined as. $r \longrightarrow (cr + d)mod\ n$, for $c, d \in \mathbb{Z}_n$, and c is a unit element in $\mathbb{Z}_n$ because otherwise, the inverse of the function is not invertible. If n is prime, then each element of $\mathbb{Z}_n$ is a unit and we have more choices for selecting c.

Example 15: Using the mapping above and affine cipher $r \longrightarrow (5r + 6)mod\ 26$, encipher the SOCRATES.

Plain text	S	O	C	R	A	T	E	S
r	18	14	2	17	0	19	4	18
$5r + 6$	96	76	16	91	6	101	26	96
$(5r + 6)mod\ n$	18	24	16	13	6	23	0	18
Cipher text	S	Y	Q	N	G	X	A	S

So the ciphertext of SOCRATES is SYQNGXAS. The inversion of affine cipher is also possible by using the inversion mapping.

Hill Cipher

The Hill cipher is the generalization of the affine cipher. Let X be a collection of plaintext and $\mathbb{Z}_n$ be a ring of modulo classes. Then the mapping $g: X^k \rightarrow (\mathbb{Z}_n)^k$ defined by $g(x_1, x_2, \dots, x_k) = (g(x_1), g(x_2), \dots, g(x_k))$ is the extension of affine cipher. Where k is a positive integer.

Now

$$\mathbb{Z}_n^r = \left\{ \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix} : c_i \in \mathbb{Z}_n \right\}$$

And

$$\mathbb{Z}_n^{r\times r} = \left\{ \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1k} \\ c_{21} & c_{22} & \cdots & c_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ c_{k1} & c_{k2} & \cdots & c_{kk} \end{bmatrix} : c_{ij} \in \mathbb{Z}_n \right\}$$

Now suppose an invertible matrix $U \in \mathbb{Z}_n^{r\times r}$, then $\det(U)$ is also invertible in $\mathbb{Z}_n$ and the mapping $g\colon \mathbb{Z}_m^r \to \mathbb{Z}_m^r$, defined by $g(C) = UC + V$, where $V \in \mathbb{Z}_m^r$. This type of encryption system is said to be Hill cipher. One can define a decryption scheme by using the inverse of a function g.

Example16: Consider the plaintext “$MATHEMATICIANS$” and the mapping defined as $g\colon \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2$ $s.t\ g(C) = (UC + V)\ mod 26,$ where $U = \begin{bmatrix} 3 & 5 \\ 2 & 5 \end{bmatrix}$ $and\ V = \begin{bmatrix} 5 \\ 3 \end{bmatrix}$. Since Det $(U) = 5$ and $(5,26) = 1$, therefore, U is invertible and encryption scheme of plaintext is given below.

$Plaintext$	MA	TH	EM	AT	IC	IA	NS
$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$\begin{bmatrix} 12 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 19 \\ 7 \end{bmatrix}$	$\begin{bmatrix} 9 \\ 12 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 19 \end{bmatrix}$	$\begin{bmatrix} 8 \\ 2 \end{bmatrix}$	$\begin{bmatrix} 8 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 13 \\ 18 \end{bmatrix}$
$f\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right)$	$\begin{bmatrix} 15 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 19 \\ 24 \end{bmatrix}$	$\begin{bmatrix} 14 \\ 3 \end{bmatrix}$	$\begin{bmatrix} 22 \\ 20 \end{bmatrix}$	$\begin{bmatrix} 13 \\ 3 \end{bmatrix}$	$\begin{bmatrix} 3 \\ 19 \end{bmatrix}$	$\begin{bmatrix} 4 \\ 15 \end{bmatrix}$
$Ciphertext$	PB	TY	OP	WU	ND	DT	EP

So PBTYOPWUNDDTEP is the ciphertext of given plaintext.

1.3 Concepts of Quasigroup and loop theory

As we know that in science history several illustrations where at definite times undoubted innovatory ideas were, so to state, in the imagination till at diverse places they demonstrate themselves in different forms independently. The ancient operation of non-associativity used by men was ordinary subtraction of natural numbers. But in 1845, Arthur Cayley introduced Cayley numbers which are first non-associative example in abstract. Later, its generalization was presented by Dickson.

In 1920, due to structural properties in alternative rings, it became the subject of potential interest. Other classes for structures of non-associativity deals with one binary operation. In 1929, Anton K. Suschkewitsch in his paper Generalization of Associative Law deals with binary system in which he explicitly mentioned the non-associativity. In the research literature of alternative algebra, there were numerous publications of America on quasigroups. In 1937, Theory of Quasi-Groups, presented by Haussmann and Ore. Then in 1939, Quasi-Groups Which Satisfy Certain Generalized Associative Laws, is given by Murdoch and in 1940 Quasi-Groups, by Garrison.

In 1942, Garrett Birkhoff firstly instigated the lattice ordered groups notion. Then, in 1944 R.H Bruck presented various results in quasigroup theory. In 1948, Zelinski designated about ordered loops. The notion of number theory non-associativity was methodically studied by Evans (1957). The theory of loop was explained by Bruck in 1963. In 1964 and 967, many critical properties of groups lattice ordered were recognized by Garrett Birkhoff. In 1971, Bruck completed a survey of binary systems. The detailed history about the quasigroups and loops is given by Hala in 1990.

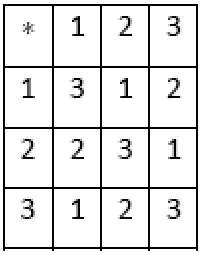
In 1930, the non-isomorphic loops up to 6 orders were established by Schönhardt [12]. Dénes and Keedwell [5] presented computations of quasigroups up to order 6, but in the statistic, count loops owed to their postulates that each quasigroup is isomorphic to a reduced square, which is noticeably incorrect for quasigroups in general. In 1985, Brant and Mullen counted loops of order 7. The number of loops of order 8 was announced in electronic forum by QSCG (2001), then Guerin independently worked on same values. Detail history of counting loops is explained by McKay et al. Now we define some basic terminologies which are helpful to understand the work which is explained in chapter 3.

1.3.1 Quasigroup

Let L be a non-void set together with a binary operation $*: (x, y) \to x * y$. Then L is called quasigroup if following axioms are satisfied.

1. The equation $x * y = z$ determine a unique element $y \in$ L for given x, z $\in$ L.
2. The equation $x * y = z$ determine a unique element $x \in$ L for given y, z $\in$ L.

Example



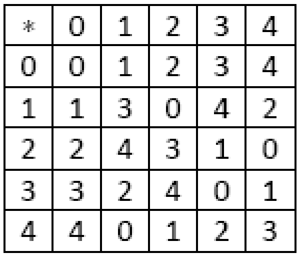
$*$	1	2	3
1	3	1	2
2	2	3	1
3	1	2	3

1.3.2 Loop

A quasigroup is said to be a loop if it has two-sided identity element e. for example

$$e * x = x * e = x \quad \text{for all } x \in L.$$

Example



$*$	0	1	2	3	4
0	0	1	2	3	4
1	1	3	0	4	2
2	2	4	3	1	0
3	3	2	4	0	1
4	4	0	1	2	3

1.3.3 Subloop

A subset H of a loop (L,$*$) is called subloop if it is itself a loop under the same binary operation.

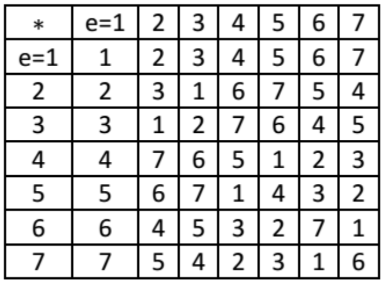
Left and Right Translation

Suppose L be loop and $a \in L$, Then a mappings $L_a: L \longrightarrow L$ and $R_a: L \longrightarrow L$ s.t $L_a(x) = ax$ and $R_a(x) = xa$ are called the left and right translation respectively.

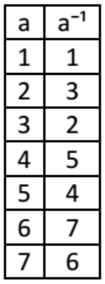
Remark

Lagrange's theorem does not hold in a loop.

Example

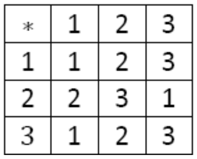


∗	e=1	2	3	4	5	6	7
e=1	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

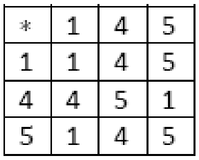


a	a^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6

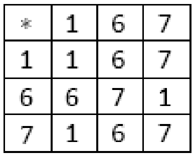
In this loop of order 7 has 3 subloops of order 3.



∗	1	2	3
1	1	2	3
2	2	3	1
3	1	2	3



∗	1	4	5
1	1	4	5
4	4	5	1
5	1	4	5



∗	1	6	7
1	1	6	7
6	6	7	1
7	1	6	7

1.3.4 Commutator:

Suppose $(L,*)$ be a loop and $x, y \in L$. Then (x, y) is called the commutator of x, y in L and is defined as,

$$xy = (yx)(x, y)$$

1.3.5 Associators:

Suppose $(L,*)$ be a loop and $x, y, z \in L$. Then (x, y, z) is called the Associator of x, y, z in L and is defined as,

$$(xy)z = \{x(yz)\}(x, y, z)$$

Commutator-Associators subloop:

Commutator-associators subloop of loop L is denoted as L' and is generated by set of all associators and commutator of loop L.So

$$L' \ = < (L, L, L), (L, L) >$$

Left Nucleus:

Left nucleus of loop L is an associative subloop of L defined as

$$\mathrm{N}_{\lambda}(L) = \{x \in L, (x, a, b) = 1, for\ all\ a, b \in L\}$$

Middle Nucleus:

Middle nucleus of loop L is an associative subloop of L defined as

$$\mathrm{N}_{\mu}(L) = \{x \in L, (a, x, b) = 1, for\ all\ a, b \in L\}$$

Right Nucleus:

Right nucleus of loop L is an associative subloop of L defined as

$$N_\rho(L)=\{x \in L, (a,b,x) = 1, for\ all\ a,b \in L\}$$

Nucleus:

Nucleus of loop L is an associative subloop of L defined as

$$N(L)= N_\lambda(L) \cap N_\mu(L) \cap N_\rho(L)$$

1.3.6 Center of loop

Center of loop is denoted by $Z(L)$ and defined as

$$Z(L)=\{x \in N(L), (a,x) = 1, for\ all\ a \in L\}$$

Normal subloop:

Let $(L,*)$ be loop and H be subloop of loop L, then H is called normal subloop if following axioms are holds.

$$Ha = aH, (Ha)b = H(ab), (aH)b = a(Hb)\ and\ b(aH) = (ba)H$$

Inverse Property Loop(IP Loop):

A loop $(L,*)$ is called inverse property loop (IP Loop) if it has unique inverse for each element of L and for all $a,b \in L$ following conditions are hold

$a^{-1} * (a * b) = b$ and $(b * a) * a^{-1} = b$

Chapter 02

S-Boxes over Galois Rings $\boldsymbol{GR(2^K,4)}$, $\mathbf{1 \leq k \leq 5}$

This chapter consist of four sections. In the first section a short history of construction of substitution boxes is describe. In the second section a brief view of Galois ring and its maximal ideal are given. In third section we present a construction of S-boxes over a maximal cyclic subgroup of Galois rings. While in last section majority logic criterion is given.

2.1 Introduction

With the global connection provided by the Internet, secure information and the techniques used to secure it, are of utmost interest in the present world. Every second of a day, millions of passwords are generated throughout the world for the sake of information. It can be seen that no matter how much we develop this study, it will not be enough. In order for it to develop faster, study and research must be encouraged across disciplines, especially in Computer Science and Mathematics.

Mathematics have many algebraic notations like Groups, Rings, Fields, Galois rings, Galois fields and G_s (maximal cyclic subgroups of groups of units of Galois rings), which if translated into programming using in disciplines like Computer Science and Information Technologies, can have remarkable impacts in the field of Cryptography. The applications of these algebraic structures are widely used in the field of coding theory. Shankar in [23] used local commutative ring $\mathbb{Z}_{p^k}$ in the construction of BCH codes, while in [4] Andrade and Palazzo used G_s in the construction of BCH codes.

Later, Shah et al [11] used G_s in construction of S-box. An S-box plays very important role in the field of cryptography. An S-box of dimension $\mathrm{n} \times \mathrm{m}$ is a mapping $\phi: \mathbb{Z}_2^{\mathrm{n}} \rightarrow \mathbb{Z}_2^{\mathrm{m}}$, where n is input bits and m is output bits. From the mapping 2^n are the number of input and 2^{m} are a number of outputs. An S-box having dimension $\mathrm{n} \times \mathrm{m}$, if $\mathrm{m} < \mathrm{n}$ means that number of input bits are large as compared to output bits. In this case, there must be some repeated entries in the S-box. However, if $m = n$, than input bits maps on unique output bits. If an S-box is one-to-one and onto, than surely inverse S-box exists. We are interested in those structures, which gives us invertible S-boxes.

S-boxes are the only nonlinear component in all cryptosystems. Many researchers are working on the construction of invertible S-boxes and many techniques have been developed so far. In this chapter, a construction technique of 4×4 S-boxes using G_s (maximal cyclic subgroups of groups of units of the Galois rings) of $\mathrm{GR}(4,4), \mathrm{GR}(8,4)$ and $\mathrm{GR}(32,4)$ is reviewed.

2.2 Galois rings and their groups of unit elements

Here we discuss some basic concepts like abelian local ring, Galois ring extension, maximal subgroup of invertible elements of a Galois ring.

Galois rings

An element x in an abelian ring with unity is said to be a unit element if there is a non-zero element y such that $x.y = e$, where e is the multiplicative identity in the ring.

If an abelian ring R has only one maximal ideal then R is called local ring. In commutative ring R, the set of non-unit elements form abelian group under addition. The rings $\mathbb{Z}_{p^m}$ are local finite rings where p is a prime and m be a positive integer.

Maximal cyclic subgroups of group of units of Galois rings

Suppose R^* and F^* be the group of units under multiplication of a ring R and field F respectively. Then R^* is commutative group under multiplication and written as the direct product of cyclic subgroups. In these cyclic subgroups, one subgroup has an order $\mathrm{p^h} - 1$. It can be written as $\mathrm{G_n}$, where $\mathrm{n} = \mathrm{p^{h-1}}$, and generated by those elements who generate the corresponding field. Therefore $\mathrm{G_n}$ is isomorphic to a finite field F^* because both are cyclic groups of same orders.

2.3 Construction of S-boxes based on Maximal Cyclic Subgroups

There are many techniques to create confusion in the data. One of them is by using an S-box. S-boxes are constructed by using different techniques, but strong S-boxes are designed by systematic calculations and mathematical formulas. There are many S-boxes are constructed by using Galois fields $GF(2^n), 1 \leq \mathrm{n} \leq 8$. In this chapter we constructed 4×4 S-boxes over the Galois rings $\mathrm{GR}(2^2, 4)$, $\mathrm{GR}(2^3, 4)$ and $\mathrm{GR}(2^5, 4)$ using maximal cyclic subgroups G_{15} in all three cases. This new designing of S-boxes have increased the convolution during encryption and decryption.

S-box construction algorithm on Galois ring $\mathbf{GR(2^m, 4)}$

Given below is the procedure, defining the S-box in 3 steps:

1. Inversion Mapping $\alpha: G_m \mathrm{U}\,\{0\} \rightarrow G_m \mathrm{U}\,\{0\}$;
2. Linear scalar multiple function $\beta : G_m \mathrm{U}\{0\} \rightarrow G_m \mathrm{U}\{0\}$;
3. Taking composition of $\alpha o \beta$ to get $(m + 1) \times (m + 1)$ S-box after applying mod 256.

The function defined above is substitution in a set $G_m \cup \{0\}$. Every element of a set is mapped into its inverse. In the other words, it is a scalar multiplication with the inverse.

We analyze and discuss the construction method for substitution box of order 4×4 in the example below. Suppose a local rings $\mathbb{Z}_4 = \{0,1,2,3\}$, $\mathbb{Z}_8 = \{0,1,2, \dots ,7\}$,$\mathbb{Z}_{16} = \{0,1,2, \dots ,15\}$ and $\mathbb{Z}_{32} = \{0,1,2, \dots ,31\}$, whereas $\mathbb{Z}_2 = \{0,1\}$, is their residue field. The basic monic, irreducible polynomial $g(x) = 1 + x + x^4$ over the rings $\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_{16}$ *and* $\mathbb{Z}_{32}$ such that $\bar{g}(x) = g(x) \bmod 2 = 1 + x + x^4$ is irreducible polynomial over $\mathbb{Z}_2$. Now take a ring extension $\mathbb{Z}_2[x] = \{c_0 + c_1x + c_2x^2 + \cdots + c_mx^m : c_i \in \mathbb{Z}_2, m \in \mathbb{Z}^+\}$ in a variable x over a binary field $\mathbb{Z}_2$. Suppose a principal ideal$< \bar{g}(x) >$ of $\mathbb{Z}_2[x]$ generated by $\bar{g}(x)$ defined as $< \bar{g}(x) >= \{p(x).\bar{g}(x): p(x) \in \mathbb{Z}_2[x]\}$. The elements of Galois field extension $F = \frac{\mathbb{Z}_2[x]}{<\bar{g}(x)>}$ of order 16 is given below in a Table 1.

Exp	*Polynomial*	
$-\infty$	0	0000
0	1	1000
1	$1 + x$	1100
2	$1 + x^2$	1010
3	$1 + x + x^2 + x^3$	1111
4	X	0100
5	$x + x^2$	0110
6	$x + x^3$	0101
7	$1 + x^2 + x^3$	1011
8	x^2	0010
9	$x^2 + x^3$	0011
10	$1 + x + x^2$	1110
11	$1 + x^3$	1001
12	x^3	0001
13	$1 + x + x^3$	1101
14	$x + x^2 + x^3$	0111

Table 1: Elements of Galois field GF (2^4)

The construction of substitution box over the Galois field extension $GF(2^4)$ is given in table 1. Table 2 show the eateries of S-box. It satisfies all the properties of a good S-box.

0	11	12	6
3	8	4	2
1	9	13	15
14	7	10	5

Table 2: S-box on GF($\mathbf{2^4}$)

S-box on Galois Rings

For the construction, S-box suppose a finite local ring $\mathbb{Z}_{2^k}$ and corresponding residue field $\mathbb{Z}_2$. Then the polynomial extension of $\mathbb{Z}_{2^k}$ in variable x is $\mathbb{Z}_{2^k}[x] = \{c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n : a_i \in \mathbb{Z}_{2^k}, n \in N\}$. Suppose $g(x) = 1 + x + x^4$ be basic irreducible polynomial of degree 4 in $\mathbb{Z}_{2^k}[x]$. Let $\mathbf{R} = \frac{\mathbb{Z}_{2^k}[x]}{<g(x)>} = \{c_0 + c_1 x + c_2 x^2 + \cdots c_{m-1} x^{m-1} : c_i \in \mathbb{Z}_{2^k}\}$ is the ring of polynomial modulo $g(x)$. It is called the Galois ring extension of $\mathbb{Z}_{2^k}$ and it is denoted by $\mathrm{GR}(2^k, m)$. It is noticed that$\mathrm{GR}(2^k, 1)$ is isomorphic to $\mathbb{Z}_{2^k}$, and $\mathrm{GR}(p, m) = \frac{\mathbb{Z}_2[x]}{<\bar{g}(x)>} = \mathbf{K}$ is isomorphic to the Galois field $\mathrm{GF}(2^4)$ an extension of $\mathbb{Z}_2$ having 2^4 elements, where $\bar{g}(x) =$ polynomial $g(x)$ which has coefficient modulo 2.

If $F^* = F\backslash\{0\}$ be a collection of all unit of a field F then it is a Group under multiplication. Now suppose R^* be a set of all unit element of a ring R. Then maximal cyclic subgroup of R^* is isomorphic to F^* of order 15 and given in Table 3. It is denoted by G_{15}.

Exp	*Polynomial*	
$-\infty$	0	0000
0	1	1000
2	$1 + 2x + x^2$	1210
4	$3x + 2x^2$	0320
6	$2 + x + 3x^3$	2103
8	x^2	0010
10	$3 + 3x + x^2 + 2x^3$	3312
12	$2 + 2x + 3x^3$	2203
14	$x + 3x^2 + x^3$	0131
16	$3 + 3x$	3300
18	$3 + x + x^2 + 3x^3$	3113
20	$x + 3x^2 + 2x^3$	0132
22	$1 + 3x^2 + x^3$	1031
24	$3x^2 + 3x^3$	0033
26	$3 + x^3$	3001
28	$1 + 3x + 2x^2 + x^3$	1321

Subgroup 1: Elements of G_{15} U {0} in GR(4,4)

Exp	*Polynomial*	
$-\infty$	0	0000
0	1	1000
2	$1 + 2x + x^2$	1210
4	$3x + 6x^2 + 4x^3$	0364
6	$2 + x + 3x^3$	2103
8	$4 + 4x + x^2 + 4x^3$	4414
10	$3 + 7x + x^2 + 2x^3$	3712
12	$6 + 6x + 3x^3$	6603
14	$x + 7x^2 + x^3$	0171
16	$7 + 7x$	7700
18	$7 + 5x + 5x^2 + 7x^3$	7557
20	$4 + x + 7x^2 + 6x^3$	4176
22	$1 + 7x^2 + 5x^3$	1075
24	$4x + 3x^2 + 3x^3$	0433
26	$7 + 5x^3$	7005
28	$5 + 7x + 2x^2 + 5x^3$	5725

Subgroup 2: Elements of G_{15} U {0} in GR(8,4)

Exp	*Polynomial*	
$-\infty$	0	0000
0	1	1000
2	$1 + 2x + x^2$	1210
4	$3x + 6x^2 + 4x^3$	0364
6	$2 + x + 8x^2 + 3x^3$	2183
8	$4 + 4x + 9x^2 + 4x^3$	4494
10	$3 + 7x + x^2 + 10x^3$	371A
12	$14 + 14x + 8x^2 + 3x^3$	EE83
14	$9x + 15x^2 + x^3$	09F1
16	$15 + 7x + 8x^3$	F708
18	$15 + 13x + 5x^2 + 15x^3$	FD5F
20	$12 + 9x + 15x^2 + 6x^3$	C9F6
22	$1 + 7x^2 + 13x^3$	107D
24	$4x + 11x^2 + 11x^3$	04BB
26	$15 + 8x + 8x^2 + 5x^3$	F885
28	$13 + 15x + 2x^2 + 13x^3$	DF2D

Subgroup 3: Elements of G_{15} U {0} in GR(16,4)

Exp	*Polynomial*	
$-\infty$	0	0000
0	1	1000
4	$3x + 6x^2 + 4x^3$	0364
8	$4 + 20x + 9x^2 + 20x^3$	4K9K
12	$30 + 14x + 8x^2 + 19x^3$	UE8J
16	$31 + 7x + 24x^3$	V70O
20	$28 + 9x + 31x^2 + 6x^3$	S9V6
24	$16 + 4x + 11x^2 + 11x^3$	G4BB
28	$13 + 15x + 18x^2 + 13x^3$	DFID
32	$17 + 2x + 17x^2 + 16x^3$	H2HG
36	$2 + 17x + 8x^2 + 3x^3$	2H83
40	$3 + 23x + x^2 + 26x^3$	3N1Q
44	$16 + 25x + 15x^2 + 17x^3$	GPFH
48	$15 + 29x + 5x^2 + 31x^3$	FT5V
52	$17 + 16x + 7x^2 + 29x^3$	HG7T
56	$31 + 8x + 24x^2 + 5x^3$	V8O5

Subgroup 4: Elements of G_{15} U {0} in GR(32,4)

Table 3: Elements of maximal cyclic subgroups of Galois Ring for *k* = 2, 3, 4, 5 with Galois Ring having orders 256, 4069, 65535 and 1048576 respectively.

In Table 4, the substitution boxes are obtained by using construction algorithm and maximal cyclic subgroups.

0	67	215	159
25	240	15	16
1	113	116	198
109	180	202	44

S-box 1: S-Box on GR(4,4)

0	3	111	123
81	224	63	100
1	193	200	10
189	195	60	152

S-box 2: S-Box on GR(8,4)

0	143	223	115
33	64	127	68
1	1	144	18
253	156	238	48

S-box 3: S-Box on GR(16,4)

0	17	34	60
96	175	81	255
1	48	237	222
31	227	144	132

S-box 4: S-Box on GR(32,4)

Table 4: S-box structures obtained from Table 3 and algorithm 3.1

In Table 4, it can be seen that after taking mod256, the S-box may contain repeating entries resulting in a non-invertible S-box. This makes its use very limited. The S-box constructed on Galois fields holds all the properties of being strong whereas, the S-box on Galois rings have some limitations.

It is not sure that the maximal cyclic subgroup of every Galois ring generates a substitution box. This means that with some polynomial and a certain Galois ring, it is not definite whether we construct a substitution box over it or not. This means that for the use of different applications, the method which is discussed in 11 is not a good technique to get substitution box even the encryption and decryption scheme as compared to a Galois field $GF(2^4)$. This means that with a compatible algorithm, then designed S-boxes can be used in different applications.

2.4 Majority Logic Criterion for the Analysis of Substitution Boxes

The statistical analysis of substitution box in application of image encryption is checked by using MLC. Disfigurement of image is created in the encryption process. The algorithm strength is checked by using these type of disfigurement. In Table 5, we arrange the MLC results which show that proposed s-box satisfy all conditions of a good s-box that are used for secure communication.

LSB Image→ MLC↓	Airplane	Baboon	Lena	Pepper
Contrast	0.2750	0.5381	0.2491	0.2944
Correlation	0.9390	0.9281	0.9778	0.9763
Energy	0.2712	0.1513	0.1689	0.1721
Homogeneity	0.9302	0.8380	0.9181	0.9222
Entropy	5.5133	5.9673	5.9698	5.9901

MLC 1: GF(2^4)

LSB Image→ MLC↓	Airplane	Baboon	Lena	Pepper
Contrast	0.2819	0.5277	0.2299	0.2921
Correlation	0.9358	0.9273	0.9789	0.9760
Energy	0.2668	0.1520	0.1722	0.1745
Homogeneity	0.926	0.8405	0.9256	0.9232
Entropy	5.4146	5.9583	5.9437	5.9923

MLC 2: GR(4,4)

LSB Image→ MLC↓	Airplane	Baboon	Lena	Pepper
Contrast	0.1876	0.5348	0.2365	0.2973
Correlation	0.9544	0.9265	0.9783	0.9756
Energy	0.3165	0.1517	0.1710	0.1733
Homogeneity	0.9449	0.8387	0.9229	0.9207
Entropy	4.7838	5.9614	5.9476	5.9870

MLC 3: GR(8,4)

LSB Image→ MLC↓	Airplane	Baboon	Lena	Pepper
Contrast	0.2835	0.5330	0.2385	0.2951
Correlation	0.9357	0.9268	0.9780	0.9758
Energy	0.2666	0.1517	0.1701	0.1738
Homogeneity	0.9257	0.8388	0.9223	0.9218
Entropy	5.4421	5.9609	5.9678	5.9935

MLC 4: GR(32,4)

Table 5: MLC of LSB's of four 512×512 images by S-box on GF(2^4), GR(4,4), GR(8,4), GR(32,4)

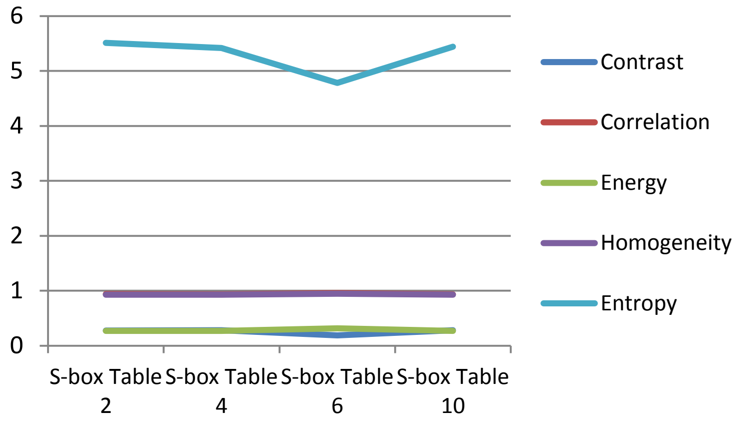


Figure 1: Comparison of the MLC result of all S-boxes on Airplane image

Figure 1 shows that with the change in the S-box, there is a change in entropy. The other behaviors do not change much and are represented by straight lines.

Conclusion

In the case when we take mod 256 for the construction of S-box, a maximum eight-degree polynomial can possibly give us a valid S-box. There is 0% chance of getting an S-box in the case of an eight-degree polynomial, whereas, all the real applications are in eight bits ($GF(2^8)$), making this method a very weak one. The histograms in Figure 3 show that, as we increase the power of 2 in our Galois ring the S-box constructed on it has more and more repeating 4 LSBs, (or in other words if we take mod 16 of our S-box) we get more repetitions causing more and more data loss in our image. This is good in some cases but it fails in many.

It also depends on the algorithm used to watermark or encrypt data using the S-boxes discussed. It can be concluded that, using the maximal cyclic subgroups, of the group of units of Galois rings, through discussed method to find S-boxes is not an efficient technique, in all the cases, due to the fact that no conditions can be scaled that allow us to know if the S-box will be generated or not. A further study is needed that will observe, for which rings will a polynomial generate an S-box.

Chapter 3

Construction Scheme of S-boxes over IP-Loop

This chapter is described as follows: Section 1, present introduction. Section 2, presents the substitution boxes and the S-boxes used in literature. In Section 3, definition and classification of inverse property loop is presented. Section 4, offers the algebraic structure of IP-Loop and proposed S-Boxes and the methods to analyze the newly developed S-boxes is presented and comparison of these S-Boxes with some of the prevalent S-boxes used in different security systems is discussed in section 5.

3.1 Introduction

With the worldwide links provided by the internet, security of information and the methods to secure it are the most dynamic themes at the moment. Every second of a day, billions of passwords are generated all over the world for the sake of information. It can be seen that no matter how much we progress in this study, it will not be sufficient. In order to develop it faster, across disciplines study and research must be encouraged, especially, crossways Computer Science and Mathematics. One of the most renowned studies in this aspect is the field of cryptography. The specialty of cryptography is to hide the information by encrypting it into an unreadable layout known as Ciphertext. It is only decrypted by the authorized people with accurate secret key. Sometimes the information is scratched by cryptanalysis mostly known as code breaking. Recently, most of the cryptographic techniques are unbreakable. In advanced cryptography, block ciphers play the main role in symmetric (private key-based) cryptosystem. In such cryptosystems, only the receiver and the sender knows the key [1]. A block cipher speaks of the bit sequences of defined length (designated as ciphertext) are transformed via complex operations into output bit sequences of exactly same length (designated as cipher text) [3].

3.2 Substitution boxes

Retrieval of the unidentified key sequence is convenient provided that the block cipher has a linear relationship between the plaintext and the cipher text. The substitution boxes (S-Boxes) is a vital component in any cryptosystem. Actually, an S-box is a change of n-binary bits into m-binary bits and generally referred as m × n S-box which is generally executed as Look-up table. If $m < n$ then there must be a repetition in the entries of S-box. Whereas for $m = n,$ there is a bijection in

S-box that is the input values mapped on unique output values and the entries of S-box are distinct [6, 16].

Normally, substation boxes are constructed over finite Galois field in advanced symmetric key cryptography. Many well-known substation boxes like AES S-box, S-8AES S-box and substitution boxes presented in [3, 4, 14, 15, 25, 27] are constructed over finite Galois field. The power of an algorithms in cryptography is determined by the nonlinear behavior of the algorithm. Hence, the designing of bijective S-boxes is need of the time for secure cryptosystem. For sound and secure communication, miscellaneous substation boxes are constructed by using different algebraic structures. Substitution boxes constructed using different algebraic structures have considered very effectual due to there distinguish cryptographic properties.

In 1997, the symmetric key encryption or decryption algorithm was first initiated by National Institute of Standard and Technology (NIST). Later in 2001, NIST appreciated the Rijndael method as the Advance Encryption Standard (AES) [3]. Since it outdated the Data Encryption Standard which has flaws of small key size and less advanced technological processing power [5]. Moreover, for the attacks on block ciphers, Rijndael S-Box algorithm was found to be more protected and effectual [1].

In cryptography, there is a lot of work on the construction of S-Boxes over the GF(2^4), GF(2^8) and also on Galois Rings. The construction method of S-Boxes over cyclic subgroup of units of Galois Rings is presented by Shah et al. (2011) [7]. In the history of cryptography, the algebraic structures have been used for the construction of S-boxes are mostly associative [1, 5-7, 11, 20]. In this work, a non-associative structure (inverse property loop) is used for the construction of S-boxes. In this chapter, an innovative idea of constructing S-boxes over inverse property (IP) loop of different orders is presented. Non-associativity and existence of inverse of zero element are the main features of proposed technique. Having these characteristics, the structure become more generalized as compared to Galois field and Galois ring. By seeing the mathematical structures for S-boxes based on Galois field and Galois ring, there is deficiency of inverse of zero. To address this problem, piecewise inversion map is used which make calculation more complex and difficult to understand. But in this work, this deficiency is overcome. The S-boxes constructed using this algebraic structure shows good properties, which shows it is useful in cryptosystem.

3.3 Inverse property loops

A loop $(L, ¤)$, where ¤ presents the binary operation is termed as inverse property loop if $\forall\, u, v \in L$ it satisfies following axioms:

i. $u¤e = u = e¤u$

ii. $u¤u^{-1} = e = u^{-1}¤u$

iii. Left inverse property existence i.e. $u^{-1}¤(u¤v) = v$

iv. Right inverse property existence i.e. $(v¤u)¤u^{-1} = v$

Remark

IP loop satisfying the following useful properties.

- $(u^{-1})^{-1} = u$
- $(uv)^{-1} = v^{-1}u^{-1}$
- $N(L)= N_{\lambda}(L) =N_{\mu}(L)= N_{\rho}(L)$

3.3.1 Weak inverse property loops

The WIPL's are firstly studied by J. M. Osborn as loops class contained inverse property loops. Let $(L, ¤)$be a loop then for three elements $u, v, w \in L$ is termed to be WIP if the following two equations are satisfied:

- $uv¤w = e$
- $u¤vw = e$

3.3.2 Non-group Smallest IP-Loop

The smallest IP-Loop which is not a group is of order 7 that is given below in Table

$*$	$e = 1$	2	3	4	5	6	7
$e = 1$	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

a	a^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6

Table 1: The smallest IP loop of order 7 with their inverses.

It is notable that the order of loop is not divisible by the order of sub-loop. This structure has proper sub-loops $\{1,2,3\}, \{1,4,5\}$ and $\{1,6,7\}$. Associativity will not hold in this structure, for example, $(2 * 2) * 4 = 3 * 4 = 7$ while$2 * (2 * 4) = 2 * 6 = 5$.This non-associativity give multiple structures as compared to associative structure like Groups, Rings, and Fields. This phenomenon rapidly increases with the increase of size. Table 2 show how much rapid increase is occurring when we move up to order 8 and onwards [8, 9].

Size	Associative Structure(Group)	Non-associative (IP Loop)	Size	Associative Structure(Group)	Non-associative (IP Loop)
1	1	1	8	5	8
2	1	1	9	2	7
3	1	1	10	2	47
4	2	2	11	1	49
5	1	1	12	5	2684
6	2	2	13	1	10342
7	1	2	14	−	−

Table 2: Number of Groups and IP Loops of given order

3.4 Designing of IP-Loop based S-boxes

In order to generate confusion in a security system, numerous procedures can be used to do so. Using an S-box is one of the most efficient technique. The S-boxes are constructed through mathematical tools, formulas and by systematic calculations. For the improvement of the worth many people have worked in this field and so far many S-boxes have been generated. The procedure of the S-box construction is given below in three steps

- Inversion function α: L → L
- linear scalar multiple function β: L → L
- β ∘ α: L → L.

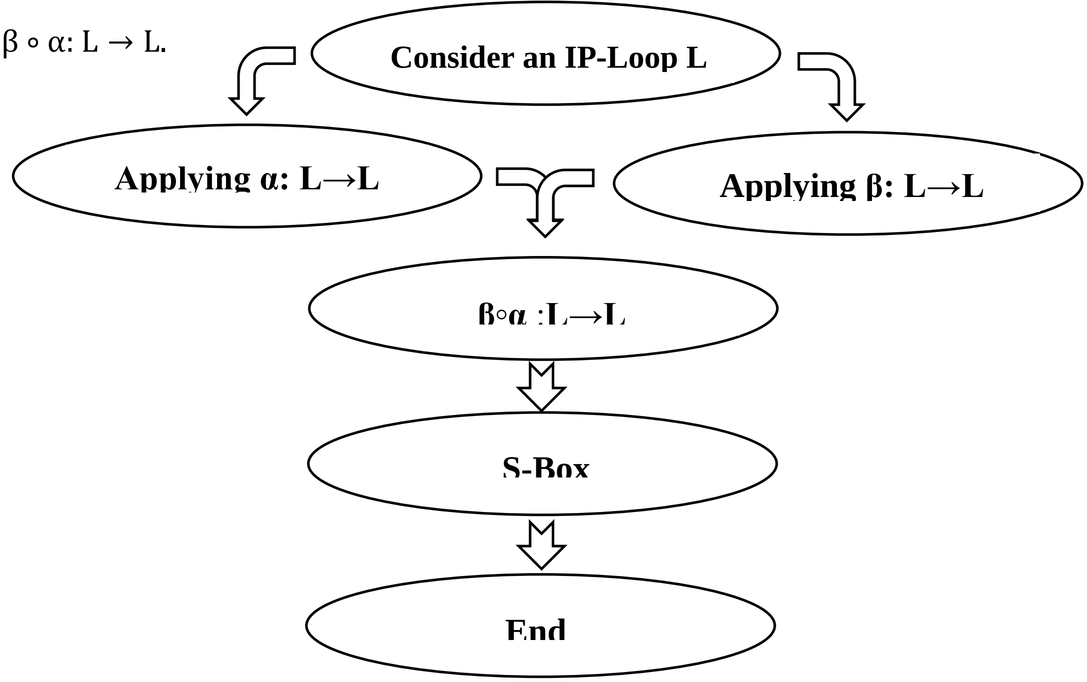


Figure 1: Diagram of proposed algorithm

In the first step, the inversion function mapped elements of the loop into their inverses. And secondly, linear scalar multiple functions is treated as a Left translation. Then taking XOR with the elements of the loop. In the third step by a composition of first two steps gives us an S-Box. By changing the elements of the loop we obtained different S-Boxes.

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	0	7	10	13	12	14	6	15	8	4	9	11	5
2	2	3	0	1	14	8	11	15	5	10	9	6	13	12	4	7
3	3	0	1	2	12	15	9	4	11	13	5	14	7	6	8	10
4	4	7	11	15	5	6	0	14	10	3	1	13	9	8	2	12
5	5	13	8	12	6	0	4	11	2	15	14	7	3	1	10	9
6	6	10	14	9	0	4	5	1	13	12	8	2	15	11	7	3
7	7	15	12	4	10	13	1	8	9	0	3	5	14	2	6	11
8	8	11	5	14	15	2	12	9	0	7	13	1	6	10	3	4
9	9	6	13	10	3	11	14	0	7	8	4	15	2	5	12	1
10	10	9	15	6	13	1	7	2	4	14	11	12	0	3	5	8
11	11	14	4	8	2	9	15	13	3	5	12	0	10	7	1	6
12	12	5	7	13	8	14	3	6	15	1	0	10	11	4	9	2
13	13	12	9	5	1	7	10	3	6	11	2	4	8	14	15	0
14	14	8	6	11	9	12	2	10	1	4	7	3	5	15	0	13
15	15	4	10	7	11	3	8	5	12	2	6	9	1	0	13	14

Table 3: IP Loop of order 16

In Table 3, IP Loop of order sixteen is given. This IP Loop is non-associative and inverse of zero is zero. The composition map is defined by the following equation.

$$\beta \circ \alpha(x) \ = 5x^{-1} \oplus 6$$

Elements of S-box are obtained through the following process. The 16 distinct values of S-box are given in Table 5.

L_{16}	$\beta \circ \alpha(x) = 5(x)^{-1} \oplus 6$	Elements of Proposed S-Box
0	$\beta \circ \alpha(0) = 5(0)^{-1} \oplus 6$	3
1	$\beta \circ \alpha(1) = 5(1)^{-1} \oplus 6$	10
.	.	.
.	.	.
.	.	.
14	$\beta \circ \alpha(14) = 5(14)^{-1} \oplus 6$	12
15	$\beta \circ \alpha(15) = 5(15)^{-1} \oplus 6$	7

Table 4: Construction of proposed S-box over L_{16}

3	10	14	11
2	6	0	9
4	13	5	1
8	15	12	7

Table 5: Proposed S-box in the form of 4 × 4 matrix

Similarly, S-Box of sixteen by sixteen is obtained by using inverse property loop of order 256 by using map.

L_{256}	$\beta \circ \alpha(x) = 5(x)^{-1} \oplus 6$	Elements of Proposed S-Box
0	$\beta \circ \alpha(0) = 5(0)^{-1} \oplus 6$	3
1	$\beta \circ \alpha(1) = 5(1)^{-1} \oplus 6$	1
.	.	.
.	.	.
.	.	.
254	$\beta \circ \alpha(254) = 5(254)^{-1} \oplus 6$	209
255	$\beta \circ \alpha(255) = 5(255)^{-1} \oplus 6$	80

Table 6: Construction of proposed S-box over L_{256}

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

Table 7: Proposed S-box in the form of 16×16 matrix

3.5 Statistical Analysis and simulation results

There is some statistical analysis which measures the strength and efficiency of S-box. These analysis includes nonlinearity, bit independence criterion, strict avalanche criterion, linear and differential approximation probability. The proposed S-box fulfill all the optimal values of different analysis. Detail of these analysis are discussed below.

3.5.1 Nonlinearity

Nonlinearity of an n-variable Boolean function $f(x)$ is the minimum distance to the set of all n-variable affine functions. It is the relationship between the nonlinearity of an n-variable Boolean $f(x)$ and the Walsh-Hadamard transform of that function is given by the following equation:

$$NL(f) = \frac{1}{2}(2^n - WHT_{max})$$

Where WHT_{max} is the maximum absolute value in the Walsh-Hadamard transform vector.

0	1	2	3
2	3	4	4

Table 8: Nonlinearity results of 4 × 4 S-box

S-Boxes	F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	Average
Proposed S-Box	104	105	105	105	102	103	102	104	103.75
[15]	104	106	106	106	110	104	100	108	105.5
[16]	106	108	110	110	108	104	100	108	106.75
AES	112	112	112	112	112	112	112	112	112
X_{yi}	104	104	108	108	108	104	104	106	105.75
Prime	94	100	104	104	102	100	98	94	99.5
Skipjack S-Box	104	104	108	108	108	104	104	106	105.5

Table 9: The results of non-linearity analysis of constituent functions of S-boxes

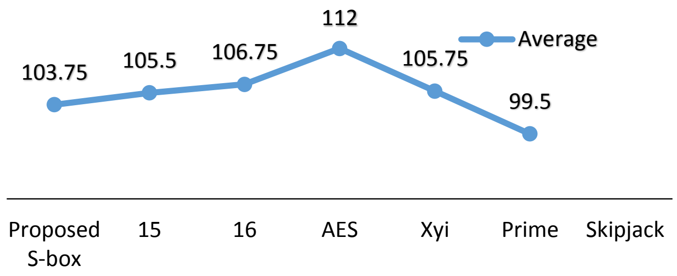


Figure 2: Graphical Representation of Non-linearity

3.5.2 Strict Avalanche Criterion

A Boolean function $f(x)$ such that for every t satisfies the expression

$$HW(t) = 1\sum_{x} f(x)f(x \oplus t) \ = 2^{n-1}$$

known as strict avalanche criterion. In other words SAC measures, how much the output bits change when a single change in input bits is made

0.507	0.539	0.507	0.445	0.492	0.492	0.507	0.515
0.492	0.523	0.523	0.476	0.476	0.460	0.507	0.531
0.539	0.429	0.523	0.460	0.507	0.523	0.445	0.515
0.554	0.476	0.523	0.492	0.539	0.507	0.492	0.515
0.539	0.492	0.523	0.523	0.492	0.476	0.507	0.515
0.523	0.460	0.507	0.523	0.523	0.539	0.523	0.531
0.523	0.523	0.523	0.523	0.539	0.507	0.507	0.515
0.523	0.507	0.507	0.492	0.507	0.429	0.507	0.500

Table 10: Strict Avalanche Criterion values of IP-Loop based S-box

S-Boxes	Average	Minimum Value	Square Deviation
Proposed S-Box	0.429	0.505	0.013
[15]	0.462	0.500	0.015
[16]	0.401	0.504	0.018
X_{yi}	0.503	0.407	0.015
Prime	0.502	0.47	0.017
Skipjack S-Box	0.499	0.464	0.018

Table 11: Comparison of SAC of IP-Loop based S-box with other S-boxes

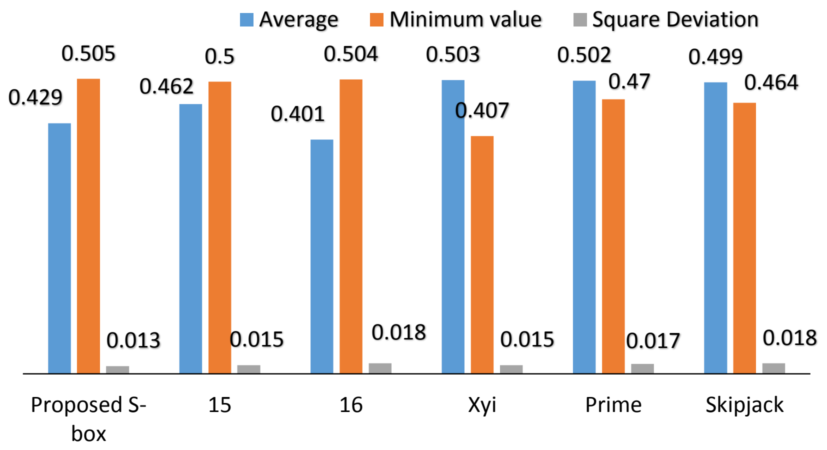


Figure 3 Graphical Representation of SAC

3.5.3 Bit Independence Criterion

Bit independence criterion (BIC) investigated about some of those the input bits which remain unchanged. The adjustment of unchanged input bits and the avalanche vectors independent performance of pairwise variables are the assets of this criterion. The non-linearity of BIC is tested, and the outcomes are given in Table 12.

-	103.000	101.000	101.000	106.000	107.000	106.000	104.000
103.000	-	106.000	106.000	107.000	106.000	105.000	105.000
101.000	106.000	-	102.000	107.000	101.000	105.000	103.000
101.000	106.000	102.000	-	103.000	108.000	103.000	101.000
106.000	107.000	107.000	103.000	-	101.000	102.000	102.000
107.000	106.000	101.000	108.000	101.000	-	101.000	103.000
106.000	105.000	105.000	103.000	102.000	101.000	-	108.000
104.000	105.000	103.000	101.000	102.000	103.000	108.000	-

Table 12: The non-linearity of BIC of IP-Loop based S-box

S-Boxes	Average	Minimum Value	Square Deviation
Proposed S-Box	103.929	101	2.052
[15]	106	102	2.138
[16]	106.27	104	1.578
X_{yi}	103.78	98	2.743
Prime	101.71	94	3.53
Skipjack S-Box	104.14	102	1.767

Table 13: Comparison of BIC results of IP-Loop based S-box with others S-boxes

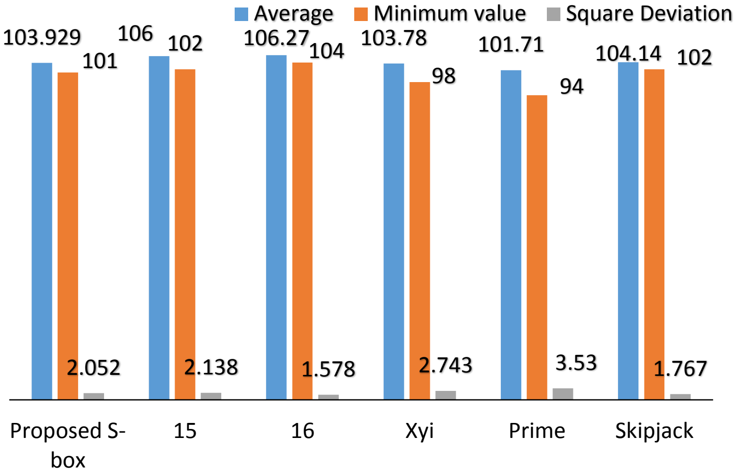


Figure 4: Graphical representation of BIC

3.5.4 Linear approximation probability

Linear approximation probability measures the imbalance of the incident. This analysis is convenient in enumerating the supreme value of the discrepancy of an event between input and output. The two masks, Γ_x and Γ_y, are applied to the parity of the input bits and output bits, respectively.

$$LP = \max_{\Gamma_x, \Gamma_y \neq 0} [\frac{\#\{x : x \cdot \Gamma_x = S(x) \cdot \Gamma_y\}}{2^n} - \frac{1}{2}]$$

Where x is all possible inputs and 2^n is a number of input element.

S-Boxes	Proposed S-Box	[15]	[16]	AES	X_{yi}	Prime	Skipjack S-Box
Max Value	159	160	161	144	168	166	156
Max LP	0.121	0.132	0.125	0.062	0.156	0.148	0.109

Table 14: LP analysis of IP-Loop based S-box with others S-boxes

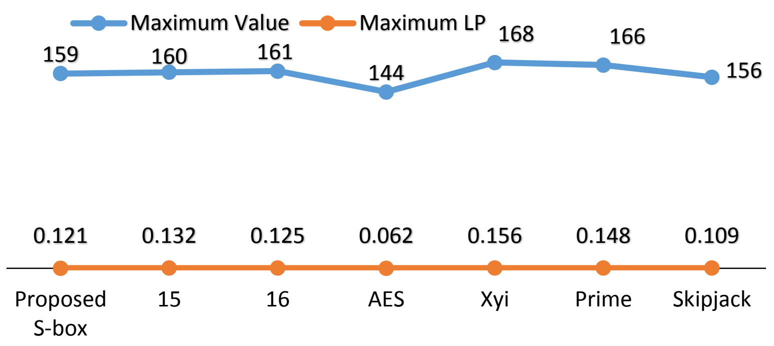


Figure 5: Graphical representation of linear approximation analysis

3.5.5 Differential approximation probability

Differential approximation probability guaranteed uniform mapping. For every differential at the input, it must uniquely map to an output differential. These features of differential approximation probability guarantee uniform mapping probability for every input bit i.

$$DP(\triangle x \rightarrow \triangle y) = [\frac{\#\{x \in X: S(x) \oplus S(x \oplus \triangle x) = \triangle y\}}{2^m}]$$

Where $\triangle x$ is the input differential and $\triangle y$ is the output differential.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0.015	0.015	0.015	0.015	0.023	0.023	0.023	0.015	0.023	0.023	0.023	0.023	0.015	0.015	0.023	0.015
0.023	0.015	0.015	0.023	0.023	0.023	0.031	0.023	0.023	0.015	0.031	0.023	0.015	0.015	0.015	0.015
0.015	0.031	0.023	0.015	0.023	0.015	0.023	0.023	0.023	0.023	0.023	0.023	0.015	0.023	0.023	0.015
0.015	0.015	0.031	0.015	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.015	0.023	0.031	0.023
0.023	0.015	0.023	0.023	0.023	0.015	0.023	0.015	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023
0.023	0.023	0.023	0.015	0.023	0.031	0.023	0.023	0.031	0.015	0.023	0.023	0.023	0.023	0.023	0.015
0.023	0.015	0.023	0.023	0.023	0.031	0.031	0.023	0.015	0.023	0.023	0.031	0.023	0.023	0.023	0.015
0.023	0.023	0.023	0.031	0.023	0.039	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.015	0.015	0.015
0.015	0.023	0.031	0.015	0.023	0.023	0.023	0.023	0.015	0.031	0.023	0.023	0.023	0.023	0.023	0.015
0.023	0.023	0.031	0.023	0.023	0.015	0.023	0.015	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023
0.015	0.023	0.023	0.023	0.015	0.031	0.023	0.023	0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.023
0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.015
0.023	0.023	0.023	0.015	0.023	0.023	0.023	0.015	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023
0.015	0.023	0.023	0.039	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023
0.015	0.023	0.015	0.023	0.015	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.015
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.015	0.015	-

Table 15: DP analysis of IP-Loop based S-box

S-Boxes	Proposed S-Box	[15]	[16]	AES	X_{yi}	Prime	Skipjack S-Box
Max DP	0.0390	0.0242	0.0267	0.0156	0.0468	0.281	0.0468

Table 16: Maximum DP of IP-Loop based S-box and comparison with other S-boxes

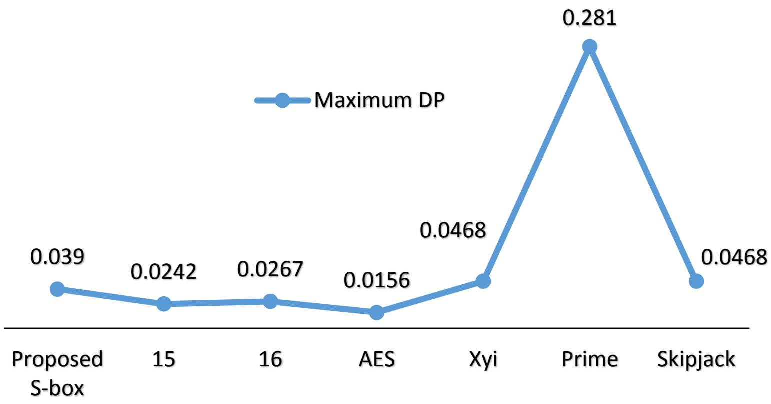


Figure 6: Graphical representation of Differential approximation analysis

Chapter 04

Applications of IP Loop based S-Boxes in watermarking and Image encryption

4.1 Introduction

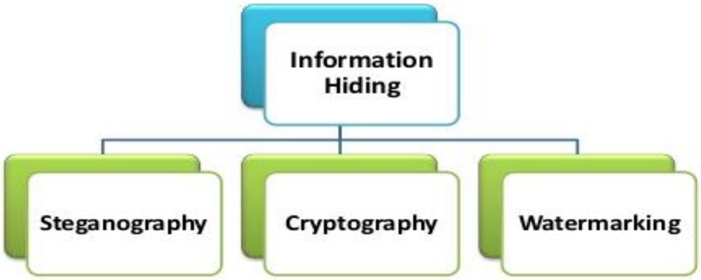
In modern era, the ways for transferring data has been changed due to the vast technology of internet and communication. Due to this vast technology, the disputes a raise for reliability and integrity of information or data. In recent epoch's, for passing data digital communication plays vital role in it. To communicate secretly a lot of internet tactics are used. So, the refuge of information against unlawful access has prime importance in this era. Hence, for the security of this data many techniques would be used to hide data. In order to hide data the most commonly used techniques are image encryption, watermarking, cryptography, and steganography.

As the exertion of S-box is generally seen in many ciphers like, DES and AES. Whereas the use of S-box in applications of encryption is broadly accomplished, a fascinating approach to digital watermarking process is presented in this chapter.

This chapter is organized as follows: In section 2, applications of watermarking have been discussed. Section 3, presents the statistical analysis of proposed S-box and Section 4, designates the methodology for the novel watermarking technique by using the application of proposed S-box. In section 5, present a majority logic certain of suggested S-boxes.

4.2 Secure information Transmission

The hiding of information means to communicate information with the help of any digital media or by hiding. Digital media includes image, an audio, a video or simply a plain text file. Information hiding is a universal term covering many sub-disciplines. The most commonly used techniques for hiding messages, information or data are Steganography, Cryptography and watermarking [23, 28, 29].



4.2.1 Steganography

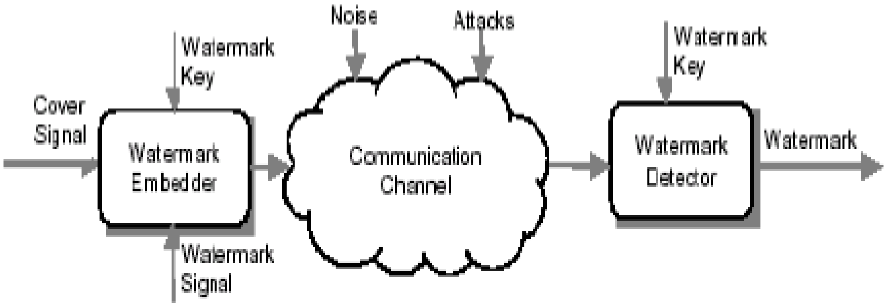
The art of converting communications is termed as steganography. By the alteration of properties of message or data, steganography embeds the message within alternative object which is referred as cover work. The output given by them is known as stegogramme.

4.2.2 Cryptography

In cryptography, with the use of encryption key the conversion of plaintext message to cipher text should be done by the sender in a similar way, the receiver decrypt the cipher text to plain text.

4.2.3 Watermarking

The technique used for insertion of information into data or image is known as digital watermarking. Later, this information could be detected by using computing operations for making allegations about data. In host data, the watermark is hidden in such a way that it's difficult to separate it from data and so it is impervious to several operations not degrading the host file. The system of digital watermarking system basically involves two types watermark embedder and a watermark detector. In watermark embedding, it embeds a watermark into the cover signal and the detector watermark detects the existence of signal of watermark. In the process of watermark detection and embedding a key known as watermark key is used which have one to one correspondence with signal of watermark. For every watermark signal, a unique key is used. The used key is private which should be known to only authorized parties and it also gives surety for the detection of watermark signal by the authorized parties.



4.3 Types of digital watermarking

The digital watermarking can be categorized into three types [28]:

- Visible watermarking
- Robust(invisible) watermarking
- Fragile(invisible) watermarking

- **Visible watermarking**

In visible watermarking a transparent coat is applied onto the image which is visible to the viewer. It is used for ownership indication protection for copyright.

- **Fragile watermarking**

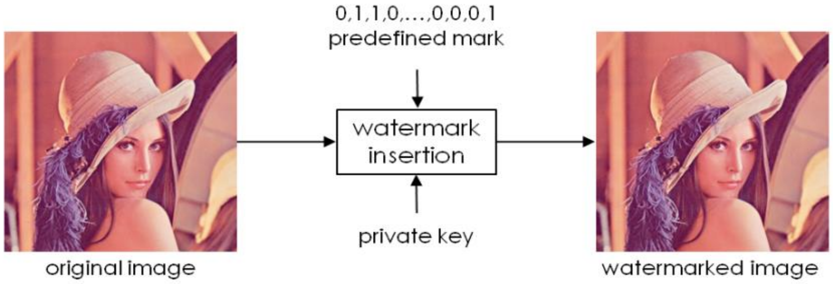
If the hidden watermark in host signal is damaged by passing through certain manipulations is known as fragile watermark.

- **Robust watermarking**

In Robust watermark information embedding into a file could not be destroyed or damaged easily. Though no mark is actually indestructible, the robustness of the system is measured by the required amount of alterations used to remove the mark which exhibits the file unworkable. Hence the mark should be hidden in that part of the file where the removal can easily be observed.

Watermark Embedding

Ofently, watermark consists of sequence of binary data which is inserted with the help of key into host signal. In this process, the embedding information routine executes bit changes in signal, resolute by the watermark and key to produce watermarked signal.

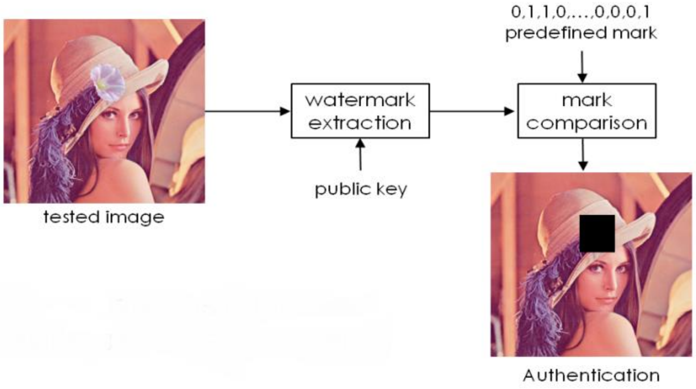


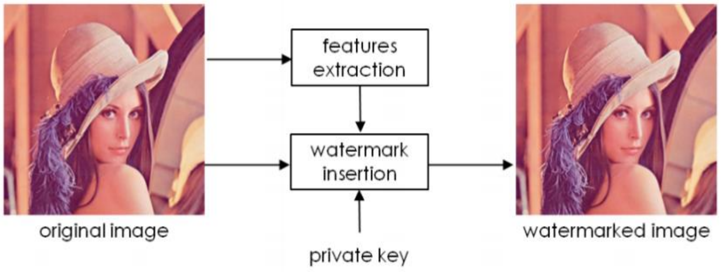
Attack

In embedding step output the signal of watermark is published or stored. In that signal, the alteration could be done, which is termed as an attack. For the removal of watermark an attack attempt should be done which alarmed the applications of copyright protection. In various forms these attacks could be done which include cropping, adding noise, rotation etc.

Watermark Extraction

Watermark extraction is a technique which attempts to extract the watermark from the attacked signal. During transmission, if the signal was unchanged then the watermark present in it should be easily extracted. In the extraction process, the inputs are watermarked image and private or public key.





4.4 Techniques of Watermarking

According to the embedding of data, the watermarking techniques are categorized into two types:

i. Spatial domain technique
ii. Transform domain technique

- **Spatial domain technique**

In spatial domain technique, the image is presented in terms of pixels. By the modification of color and intensity value for few selected pixels, this watermarking technique embeds a watermark. With the comparison to transform domain technique spatial domain watermarking technique is very simple, having a less computing time but against algebraic attacks, it is less strong. To any image, it could be easily applied. The most significant methodology of this technique is least significant bit (LSB) [29].

- **Least Significant Bit**

The easiest and simplest technique of spatial domain watermarking is LSB in which by selecting any random pixel of cover image can embed watermark in LSB's. The following are the steps used for embedding watermark in original image with the help of LSB are:

i. Conversion of RGB image into gray-scale-image
ii. Create double accuracy for image.
iii. Shifting high significant bits of watermark image to less significant bits.
iv. Making host image LSB's zero.
v. Adding (step 3) watermarked image shifting version to modified host image (step4).

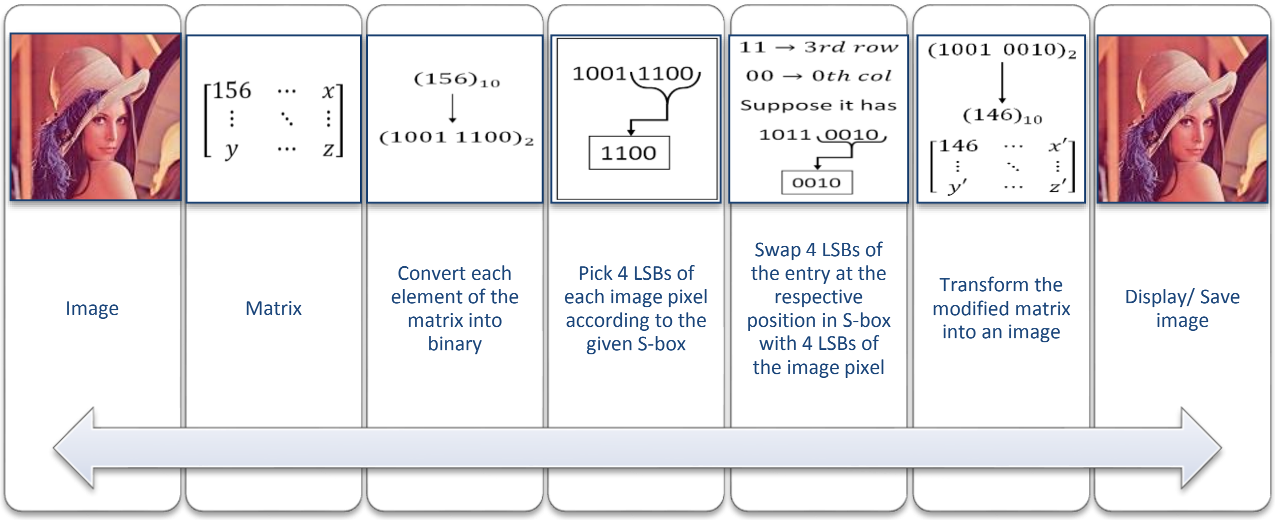
The main benefit of this method is that it could be easily performed on images. Using LSB in embedding of watermark the quality of image will not be altered.

- **Transform domain technique**

In this watermarking technique, relatively to a pixel value, the coefficients transform coefficients are modified. For the detection of the watermark, the inverse transformation is applied. The most commonly used transform techniques are DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform) etc.

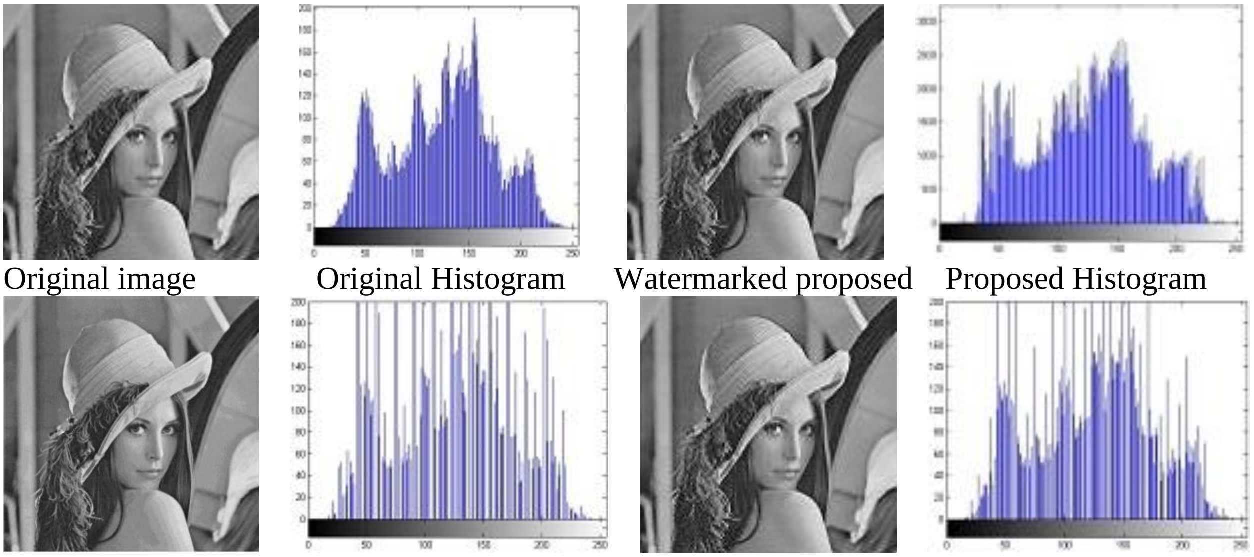
4.5 Watermarking application of proposed S-box

The detailed algorithm of suggested S-box is illustrated in Fig 11. By establishment of matrix consisting of unit pixels, the image has been processed. After this convert each element of matrix in binary form. The induced watermarking algorithm on image offered in this dissertation consists of per pixel 8 bits. In this algorithm, the S-box transformation is appealed over 4 LSB's of every image pixel. By the figure 11, it can be seen that in this process the partition of 4 LSB's in two paired LSB's should be done, the values possible range in these pairs is {0,1,2,3}. Those values help in selection of S-box column or row for the identification of substituted element. So, the image bits should be replaced with bits taken from S-box, hence it completes the nonlinear transformation. This way should be repeated for each pixel in image. Then transform the resulting matrix into image after that display and save the watermarked image.



$\begin{bmatrix} 156 & \cdots & x \\ \vdots & \ddots & \vdots \\ y & \cdots & z \end{bmatrix}$
$(156)_{10}$
$(1001\ 1100)_2$
1001 1100
1100
11 → 3rd row
00 → 0th col
Suppose it has
1011 0010
0010
$(1001\ \ 0010)_2$
$(146)_{10}$
$\begin{bmatrix} 146 & \cdots & x' \\ \vdots & \ddots & \vdots \\ y' & \cdots & z' \end{bmatrix}$
Image
Matrix
Convert each element of the matrix into binary
Pick 4 LSBs of each image pixel according to the given S-box
Swap 4 LSBs of the entry at the respective position in S-box with 4 LSBs of the image pixel
Transform the modified matrix into an image
Display/ Save image

Figure 1: Watermarking Algorithm of Suggested S-box


Original image Original Histogram Watermarked proposed Proposed Histogram

[15]Watermarked [15] Histogram [16] Watermarked [16] Histogram

Figure 2: The Original Image, Watermarked Images, and their Histograms

MLC	Entropy	Contrast	Correlation	Energy	Homogeneity
Original Image	7.4881	0.8650	0.8163	0.0948	0.8110
Proposed Watermarked	7.4682	0.8550	0.8362	0.0903	0.8230
Watermarked Image [15]	7.0014	0.7145	0.6591	0.0722	0.8152
Watermarked Image [16]	7.3244	0.8145	0.8115	0.0837	0.8112

Table 1: MLC analysis of original and watermarked image of Lena with different S-boxes

4.6 Image encryption of IP-Loop S-boxes

In [15] Shah et al. (2011) have given a majority logic criterion (MLC). MLC analysis measures the suitability of an S-box in encryption process. In MLC, statistical analysis is implemented on the plain and cipher data. MLC is very beneficial to investigate the statistical futures such as in the enciphering process manipulation of data, which yields alterations in the plain data. MLC defines a judgment criterion, which judges the outcomes of different statistical analysis such as homogeneity, energy, correlation, contrast, entropy, and the last one is mean absolute deviation.

- **Homogeneity**

The data image has a natural distortion having a relation to that image contents. The analysis of homogeneity measures the nearness of elements distribution in Grey-level co-occurrence matrix (GLCM) to GLCM diagonal. This process called as spatial gray tone dependent matrix. The further extension of this process should be done from GLCM in process entries. The mathematical form of homogeneity is as follows:

$$\text{Ƕ} = \sum_{k}\sum_{l}\frac{\text{Ƞ}(k,l)}{1+|k-l|}$$

Here k, l presents the pixels in image, and Ƞ is presentation of a number of GLCM matrices [24].

- **Energy**

For the calculation of encrypted image, energy analysis should be used. In this process GLCM is used, square elements sum in GLCM is termed as energy. The mathematical formulation of energy analysis is given as:

$$Ę = \sum_{k}\sum_{l} Ƞ^{2}|k, l|$$

For constant images, it should be 1.

- **Correlation**

In this analysis three different types are involved: horizontal, vertical and diagonal. For the partial regions analysis, the whole image includes in the process. It measures the neighbor correlation pixels with the attention of whole image texture. Its mathematical form is given as:

$$Ķ = \sum_{k,l} \frac{(k - \pi k)(l - \pi l)Ƞ(k, l)}{\rho_k \rho_l}$$

- **Contrast**

The contrast value allows the viewer to detect the hidden object in image. An amount of level contrast in image steeps the artifacts which allow identification of image clearly. When the image passes through encryption the level of randomness increased, which results in the increment of high contrast value. Due to the substitution non-linear mappings the objects present in image completely distorted. The whole reading concludes that the high level of contrast in encrypted image depicts strong encryption power. In mathematical form, contrast is defined as:

$$Ć = \sum_{k}\sum_{l}(k - l)^{2}Ƞ(k, l)$$

- **Entropy**

The measured amount of randomness can be evaluated by entropy. The high amount of randomness cause difficulty in detection of image [25]. The non-linear part of S-box increased the amount of randomness of image its mathematical representation is as follows:

$$È = \sum_{k=0}^{n} Ƞ(u_k) \log_{a} Ƞ(u_k)$$

Where $u_k$is signification of histogram calculations.

Table 2 and Table 3 shows MLC of proposed 4×4 S-Box over IP Loop is comparable with the S-Boxes constructed by Galois Field and Galois Ring. It shows that the suggested S-box satisfies all the criteria appropriate for the standard and can be used for secure communication. Table 4 shows the MLC of our proposed S-Box 16×16 over IP Loop and a comparison of results is made with others well known standard S-Boxes like AES, S_8 AES, X_{yi} and Prime is shown in Table 4. The proposed S-Box has better results than some of the standard S-Boxes, which is observed from the Table 4. Figure 2 and Figure 3 show encryption of lena image with our proposed S-Boxes and comparable with different S-Boxes and corresponding Histogram respectively.

MLC	Contrast	Correlation	Energy	Homogeneity	Entropy
MSB Image					
Plain image	0.2293	0.9502	0.1316	0.9055	7.4455
IP-Loop S-box	2.2665	0.9788	0.1632	0.9178	5.8599
S-box on $GF(2^4)$	0.2491	0.9778	0.1689	0.9181	5.9698
S-box on $GR(4,4)$	3.322085	0.087904	0.024477	0.483523	4.73018

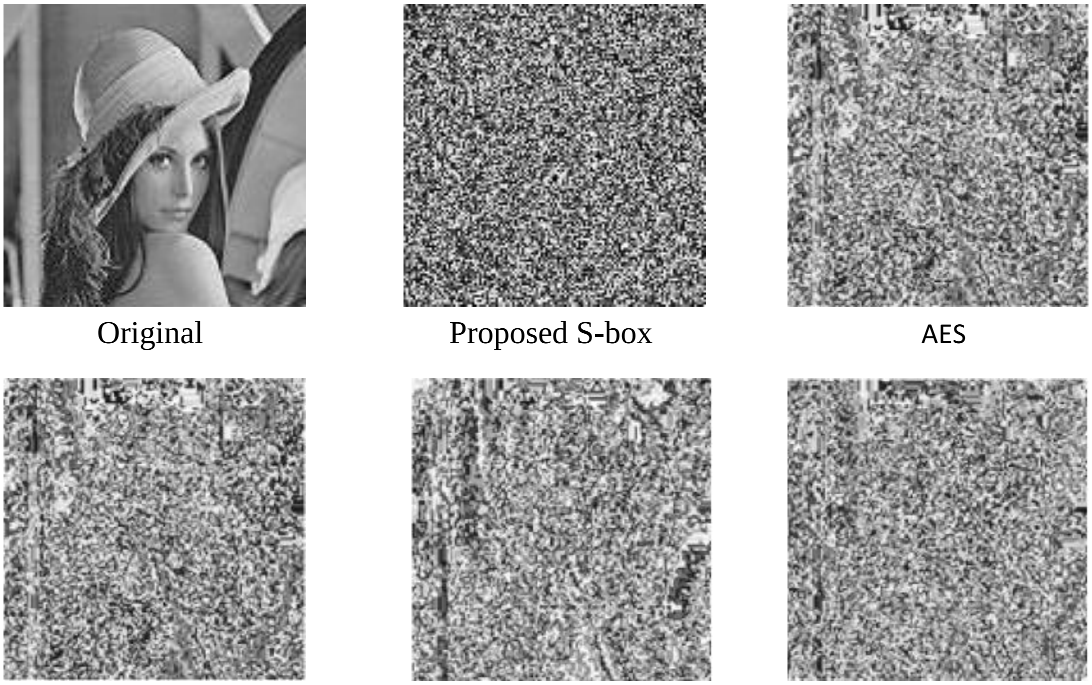
Table 2: MLC of LSB's of Lena grey 512×512 image by S-boxes over IP-loop, $GF(2^4)$ and GR(4,4)

MLC→	Contrast	Correlation	Energy	Homogeneity	Entropy
MSB Image↓					
Plain image	0.2293	0.9502	0.1316	0.9055	7.4455
IP-Loop S-box	2.5615	0.7980	0.1670	0.8230	5.8582
S-box on $GF(2^4)$	1.6909	0.8864	0.1887	0.8477	5.7457
S-box on $GR(4,4)$	2.0590	0.7962	0.3258	0.8729	5.0659

Table 3: MLC of MSB's of Lena grey 512×512 image by S-boxes over IP-loop, $GF(2^4)$ and GR(4,4)

S-Boxes	Entropy	Contrast	Correlation	Energy	Homogeneity	MAD
Proposed	7.9633	8.5969	0.0019	0.0174	0.4070	38.5638
AES	7.7301	7.3220	0.0879	0.0244	0.4835	36.3631
S_8 AES	7.7094	8.1685	0.2309	0.0227	0.4870	43.5660
Prime	7.6595	6.3683	0.0996	0.0260	0.4984	36.3082
X_{yi}	7.6850	7.0652	0.1384	0.0310	0.4928	27.4974

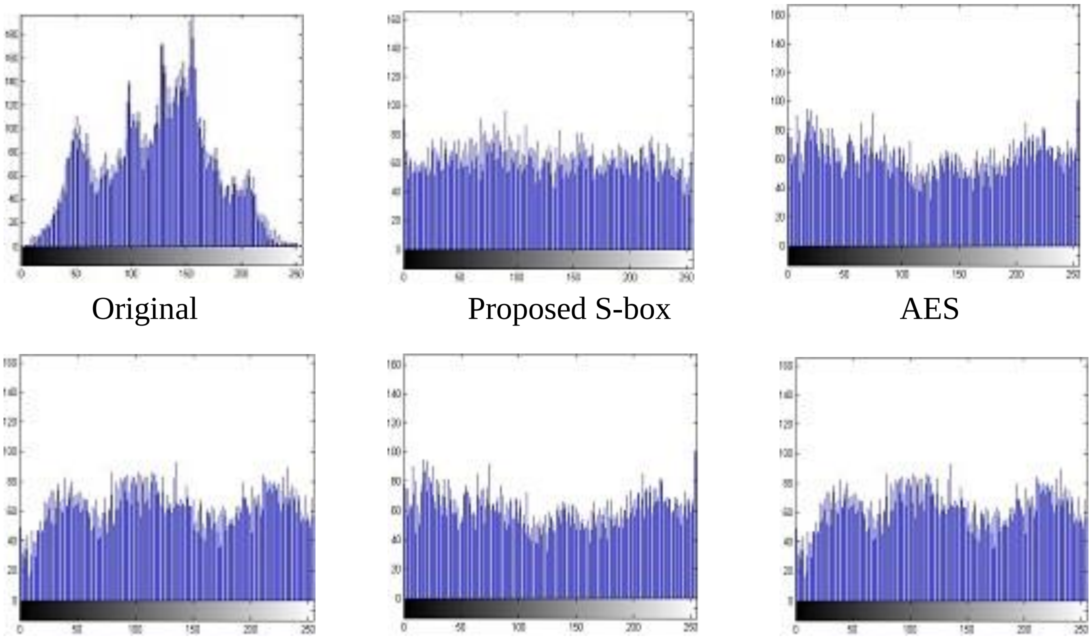
Table 4: Statistical analysis results used by MLC of 16×16 S-box



Original Proposed S-box AES

S_8 AES Prime Xyi

Figure 3: Plain image and encrypted image by using various S-Boxes



Original Proposed S-box AES

S_8AES Prime X_{yi}

Figure 4: Histogram of the corresponding images in figure 3

Chapter 05

Conclusion

In this dissertation, a novel construction of 4×4 and 16×16 S-boxes was proposed. These S-boxes were constructed by using a special type of loops (IP-Loops) of order 16 and of order 256 respectively. The possibility of getting inverse of zero element which was not possible in S-boxes over Galois Field GF (2^4) and GF (2^8) is counted as remarkable feature of proposed work. In addition to this, multiple structures of different orders are also possible due to non-associativity property of the proposed structure. In the case of 16×16 S-box over IP-Loop, it takes millions of years to find all possible IP-Loop of order 256. Security analysis of constructed S-boxes depict the high level of randomness and better security. All the standard tests such as NL, BIC, LP, DP and SAC are used for evaluation of our S-boxes. The results of these algebraic and statistical analyses tests demonstrate that proposed S-boxes are cryptographically strong S-boxes. The comparison of loop based S-boxes with different well-known S-boxes like AES, Skipjack, X_{yi} and Prime S-boxes show that our proposed S-boxes have better performance as compared to Skipjack, X_{yi} and Prime S-boxes. The quality of proposed S-boxes for image encryption techniques is evaluated with the help of MLC analyses. The proposed S-box is extremely valuable for information hiding techniques and different encryption process. In chapter 4, the improved security is observed by applying the proposed S-box in watermarking. This novel method has influential algebraic intricacy. It can also be used in different software/ hardware without any complexity.

References

[1] C. Paar, and J. Pelzl, *Understanding cryptography*, Springer, 2009.

[2] J. B. Fraleigh., A first course in abstract algebra, Pearson Education India, 2003.

[3] J. Daemen, V. Rijmen, *The design of Rijndael-AES*: the advanced encryption standard. Springer, 2002.

[4] L. Washington, W. Trappe, *Introduction to cryptography with coding theory*, Pearson Education India, 2006.

[5] I. Hussain, T. Shah, *Literature survey on nonlinear components and chaotic nonlinear components of block ciphers*, Nonlinear Dynamics, 74(4): 869-904, 2013.

[6] M. Sumathi, D. Nirmala, R. Immanuel, R. Kumar, *Study of data security algorithms using Verilog HDL*, International Journal of Electrical and Computer Engineering, 5(5): 2015.

[7] J. Cui, H. Zhong, J. Wang and R. Shi, *Generation and optimization of Rijndael S-box equation system*, Information Technology Journal, 13(15): 2482, 2014.

[8] H. O. Pflugfelder, *Historical notes on loop theory,* Commendations Mathematicae Universitatis Carolineae, 41(2): 359-370, 2000.

[9] A. Ali, J. Slaney, *Counting loops with the inverse property*, Quasigroups and related Structures, 16:13-16, 2008.

[10] Attaullah, S.S. Jamal, T. Shah, *A novel construction of substitution box using a combination of chaotic maps with improved chaotic range*, Nonlinear Dynamics, DOI 10.1007/s11071-017-3409-1

[11] T. Shah, A. Qamar, I. Hussain, *Substitution box on a maximal cyclic subgroup of units of a Galois ring*, Zeitschrift Fur Naturforschunga, 67(12): 705-710, 2012.

[12] I. Hussain, T. Shah, *Construction of cryptographically strong 8×8 S-boxes*, World Applied Sciences Journal, 13(11):2389-2395, 2011.

[13] Bruch, H. Richard, *A survey of binary systems*, Berlin: Springer, 1971.

[14] I. Hussain, T. Shah, S. K. Aslam, *Graphical SAC analysis of S_8 APA S-box*, Adv. Algebra, 3(2):57-62, 2010.

[15] S. S. Jamal, T. Shah, A. Attaullah, *A group action method for construction of strong substitution box*, 3D Res DOI 10.1007/s13319-017-0125-z, 2017.

[16] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, *A projective general linear group based algorithm for the construction of substitution box for a block cipher*, Neural Comput & Appli DOI 10.1007/s00521-012-0870-0, 2012.

[17] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoon, *Secure spread spectrum watermarking for multimedia*. Image Processing, IEEE Transactions on, 6(12): 1673-1687, 1997.

[18] M. T. Tran, D. K. Bui, A. D. Doung, *Gray S-box for advanced encryption standard*, Int Conf Comp Intel Secur, 253–256, 2008.

[19] L. Cui, Y. Cao, *A new S-box structure named affine power-affine*, Int J Innov Comput I, 3(3):45–53, 2007.

[20] K. Nyberg, *Perfect nonlinear S-boxes, in advances in cryptology*, Proc. of Eurocrypt '91, Springer-Verlag, pp.378-386, 1991.

[21] Luke O’Connor, *An analysis of a class of algorithms for S-box construction*, Journal of cryptology, 7(3):133-151, 1994.

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

[23] C. M. Adams, S. E. Tavares: *The structured design of cryptographically good S-boxes*. Journal of cryptology, 3(1):27-41, 1990.

[24] S. S. Jamal, M. U. Khan, T. Shah, *A watermarking technique with chaotic fractional s-box transformation*, Wireless pers commun, DOI 10.1007/s11277-016-03436-0.

[25] Y. Wu, J.P. Noonan, S. Agaian, *NPCR and UACI randomness tests for image encryption*, Journal of selected areas in telecommunications, April Addition, 2001.

[26] A. Altaleb, M. S. Saeed, I. Hussain, M. Aslam, *An algorithm for the construction of substitution box for block ciphers based on projective general linear group*, AIP Advances 7, 035001(2017).

[27] M. Khan, T. Shah, S. I. Batool, *A new approach for image encryption and watermarking based on substitution box over the classes of chain rings*, Multimed Tools Appl, DOI:10.1007/s11042-016-4090-y.

[28] A. F. Webster, S. E. Tavares, *On the design of S-boxes, lecture notes in Computer Science*-Springer, 218, 523-534, 1986.

[29] A. Rashid, *Digital watermarking applications and techniques*, A brief review, International Journal of Computer Applications Technology and Research 5(3) 2016 ,147-150.

[30] P. Dabas, K. Khanna, *A study on spatial and transform domain watermarking techniques*, International Journal of Computer Applications, 71(14) 2013.

Index