CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
ISLAMABAD

S-BOXES GENERATED BY CHAOTIC LOGISTIC MAP OVER A FINITE FIELD

by

Afsheen Nazar
MMT151016

A thesis submitted in partial fulfillment for the degree of Master of Philosophy

in the
Faculty of Computing
Department of Mathematics

May 2017

Declaration of Authorship

I, Afsheen Nazar, declare that this thesis titled, 'A construction Of S-Boxes Based On Chaotic Logistic Maps' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: ________________________________

Date: ________________________________

“Mathematics is not about numbers, equations, computations, or algorithms: it is about understanding”.

William Paul Thurston

CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
ISLAMABAD

Abstract

Faculty of Computing
Department of Mathematics

Master of Philosophy

by Afsheen Nazar
MMT151016

Substitution box plays an essential role in symmetric cryptographic algorithms. The most important property of S-box is non-linearity that strengthen the cryptographic security. The construction of S-boxes is to increase the confusion ability of the cipher. A number of researchers proposed different methods for the construction of S-boxes based on chaotic map. In this thesis, we construct S-boxes based on chaotic map by using the logistic map equation. The total number of S-boxes generated are $32,640$. After this, S-boxes can be analyzed by using a software tool SET.

Acknowledgements

Starting with the name of **ALLAH** the most beneficent and the most merciful whose blessings are abundant and favors are unlimited. This thesis would not have been possible without the inspiration and support of a wonderful individuals, my thanks and appreciation to all of them for being part of this journey and making this thesis possible.

First of all, I would like to express my sincere gratitude to my supervisor Dr. Rashid Ali for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. My sincere thanks also goes to Dr. Muhammad Sagheer and Dr. Shafqat Hussain for their appreciation and support.

I also feel honored to have such supporting friends. I would like to specially thank my Friend Asma Mehmood, Urwa Aftab, Asifa Ashraf, Atiya illyas, for providing me the strength to get focused toward my main objectives.

Finally, I would like to thank my family for being always with me and bringing all the care and support for my career. Specially, I am grateful to my parents, who have given all the love and care and brought me up in this stage.

Afsheen Nazar

Contents

List of Tables

Dedicated to

My Parents

without their effort and support, I would never have reached so far

Chapter 1

INTRODUCTION

1.1 Cryptography

Cryptography is the study of techniques for secure communications and data in the presence of adversaries. It is the science of secret writing which converts plaintext into ciphertext for the transmission over the public network. Plaintext is converted into ciphertext to the sender with the help of an encryption algorithm, whereas ciphertext is changed into plaintext by the receiver through the corresponding decryption algorithm. Both encryption and decryption have some special kind of information for the sender and receiver which is known as key. Cryptography uses some techniques to generate a more complex algorithm known as cryptosystem. On the basis of these complex algorithms, cryptography is divided into two main branches. Namely, the Symmetric key cryptography and the Asymmetric key cryptography.

In **Symmetric key cryptography**, same key is used for both data encryption and decryption. Sender and receiver share a common secret key for both data encryption and decryption. For example (DES) Data Encryption Standard [45] and (AES) Advanced Encryption standard[9].

In 1976 White field Diffie and Martin Hellman[17] have proposed the concept of public key cryptography or asymmetric key cryptography. This concept is based on trapdoor functions. In **Asymmetric key cryptography**, two keys are used one for encryption and the other for decryption. A person designed two keys, one key is shared publicly and the other key is kept secret. Examples are RSA [41] El.Gamal cryptosystem[38] and Elliptic curve cryptosystem[2].

1.2 Where are S-Boxes in a Cryptography?

Many Symmetric key cryptosystems are used to encrypt and decrypt one block at a time such systems are referred to as block ciphers. These are designed on the basis of Shannon's theory of confusion and diffusion [6] also implemented in a Substitution-Permutation(SP) networks. To make the encryption and decryption process efficient, the process substitution is done with the help of look-up tables. These look-up tables are known as substitution boxes (S-boxes). A typical **S-box** takes an n bits input to produce an m bits output. Infact, S-box is the only component in symmetric block ciphers that provides nonlinearity in the encryption process. The desirable properties of an S-box are its design simplicity, fast encryption and decryption speed and resistance against known cryptanalysis attacks. There are many methods for making good S-Boxes such as the construction used in blowfish [14], DES [45] , AES [9], Serpent [3], GOST [35] etc. S-box having one to one mapping are divided into three types that is straight, compressed and expansion.

A straight S-box is defined as "number of input bits is same as the number of output bits" that is $(n = m)$.
A compressed S-box is defined as " number of input bits is smaller than number of output bits" that is $(n < m)$.
A expansion S-box is defined as "number of input bits is larger than number of output bits" that is $(n > m)$.

Reasearchers and Cryptophers have proposed many approaches and methods for the construction of a strong S-box. A human made approach was introduced which have been used in DES [45] as well. Later on, mathematical based approaches were used to generate the values for S-box. For the instance, construction of S-box for AES [9] block cipher is based on a transformation and a translation. For this S-box, $m = n = 8$ and all the operation are performed in the finite Galois field $GF(2^8)$. With this S-box a byte is replaced by another byte in various rounds of the AES encryption algorithms. The hexadecimal representation of AES S-box is a 16 × 16 table given below:

63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Table 1.1: AES S-Box

Further work in this direction have been proposed by [10], [24], [29], [22], [25]. The properties of S-box are used to determined the strength of AES but the most important one is nonlinearity. High non-linearity increases the strength of S-box. S-box are constructed against linear and differential crypt-analysis attacks. To protect S-box from these attacks, S-box must satisfy high non-linearity [1], low number of fixed and opposite fixed points, high algebraic degree [32]and low differential uniformity.

1.3 Objective Of The Thesis

Strength of S-box is increased by using dynamic system instead of static system. Many methods have been proposed by researchers [40], [27], [44], [33] for a construction of dynamic S-boxes. A dynamic S-boxes are constructed by using key schedule algorithm of RC4 ,then rotate the generated S-box for each round[40]. After this, random S-box and inverse S-box are designed[27]. Later on, dynamic S-box are constructed by using chaotic maps [44], [33]. Most of the researchers believe that there is strong relationship between chaos and cryptography. A chaotic map is a map which present some kind of chaotic behavior. Their behavior may be continuous or discrete. Chaotic systems are sensitive to initial conditions and thus even with a small change in initial conditions will be able to design a very different maps from the same dynamical system. The natures of chaotic maps are deterministic, reproducible, uncorrelated and random like, which can be helpful to increase the security of transmission in communication. Different techniques have been proposed in [19], [16], [46], [37], [15] for the construction of S-boxes based on chaotic maps.

We focused our work to rewiew the article [31], chaotic binary sequence are generated by using chaotic logistic map equations defined over $GF(2^8)$. By using chaotic logistic map equations:

$$x_{i+1} = r_1(r_2 + x_i)$$

$\forall x_i, r_1, r_2 \in GF(2^8)$ and $x_0 = 0$.

We observed that the sequences of size 255 can be used to construct a chaotic S-box by adding one missing element into this sequence. In this way, for a fixed values of the initial parameter x_0, we were able to construct $32,640$ S-boxes. Varies x_0 over all the elements of $GF(2^8)$, there are $256 \times 32,640 = 8,355,840$ number of S-boxes. After this, we have randomly chosen 50 S-boxes out of $8,355,840$ S-boxes and studied their properties using the S-box Evaluation Tool (SET)**SET**.

1.4 Software Tools For S-Boxes Analysis

Some tools are available for study the properties of an S-box. A brief description of such tools is given below:

1. **Boolfun Package in *R***

   R is the free open source Mathematics software used for graphics and computing statistics. It works on various Windows, UNIX and Mac OS platforms, while the standard version of ***R*** does not support the evaluation of Boolean functions but it is possible to load a package named as **Boolfun** [18][7] which provides functionality related to the cryptographic analysis of Boolean functions.

2. **SageMath**

   SageMath library [42] is the free open source Mathematics tool which contains a module called Boolean functions and a S-Box. It allows the algebraic treatment of S-Boxes and studied the cryptographic properties of boolean function. This tool can evaluate the cryptographic properties related to linear approximation matrix and difference distribution table for S-boxes and Boolean functions.

3. **VBF**

   VBF stands for Vector Boolean Function Library. Alverez-Cubero and Zuffiria [8] presented this tool for the analysis of vector boolean functions that are used to evaluate the cryptographic properties of S-boxes.

4. **SET**

   SET stands for S-box Evaluation Tool. It is a free open source Mathematics tool which are simple and easy to use. It works in VS(visual studio). Stjepan Picek and team [43] presented this tool for the analysis of cryptographic properties of Boolean function and S-boxes.

The rest of the thesis is organized as follows

- **Chapter 2** we will present the basic concepts and definition that are needed for Boolean functions, their general properties, and how these are used for the S-boxes.

- **Chapter 3** we will present the basic concept of Chaotic maps and introduced an algorithm for the construction of S-boxes by using Logistic map equations. Using our algorithm, 50 S-boxes are choosen randomly and their properties are investigated by using the S-box Evaluation Tool (SET)[43]. In the end a brief conclusion is presented in our thesis.

Chapter 2

PRELIMINARIES

In this chapter we want to present and explain the definitions that are used in the next chapters.

2.1 Cryptography

It is the science of secret communication which changes original message into coded message or unreadable format for the transmission over the public networks in the presence of adversaries. For this purpose, we need a system or procedure for converting data or message into secret codes. Such a system is known as **Cryptosystem**. A typical cryptosystem has the following components.

1. **Plaintext**: it is the original form of data or message.
2. **Ciphertext**: it is the coded form of data or message.
3. **Encryption algorithm**: it converts plaintext into ciphertext.
4. **Decryption algorithm**: it converts ciphertext into plaintext.
5. **Key**: it is the special information used in encryption and decryption algorithms.

On the basis of design of a cryptosystem the cryptography is further divided in the following two main categories:

1. **Symmetric key cryptosystem**
2. **Asymmetric key cryptosystem**

2.1.1 Symmetric key cryptosystem

Symmetric key cryptosystem uses a same key for both data encryption and decryption. It is also known as secret key cryptosystem. Sender and receiver share a common secret key for both data encryption and decryption. For example (DES) Data Encryption Standard [45] and (AES) Advanced Encryption standard[9]. Merits of Symmetric key cryptosystem are simple to use, easier to implement and fast speed. Demerits of Symmetric key cryptosystem are key management and security issues. It may be categorized by either stream cipher or block cipher. Block cipher encrypts one block of data at a time where as stream cipher encrypts one bit or byte of data at a time.

2.1.2 Asymmetric key cryptosystem

In 1976 White field Diffie and Martin Helman [17] have proposed an idea for data encryption and decryption, known as Asymmetric key cryptosystem or public key cryptosystem. Asymmetric key cryptosystem uses two keys, one for data encryption and other for data decryption. Encryption key is shared publicly, known as Public key and the decryption key is kept secret, known as Private key. In this way data encrypted with the public key can only be decrypted by the owner of the corresponding secret key. This concept is based on trapdoor functions. Examples are RSA cryptosystem[41], El.Gamal cryptosystem [38], Elliptic curve cryptosystem [2]

Definition 2.1.1. (Block Cipher)

A symmetric key cryptosystem which encrypts or decrypts one block of data at a time is known as block cipher.

Data encryption Standard (DES)[45] is a symmetric block cipher which was published by IBM in 1970. DES uses 56 bit key to encrypt 64 bit data, having a block of 8 bytes. Due to its small key size, it was breakable through brute force within 24 hours, to overcome this drawback, $2DES$ and $3DES$ were designed. In $2DES$, 112 bit key is used for encryption. Similarly in $3DES$, 168 bit key is used for encryption. $3DES$ proved more secure as compared to others, but the drawback is that it has slow speed. In 2001 Vincent Regimen, John Daemon gave a more complicated algorithm called Rinjindael, which was named as Advanced encryption standard [9]. It is a private key symmetric block cipher. It is six times faster than $3DES$. AES use a key of 128 | 192 | 256 bits to encrypt 128 bit data, having a block of 16 bytes. Its main components is Substitution box (S-box). The purpose of such S-box is to produce non-linearity, confusion, and diffusion in the ciphertext. Since our works depends on the construction of S-boxes. The arithmetic of AES depends upon Galois field . Now we will present the brief introduction of Galois field and boolean functions.

Definition 2.1.2. (**Group**)
A set together with a binary operation " $* : G \times G \to G$ " is called a Groupiod. A Groupiod along with associative property is called a semi-group. A semi-group along with identity is called a monoid. A monoid together with inverses is called a Group. A Group along with commutative property is called an abelian group.

Definition 2.1.3. (**Ring**)
A set $(R, +, *)$ is said to be a Ring if $(R, +)$ is an abelian group. $(R\backslash\{0\}, *)$ is a semi-group. Further multiplication ' $*$ ' is distributive over addition '$+$'. Moreover, if the operation '$*$' is also commutative then $(R, +, *)$ is called a commutative ring.

Forexample: The set of real numbers R together with usual operation of addition and multiplication of real numbers is a ring.

Definition 2.1.4. (**Field**)
A set $(F, +, *)$ is said to be a Field if it holds all the properties of a Ring $(F, +, *)$ and $(F\backslash\{0\}, *)$ is an abelian group. For example $1 \in F$.

Definition 2.1.5. (**Finite Field**)

A field which contains a finite number of elements is known as a Finite Field.

2.2 Galois Field

An order of a finite feild is a power of prime q^n, known as Galois feild [26]. Its representation are $GF(q^n)$. The elements of Galois Field $GF(q^n)$ is defined as

$$\begin{aligned} GF(q^n) = & (0, 1, 2, \cdots q-1) \cup \\ & (q, q+1, q+2, \cdots q+q-1) \cup \\ & (q^2, q^2+1, \cdots q^2+q+1) \cup \cdots\cdots \cup \\ & (q^{n-1}, q^{n-1}+1, q^{n-1}+2, \cdots\cdots q^{n-1}+q-1) \end{aligned}$$

where $n \in Z^+$. The order of the field is given by q^n while q is called the characteristic of the field. The degree of polynomial of each element is at most $n-1$. From the cryptographic point of view, we are most interested in the cases:

- $GF(q), n = 1$
- $GF(2^n), q = 2$

Definition 2.2.1. (**Galois field** $GF(q)$)

A Galois field $GF(q)$ is a set of integers $Z_q = \{0, 1, 2, \cdots, q-1\}$ with arithmetic operations modulo prime q. As we know that q is prime, so $gcd(q, v) = 1$ for each $v \in Z_q$. This means that q is relatively prime to every element of Z_q.

Definition 2.2.2. (**Polynomial over** $GF(2)$)

A function which consists of variables and coefficients and also satisfy the arithmetic operation called a **polynomial**. A polynomial over $GF(2)$ [45]can be written as

$$f(x) = \sum a_i x^i, \qquad \forall i = 0, 1, \cdots, n.$$

where a_i are its coefficients, x^i are its variables, degree of polynomial is highest power of x.

2.3 Finite Field $GF(2^8)$

It is used in advanced encryption standard(AES) with $n = 8$ and $q = 2$. There are 256 different polynomials or elements in $GF(2^8)$ with degree $n < 8$ and coefficient $q < 2 = \{0, 1\}$. The polynomial representation of the elements of $GF(2^8)$ is obtained by reducing the set of all polynomials modulo an irreducible polynomial of degree 8. All the elements in it can be written in binary form with 8 bit pattern, which are given in the table below:

Decimal	Polynomial	Binary	Hexa
0	0	00000000	00
1	1	00000001	01
2	x	00000010	02
3	$x+1$	00000011	03
4	x^2	00000100	04
5	x^2+1	00000101	05
6	x^2+x	00000110	06
7	x^2+x+1	00000111	07
8	x^3	00001000	08
9	x^3+1	00001001	09
10	x^3+x	00001010	$0A$
.	.	.	.
.	.	.	.
.	.	.	.
255	$x^7+x^6+x^5+x^4+x^3+x^2+x+1$	11111111	FF

TABLE 2.1: Elements of Finite Field $GF(2^8)$

Definition 2.3.1. (**Irreducible polynomial**)
A polynomial $m(x)$ is said to be irreducible polynomial which cannot be factorized as a product of two polynomials of lesser degree. Otherwise it is known as reducible polynomial.
For example, the polynomials x^2+1, x^2+x are reducible polynomials over $GF(2)$, and x^2+x+1, x^3+x+1 are irreducible polynomials over $GF(2)$.
Polynomial multiplication in $GF(q^n)$ are performed modulo an irreducible polynomial of degree n.

Example 2.3.2. Consider an irreducible polynomial $m(x) = (x^8+x^6+x^5+x^4+1)$, consider the two polynomials (x^7+x^2+1) and $(x^6+x^4+x^2+x+1)$, and then their product mod m is:

$$\begin{aligned}
&(x^7+x^2+1)(x^6+x^4+x^2+x+1) \quad \text{mod } (x^8+x^6+x^5+x^4+1)\\
&= (x^{13}+x^{11}+x^9+x^7+x^3+x+1) \quad \text{mod } (x^8+x^6+x^5+x^4+1)\\
&= (x^5+x^4+x^3+x) \quad \text{mod } (x^8+x^6+x^5+x^4+1)
\end{aligned}$$

For two polynomials $a(u)$ and $b(u)$ we say $b(u)$ *divides* $a(u)$, mathematically $b(u)|a(u)$, if in the following equation, $r(u) = 0$

$$a(u) = q(u)b(v) + r(u)$$

There are 30 irreducible polynomials [36] of degree 8 with coefficients in $GF(2^8)$.

1. $u^8+u^7+u^6+u^5+u^2+u+1$
2. $u^8+u^7+u^6+u^5+u^4+u+1$
3. $u^8+u^7+u^6+u^5+u^4+u^2+1$
4. $u^8+u^7+u^6+u^5+u^4+u^3+1$
5. $u^8+u^7+u^6+u^4+u^2+u+1$
6. $u^8+u^7+u^6+u^4+u^3+u^2+1$
7. $u^8+u^7+u^6+u+1$
8. $u^8+u^7+u^6+u^3+u^2+u+1$
9. $u^8+u^7+u^5+u^4+u^3+u^2+1$
10. $u^8+u^7+u^5+u+1$
11. $u^8+u^7+u^4+u^3+u^2+u+1$
12. $u^8+u^7+u^5+u^3+1$
13. $u^8+u^7+u^5+u^4+1$
14. $u^8+u^7+u^3+u+1$
15. $u^8+u^7+u^3+u^2+1$
16. $u^8+u^7+u^2+u+1$
17. $u^8+u^6+u^4+u^3+u^2+u+1$
18. $u^8+u^6+u^5+u^4+u^2+u+1$
19. $u^8+u^6+u^5+u^4+u^3+u+1$
20. $u^8+u^6+u^5+u+1$
21. $u^8+u^6+u^5+u^2+1$
22. $u^8+u^6+u^5+u^3+1$
23. $u^8+u^6+u^5+u^4+1$
24. $u^8+u^6+u^3+u^2+1$
25. $u^8+u^5+u^4+u^3+u^2+u+1$
26. $u^8+u^5+u^3+u^2+1$

27. $u^8 + u^5 + u^4 + u^3 + 1$

28. $u^8 + u^5 + u^3 + u + 1$

29. $u^8 + u^4 + u^3 + u^2 + 1$

30. $u^8 + u^4 + u^3 + u + 1$

AES has a fixed mod $(m) = u^8 + u^4 + u^3 + u + 1$, which is used for multiplication and addition in $GF(2^8)$.

Definition 2.3.3. (**Primitive Polynomial**)
An irreducible polynomial $m(x)$ of degree u over $GF(q)$ is said to be a primitive polynomial, if there exists a smallest positive integer t such that $m(x)$ divides $x^t - 1$ is $t = q^u - 1$, where q is a prime number.
There are u different roots of a primitive polynomial of degree u in $GF(q^u)$, the order of all roots is $q^u - 1$. Therefore, if β is such a root, then $\beta^{q^u - 1} = 1$.

Example 2.3.4. The polynomial $m(u) = u^3 + u + 1$ is a primitive polynomial of degree 3 over $GF(2)$, where $q = 2$ and $n = 3$. If there exists a smallest positive integer $t = 7$ then $m(u) = u^3 + u + 1$ divides $u^t - 1 = u^7 + 1$. Since

$$u^7 + 1 = (u^3 + u + 1)(u^4 + u^2 + u + 1)$$

So if β is the root of $u^3 + u + 1$, then $\beta^7 = 1$. The powers of β over $GF(2^3)$ is given in the table below:

Decimal	Roots	polynomials
0	β^0	1
1	β^1	β
2	β^2	β^2
3	β^3	$\beta + 1$
4	β^4	$\beta^2 + \beta$
5	β^5	$\beta + 1 + \beta^2$
6	β^6	$\beta^2 + 1$
7	β^7	1

Table 2.2: roots of primitive polynomial in $GF(2^3)$

Thus powers of β can be used to represent all the elements of $GF(2^3)$.

There are 16 primitive polynomials of degree 8 with coefficients in $GF(2)$.

1. $u^8 + u^7 + u^6 + u^5 + u^4 + u^2 + 1$
2. $u^8 + u^7 + u^6 + u^5 + u^2 + u + 1$
3. $u^8 + u^7 + u^6 + u^3 + u^2 + u + 1$
4. $u^8 + u^7 + u^6 + u + 1$
5. $u^8 + u^7 + u^5 + u^3 + 1$
6. $u^8 + u^7 + u^3 + u^2 + 1$
7. $u^8 + u^7 + u^2 + u + 1$
8. $u^8 + u^6 + u^4 + u^3 + u^2 + u + 1$
9. $u^8 + u^6 + u^5 + u^3 + 1$
10. $u^8 + u^6 + u^5 + u^4 + 1$
11. $u^8 + u^6 + u^5 + u^2 + 1$
12. $u^8 + u^6 + u^5 + u + 1$
13. $u^8 + u^6 + u^3 + u^2 + 1$
14. $u^8 + u^5 + u^3 + u^2 + 1$
15. $u^8 + u^5 + u^3 + u + 1$
16. $u^8 + u^4 + u^3 + u^2 + 1$

Remarks: Polynomial representation of elements of $GF(2^8)$ with primitive polynomial are given in Appendix (A). Polynomials having degree less than 8 can be expressed in the form of exponential.

2.4 Boolean Function

A function $f(u) : GF(2^p) \rightarrow GF(2^q)$ is called to be Boolean function, if it has the possibility p tuples of $V = (v_1, v_2, ..., v_p)$ of $GF(2^p)$ as input and produce only output bit. The set of all p-variable boolean functions are shown by V. If $q = 1$ then it is called Binary boolean function.[4], [32].

Example 2.4.1. (**Application of Boolean Function**)
In cryptography, Boolean functions plays an important role for designing a substitution boxes. The $n\times$m *substitution box* is a function defined as $S : GF(2^n) \rightarrow GF(2^m)$ which takes n-bits as input to produce m-bits as a output. S-box can be characterized by $S(v) = (f_1(v), f_2(v), \ldots, f_m(v))$, where f_i corresponds m-variable boolean functions and boolean functions are assumed to be the components of S-Boxes.

Definition 2.4.2. (**Sequence of the function**)

Here the sequence of the form $\{(-1)^{f(\beta_0)}, (-1)^{f(\beta_1)}, \ldots, (-1)^{f(\beta_{2^n-1})}\}$ is known as **Sequence** of a boolean function f. If a sequence has a equal number of ones and minus ones then it is called a balanced sequence, otherwise unbalanced sequence.

Example 2.4.3. Consider the following boolean function with input bits v_1, v_2, v_3 and v_4.

$$f(v_1, v_2, v_3, v_4) = v_1v_2v_3 \oplus v_2v_3v_4 \oplus v_1$$

So we defined below:

i	$\beta = v_1v_2v_3v_4$	$f(\beta_i)$
0	0 0 0 0	0
1	0 0 0 1	0
2	0 0 1 0	0
3	0 0 1 1	0
4	0 1 0 0	0
5	0 1 0 1	0
6	0 1 1 0	0
7	0 1 1 1	1
8	1 0 0 0	1
9	1 0 0 1	1
10	1 0 1 0	1
11	1 0 1 1	1
12	1 1 0 0	1
13	1 1 0 1	1
14	1 1 1 0	0
15	1 1 1 1	1

TABLE 2.3: Truth table of $GF(2^4)$

So the sequence of the function f can be written as

$$\{(-1)^{f(\beta_0)}, (-1)^{f(\beta_1)}, (-1)^{f(\beta_2)}, (-1)^{f(\beta_3)}, (-1)^{f(\beta_4)}, (-1)^{f(\beta_5)}, (-1)^{f(\beta_6)}, (-1)^{f(\beta_7)}, (-1)^{f(\beta_8)}, (-1)^{f(\beta_9)}, (-1)^{f(\beta_{10})}, (-1)^{f(\beta_{11})}, (-1)^{f(\beta_{12})}, (-1)^{f(\beta_{13})}, (-1)^{f(\beta_{14})}, (-1)^{f(\beta_{15})}\}$$

$$= \{(-1)^0, (-1)^0, (-1)^0, (-1)^0, (-1)^0, (-1)^0, (-1)^0, (-1)^1, (-1)^1, (-1)^1, (-1)^1, (-1)^1, (-1)^1, (-1)^1, (-1)^0, (-1)^1\}$$

$$= \{1, 1, 1, 1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, -1\}$$

Hence the sequence of a function is balanced.

Definition 2.4.4. (**linearity**)

A **linearity** of boolean function f can be written in the form of linear combination defined as

$$L_n(f) = \sum f_i v_i = AV \quad \forall \;\; i = 1, \cdots, N$$

the linear combination of two boolean function $f(v), g(v)$ is defined as

$$(f \oplus g)v = f(v) \oplus g(v)$$

Definition 2.4.5. (**Affine function**)[23], [32]

A boolean function f which is the combination of linearity and a constant is called **Affine function**, which can be expressed as

$$f(V) = AV \oplus C$$

Where $V = v_1, v_2, \ldots, v_n$. Affine function is also called an **affine cipher**, which is a simple substitution cipher. Due to its less security it was easily breakable. This cipher performs addition and multiplication using the function;

$$f(V) = (AV \oplus C) \mod M$$

which is used for encryption.

Example 2.4.6. consider the encryption function

$$f(V) = (5V \oplus 2) \mod 26$$

suppose the plaintext message is "LEO" then

$$L = f(11) = 5 \mod 26$$

$$E = f(4) = 22 \mod 26$$

$$O = f(14) = 20 \mod 26$$

The ciphertext message is "FWU".

consider the decryption function

$$V = [f(V) - 2] * 5^{-1} \mod 26$$

$$5^{-1} = -5 \mod 26$$

$$F = -5 * [5 - 2] \mod 26 = 11 = L$$

$$W = -5 * [22 - 2] \mod 26 = 4 = E$$

$$U = -5 * [20 - 2] \mod 26 = 14 = O$$

The plaintext message is ”LEO”.

Hence affine cipher is easily decrypt.

Definition 2.4.7. (**Hamming weight and Hamming distance**)
The number of non-zero digits in a binary sequence is called hamming weight. It is denoted by $H(w)$, where $w \in GF(2^n)$

For example: $w = 111001$ then $H(111001) = 4$.

Now the hamming distance between two functions $f(v), g(v) : GF(2^n) \longrightarrow GF(2)$ is defined as:

$$d(f, g) = H(f(v) \oplus g(v))$$

Here,

$$f(v) \oplus g(v) = f(v_0) \oplus g(v_0) \oplus f(v_1) \oplus g(v_1) \oplus \ldots \oplus f(v_{2^n-1}) \oplus g(v_{2^n-1}) \text{ [23]}$$

Example 2.4.8. Consider the two Boolean functions, $f(v) = v_1v_2v_3$ and $g(v) = v_1 \oplus v_2 \oplus v_3$ with input bits v_1, v_2, v_3. Hamming distance of these boolean functions are

$$\begin{aligned} d(f, g) &= H(f(v) \oplus g(v)) \\ &= H(v_1v_2v_3 \oplus v_1 \oplus v_2 \oplus v_3) \end{aligned}$$

So we defined below:

i	$v_i = v_1v_2v_3$	$(f \oplus g)(v_i)$
0	0 0 0	0
1	0 0 1	1
2	0 1 0	1
3	0 1 1	0
4	1 0 0	1
5	1 0 1	0
6	1 1 0	0
7	1 1 1	0

Table 2.4: Truth table of $GF(2^3)$

Hence, the hamming distance of f and g is 3.

Definition 2.4.9. (**Walsh transform**)

The measurement of correlation between the boolean function f and all of the linear combinations is known as **Walsh transform**. The Walsh transform [5] of a boolean function f is defined by

$$WHT_f(\beta) = \sum(-1)^{f(v)+\beta.v} \quad \forall \;\; v \in GF(2^n)$$

Example 2.4.10. Let us consider the example of walsh transform with boolean function,

$$f(v) = v_1v_2v_3 \oplus v_1v_4 \oplus v_2$$

is given in the table below:

$v = v_1v_2v_3v_4$	$f(v)$	$(-1)^{f(v)}$	$dim3$	$dim2$	$dim1$	$dim0$
0 0 0 0	0	1	2	4	0	0
0 0 0 1	0	1	0	0	0	0
0 0 1 0	1	-1	-2	-4	8	8
0 0 1 1	1	-1	0	0	0	8
0 1 0 0	0	1	2	0	0	0
0 1 0 1	0	1	0	0	0	0
0 1 1 0	1	-1	-2	0	0	0
0 1 1 1	0	1	0	0	0	0
1 0 0 0	0	1	0	0	0	4
1 0 0 1	1	-1	2	4	4	-4
1 0 1 0	1	-1	0	0	0	4
1 0 1 1	0	1	-2	0	4	-4
1 1 0 0	0	1	0	0	0	-4
1 1 0 1	1	-1	2	0	-4	4
1 1 1 0	1	-1	0	0	0	
1 1 1 1	1	-1	2	-4	4	-4

Table 2.5: Truth table of WHT

So the Walsh transform of f is 12.

2.5 Substitution Boxes

Substitution box plays an important in the science of cryptography. Generally an S-box has $n \times m$ bits in which n-bits as a input to produce m-bits as a output using some bijective function. S-Box depends on the boolean functions. After understanding this boolean function, we will move towards the properties of S-box. A good S-box has following properties.

Definition 2.5.1. (**Balanced**)

A binary sequence is called **balanced** if there are equal number of zeros and ones in the corresponding truth table.

Example 2.5.2. We will proceed towards the comparison of balanced and unbalanced examples. Now we consider an example $f(v)$ from $GF(2^4)$.

$$f(v_1, v_2, v_3, v_4) = v_1v_2v_3 \oplus v_2v_3v_4 \oplus v_1$$

So we defined below:

i	$\beta = v_1v_2v_3v_4$	$f(\beta_i)$
0	0 0 0 0	0
1	0 0 0 1	0
2	0 0 1 0	0
3	0 0 1 1	0
4	0 1 0 0	0
5	0 1 0 1	0
6	0 1 1 0	0
7	0 1 1 1	1
8	1 0 0 0	1
9	1 0 0 1	1
10	1 0 1 0	1
11	1 0 1 1	1
12	1 1 0 0	1
13	1 1 0 1	1
14	1 1 1 0	0
15	1 1 1 1	1

TABLE 2.6: Truth table of $GF(2^4)$

The last column contains 8 zeros and 8 ones. So the sequence of f is balanced.

Definition 2.5.3. (**Non-linearity**)
The *non-linearity* [1], $NL(f)$, of a boolean function $f(v) : GF(2^n) \longrightarrow GF(2)$ is defined as the minimum hamming distance of f from any of its n-variable affine functions. Using Walsh transform, non-linearity can be shown as

$$NL(f) = \min_{g \in A} d(f, g)$$

If n is even $f(v)$ attains maximum non-linearity , that is, $2^{n-1} - 2^{\frac{n}{2}-1}$, such functions are called *bent functions.*

Definition 2.5.4. (**Correlation Immunity**)
A boolean function has a correlation immunity [30] (CI) which denotes the independence size between the linear combination of input bits and output. Its functional order can be determined by a relationship between Walsh transform and hamming weight of its inputs . A boolean function is said to be correlation immunity if its $WHT_f(\beta) = 0$, whenever $1 \leqslant H(w) \leqslant p$.

Definition 2.5.5. (**Absolute indicator and Sum of square indicator**)
The absolute indicator [30] of boolean function $h(v)$ is defined as the minimum absolute value of autocorrelation, which can be expressed as

$$\Delta_h = \max \mid \Delta_h(b) \mid \quad \text{where} \quad b \in GF(2^n)$$

The Sum of square indicator [30] of boolean function $h(v)$ also derived from autocorrelation function $\Delta_h(b)$ which can be expressed as

$$\sigma_h = \sum_{b \in GF(2^n)} \Delta_h^2(b)$$

Where, Autocorrelation (AC) of boolean function $h(v)$ is defined by

$$\Delta_h(b) = \sum (-1)^{h(v)+h(v+b)} \quad \text{where} \quad v \in GF(2^n)$$

Example 2.5.6. Let us consider the example of Absolute indicator and Sum of square indicator. The boolean function

$$h(v) = v_1v_2 + v_3$$

to compute autocorrelation at $b = 001$.

$v = v_1v_2v_3$	$h(v)$	$h(v+b)$	$(-1)^{h(v)+h(v+b)}$	*dim*2	*dim*1	*dim*0
0 0 0	0	1	1	2	4	8
0 0 1	1	0	1	2	4	0
0 1 0	0	1	1	2	0	0
0 1 1	1	0	1	2	0	0
1 0 0	0	1	1	0	0	0
1 0 1	1	0	1	0	0	0
1 1 0	1	0	1	0	0	0
1 1 1	0	1	1	0	0	0

TABLE 2.7: Truth table of *AC*

Hence the Absolute indicator of $h(v)$ is 8 and Sum of square indicator of $h(v)$ is 64.

Definition 2.5.7. (**Global Avalanche Criteria (GAC)**)
A boolean function $f(v)$ which are used for both absolute indicator and sum of square indicator is called a Global Avalanche Criteria (GAC).[1]

Definition 2.5.8. (**Algebric immunity**)
An Algebric Immunity of two boolean functions $f(v)$ and $h(v)$ is defined as the lowest degree of non-zero function h such that either

$$(f + 1)h = 0 \quad \text{or} \quad f.h = 0$$

where a function h for which $f.h = 0$ is called annihilator of f.[1]

Example 2.5.9. Consider the two boolean functions

$$f(v) = v_1 + v_1v_2 \quad \text{and} \quad h(v) = v_2$$

to compute the algebric immunity;

$v = v_1v_2$	$f(v)$	$f.h$	$(f+1)$	$(f+1)h$
0 0	0	0	1	0
0 1	0	0	1	1
1 0	1	0	0	0
1 1	0	0	1	1

Table 2.8: Truth table of AI

From the above table it shows that $f.h = 0$ and $(f+1)h = 0$.

Definition 2.5.10. (**Algebraic degree**)

An algebraic degree is related with the nonlinearity measures. An algebric degree [32] of boolean function $h(v)$ is defined as the highest degree of a function h, which can be expressed as

$$deg(h) = n - 1$$

Higher algebraic degree is considered more better than the lower algebraic degree.

Definition 2.5.11. (**DPA**)

Differential Power Analysis (DPA) is a strong cryptanalytic technique which is used to remove secret data from cryptographic device.

Definition 2.5.12. (**Transparency order**) [13]

The transparency order of S-box is small provides a high resistance against differential power analysis (DPA) attacks. If the transparency order of a S-box is high then S-box cannot achieve its resistance against differential power analysis (DPA) attacks depends on the quality of the measurements an attacker can achieve.

Definition 2.5.13. (**Fixed and Opposite fixed points**)

S-box are considered to be better without fixed and opposite fixed points as compared with those which have a fixed and opposite fixed points.

Chapter 3

CHAOTIC LOGISTIC MAP

In this chapter, the construction of S-boxes using chaotic logistic map is discussed. The properties of S-boxes using **SET** [43] are also presented. We start with a brief introduction of chaos theory and chaotic mappings.

3.1 Chaotic Map

When the smallest change in a system creates a large difference in a system behavior, then it is called chaos. This behavior is called butterfly effect. This effect was firstly demonstrated by **Edward Lorentz** in 1963 [12]. Chaotic theory deals with non-linear dynamical system that are highly sensitive to initial conditions. It also deals with the mixing property and a randomness behavior of a system such properties are confusion and diffusion. These properties make the chaotic system more reliable for constructing the cryptosystem. An application of chaos theory is to transmit data securely in the presence of third party called chaos cryptography. A map which present any kind of chaotic behavior is known as **chaotic map**. Their behavior may be discrete or continuous. Chaotic maps deals with **discrete time dynamical system** which is defined by the equation.

$$x_{i+1} = f(x_i) \tag{3.1}$$

where f maps the state x_i to the next state x_{i+1}. Starting with a initial condition x_0, repeating applications of map f give rise to the sequence of points

$$\{x_i : i = 0, 1, 2, \ldots\}$$

is called orbit of dynamical system.

Jakimoshi and Koravec [19] have proposed two well known methods to create a S-box based on chaotic maps, one is logistic and other is exponential. Logistic chaotic map consists of four step method to generate S-box. This map includes a proper choice of parameters, discretization for designing a secure cryptosystem. **Tang et al** [20] have proposed the method for designing 8 × 8 S-boxes based on $2D$ chaotic baker map and analyzed their cryptographic properties. Chaotic baker map consists of two steps to generate S-box. Afterwards, **Chen** [21] proposed the method for designing S-boxes by using $3D$ chaotic baker map. Their method was better than Tang et al method. **Ozkaynak** [16] have proposed the method for designing strong S-boxes based on chaotic map. They choose a Lorentz system for chaotic map and analyzed that system was better for secure communication. Now we can generate the S-boxes using chaotic map based on logistic map.

3.1.1 Logistic map

A mapping from initial value x at any time step to its value to the next time step is called **logistic map** which was proposed by **Robert May** in 1976. Logistic map are defined over real numbers which can be expressed as

$$x_{i+1} = rx_i(1 - x_i) \tag{3.2}$$

where r is called bifurcation parameter which is defined as "when a small smooth change occurs at the parameter values of a system causes by a qualitative change in its behavior" and $r \in (3.57, 4)$. For any initial value $x_0 \in (0, 1)$, its sequence is non-converging and non-periodic.

Example 3.1.1. Let $x_0 = \frac{1}{2}$ and $r = 3$ then by logistic map equation (3.2), we get

$$
\begin{aligned}
x_1 &= rx_0(1-x_0) = 3(0.5)(1-0.5) = 0.75\\
x_2 &= rx_1(1-x_1) = 3(0.75)(1-0.75) = 0.5625\\
x_3 &= rx_2(1-x_2) = 3(0.5625)(1-0.5625) = 0.73828125\\
x_4 &= rx_3(1-x_3) = 3(0.73828125)(1-0.73828125) = 0.5796661377
\end{aligned}
$$

similarly the process continues.
Hence the sequence $\{x_n\} = \{0.75, 0.5625, 0.73828125, 0.5796661377, \ldots\}$ is non-converging and non-periodic.

The graphical representation of (3.2) for $r = 3$ is given below:

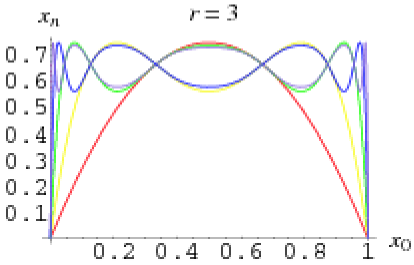

FIGURE 3.1: Logistic Map

3.1.2 Logistic map over $GF(2^8)$

Let us consider finite field $GF(2^8)$ with addition, multiplication modulo the primitive polynomial:

$$M = x^8 + x^6 + x^5 + x^4 + 1$$

over $GF(2)$. Let β be the root of $M = 0$, then $\beta^{255} + 1$ is always divisible by $\beta^8 + \beta^6 + \beta^5 + \beta^4 + 1$ s.t., $\beta^{255} = 1$ where β is the primitive polynomial whose powers $\{\beta^0, \beta^1\beta^2, \beta^3, \cdots, \cdots, \beta^{255}\}$ along with β give all the non-zero elements in

$GF(2^8)$. Logistic map equations over $GF(2^8)$ are investigated in [31] by

$$x_{i+1} = r_1 x_i (r_2 + x_i) \mod M \qquad \{i = 1, 2, 3, \ldots\} \tag{3.3}$$

$\forall x_i, r_1, r_2 \in GF(2^8) \quad \text{and} \quad x_0 \neq 0$

Fix a primitive polynomial

$$M = x^8 + x^6 + x^5 + x^4 + 1$$

and choose a random elements of x_0, r_1, r_2 in $GF(2^8)$. Examples of sequences generated from the logistic map equation (3.3) are given below for different values of the parameter x_0, r_1, and r_2.

Example 3.1.2. Let us choose
$x_0 = x, \quad r_1 = x^7, \quad \text{and} \quad r_2 = x^6 + x^5 + x^4 + 1 \quad \text{in} \quad GF(2^8)$.
Then using (3.3) we get:

$$\begin{aligned} x_1 &= r_1 x_0 (r_2 + x_0) \mod M \\ &= (x^7)(x)(x^6 + x^5 + x^4 + 1 + x) \mod M \\ &= x^{14} + x^{13} + x^{12} + x^9 + x^8 \mod M \\ &= x^4 + 1 \mod M \\ &= 00010001 \text{ (in 8-bit binary form)} \\ &= 17 \text{ (in decimal form)} \\ &= 11 \text{ (in Hexadecimal form)} \end{aligned}$$

$$\begin{aligned} x_2 &= r_1 x_1 (r_2 + x_1) \mod M \\ &= (x^7)(x^4 + 1)(x^6 + x^5 + x^4 + 1 + x^4 + 1) \mod M \\ &= x^{17} + x^{16} + x^{13} + x^{12} \mod M \\ &= x^5 + x^4 + x^3 + x^2 + x \mod M \\ &= 00111110 \text{ (in 8-bit binary form)} \\ &= 62 \text{ (in decimal form)} \\ &= 3E \text{ (in Hexadecimal form)} \end{aligned}$$

similarly, the process continues.
We get the random sequence $\{x_n\} = \{x_0, x_1, \ldots, x_{62}\}$ of 63 elements. It's decimal

representation are

$$\{2,\ 17,\ 62,\ 75,\ 199,\ 86,\ 70,\ 57,\ 151,\ 141,\ 208,\ 245,\ 162,\ 165,\ 121,\ 51,$$
$$181,\ 6,\ 157,\ 175,\ 91,\ 184,\ 248,\ 92,\ 100,\ 178,\ 218,\ 215,\ 41,\ 232,\ 35,\ 202,$$
$$168,\ 135,\ 242,\ 126,\ 239,\ 255,\ 128,\ 46,\ 52,\ 105,\ 76,\ 27,\ 28,\ 192,\ 138,\ 12,$$
$$191,\ 36,\ 22,\ 226,\ 1,\ 65,\ 229,\ 221,\ 11,\ 99,\ 110,\ 144,\ 81,\ 154,\ 115\}$$

Hence $\{x_n\}$ is the periodic sequence of 63 elements.

Example 3.1.3. Let us choose
$x_0 = x^2, \quad r_1 = x^3 + x, \quad \text{and} \quad r_2 = x^5 + x^3 \quad \text{in} \quad GF(2^8).$
Then using (3.3) we get:

$$\begin{aligned}
x_1 &= r_1 x_0 (r_2 + x_0) \mod M \\
&= (x^3 + x)(x^2)(x^5 + x^3 + x^2) \mod M \\
&= x^{10} + x^7 + x^6 + x^5 \mod M \\
&= x^6 + x^4 + x^2 + 1 \mod M \\
&= 01010101 \text{ (in 8-bit binary form)} \\
&= 85 \text{ (in decimal form)} \\
&= 55 \text{ (in Hexadecimal form)}
\end{aligned}$$

$$\begin{aligned}
x_2 &= r_1 x_1 (r_2 + x_1) \mod M \\
&= (x^3 + x)(x^6 + x^4 + x^2 + 1)(x^5 + x^3 + x^6 + x^4 + x^2 + 1) \mod M \\
&= x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^4 + x^3 + x \mod M \\
&= x^6 \mod M \\
&= 01000000 \text{ (in 8-bit binary form)} \\
&= 64 \text{ (in decimal form)} \\
&= 40 \text{ (in Hexadecimal form)}
\end{aligned}$$

similarly, the process continues.
We get the random sequence $\{x_n\} = \{x_0, x_1, \ldots, x_{31}\}$ of 32 elements. It's decimal representation are

$$\{4,\ 85,\ 64,\ 192,\ 76,\ 108,\ 149,\ 12,\ 172,\ 217,\ 96,\ 57,\ 213,\ 204,\ 224,\ 181,$$
$$245,\ 53,\ 121,\ 21,\ 128,\ 140,\ 32,\ 249,\ 153,\ 160,\ 117,\ 185,\ 89,\ 236,\ 25,\ 44\}$$

Hence $\{x_n\}$ is the periodic sequence of 32 elements.

Sequence over $GF(2^8)$ attains a maximum possible period that is 255. The periodic sequence of (3.3) having elements less than 255, so logistic map equation (3.3) cannot be used. Modified form of logistic map equation (3.3) over $GF(2^8)$ are investigated in [31] by

$$x_{i+1} = r_1(r_2 + x_i) \quad \mod M \tag{3.4}$$

$\forall x_i, r_1, r_2 \in GF(2^8)$ and $x_0 = 0$.
Fix a primitive polynomial

$$M = x^8 + x^6 + x^5 + x^4 + 1$$

and choose random elements of x_0, r_1, r_2 in $GF(2^8)$. Examples of sequences generated from the logistic map equation (3.4) are given below for different values of the parameter x_0, r_1, and r_2.

Example 3.1.4. Let us choose
$x_0 = x, \quad r_1 = x, \quad$ and $\quad r_2 = x \quad$ in $\quad GF(2^8)$.
Then using (3.4) we get:

$$\begin{aligned} x_1 &= r_1(r_2 + x_0) \quad \mod M \\ &= x(x + x) \quad \mod M \\ &= 00000000 \text{ (in 8-bit binary form)} \\ &= 0 \text{(in decimal form)} \\ &= 0 \text{ (in Hexadecimal form)} \\ x_2 &= r_1(r_2 + x_1) \quad \mod M \\ &= x(x + 0) \quad \mod M \\ &= x^2 \quad \mod M \\ &= 00000100 \text{ (in 8-bit binary form)} \\ &= 4 \text{(in decimal form)} \\ &= 4 \text{ (in Hexadecimal form)} \end{aligned}$$

similarly, the process continues.
We get a random sequence $\{x_n\} = \{x_0, x_1, \ldots, x_{254}\}$ of 255 elements. Its decimal

representation are

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

Hence $\{x_n\}$ is the periodic sequence of 255 elements.

Example 3.1.5. Let us choose

$x_0 = x, \quad r_1 = x + 1, \quad$ and $\quad r_2 = x^2 \quad$ in $\quad GF(2^8)$.

Then using (3.4) we get:

$$
\begin{aligned}
x_1 &= r_1(r_2 + x_0) \quad \bmod M\\
&= (x+1)(x^2+x) \quad \bmod M\\
&= x^3 + x \quad \bmod M\\
&= 00001010 \text{ (in 8-bit binary form)}\\
&= 10 \text{ (in decimal form)}\\
&= A \text{ (in Hexadecimal form)}\\
x_2 &= r_1(r_2 + x_1) \quad \bmod M\\
&= (x+1)(x^2+x^3+x) \quad \bmod M\\
&= x^4 + x \quad \bmod M\\
&= 00010010 \text{ (in 8-bit binary form)}\\
&= 18 \text{ (in decimal form)}
\end{aligned}
$$

$= 12$ (in Hexadecimal form)
similarly, the process continues.
We get a random sequence $\{x_n\} = \{x_0, x_1, \ldots, x_{84}\}$ of 85 elements. It's decimal representation are

$$\{2, 10, 18, 58, 66, 202, 35, 105, 183, 164, 145, 206, 47, 125, 139, 224, 93,\\ 235, 64, 204, 41, 119, 149, 194, 59, 65, 207, 44, 120, 132, 241, 110, 190, 191,\\ 188, 185, 182, 167, 148, 193, 62, 78, 222, 31, 45, 123, 129, 254, 127, 141, 234,\\ 7, 201, 38, 102, 166, 151, 196, 49, 95, 237, 74, 210, 11, 17, 63, 77, 219,\\ 16, 60, 72, 212, 1, 15, 29, 43, 113, 159, 220, 25, 39, 101, 163, 152, 213\}$$

Hence $\{x_n\}$ is the periodic sequence of 85 elements.

Above examples shows that most of the sequence of equation (3.4) are periodic having elements less than or equal to 255. We select the maximum possible periodic sequence over $GF(2^8)$ which was 255. Chaotic map have a random finite element for a periodic sequence of length 255. After this, find a missing element and then append a missing element in a periodic sequence. Now the length of a periodic sequence is 256, then S-box is generated. The initial values x_0, bifurcation parameters r_1 and r_2 are all from $GF(2^8)$ and the total number of field elements are 256 for each x_0, r_1 and r_2. Hence the total number of possible input combinations is $256 \times 256 \times 256 = 16,777,216$. For the random selection of x_0, r_1 and r_2 over $GF(2^8)$, maximum possible periodic sequence for the input combination of x_0, r_1 and r_2 are 255. For all x_0, r_1 and r_2 over $GF(2^8)$, maximum possible periodic sequence for the input combination of x_0, r_1 and r_2 are $32,640$.
We have implemented the following algorithm in the computer algebra system ApCoCoA [28] for creating all the possible S-Boxes for a given initial choice for x_0 and a fixed irreducible polynomial M of degree 8 with coefficients from $GF(2^8)$.

Algorithm 3.1.6. (DLMSbox(x_0, M))

Input: A random element $x_0 \in GF(2^8)$

Output: Set of all possible S-Boxes of size 256.

Initialize an empty array *Sbox*.

```
1. For each element $r_1 \in GF(2^8)$ Do
2.     For each element $r_2 \in GF(2^8)$ Do
3.         Create a sequence $\{x_n\}$ as follows:

                   $x_{i+1} = r_1(r_2 + x_i).$

4.         If the size of the resulting sequence is 255, then
               Append the missing element $GF(2^8) \setminus \{x_n\}$ in $\{x_n\}$.
5.             Append $\{x_n\}$ in the array Sbox.
6.         End If;
7.     End Foreach;
8. End Foreach
9. Return Sbox.
```

Illustration: Fix an irreducible polynomial

$$M = x^8 + x^6 + x^5 + x^4 + 1$$

and choose random elements of x_0, r_1, r_2 over $GF(2^8)$. We now illustrate Algorithm (3.1.6) by the following examples:

Example 3.1.7. Let us choose

$x_0 = x, \quad r_1 = x^6 + x^5 + x^3, \quad \text{and} \quad r_2 = x^7 + x^6 + x^4 \quad \text{in} \quad GF(2^8).$

Then using (3.4) we get:

$$\begin{aligned} x_1 &= r_1(r_2 + x_0) \mod M \\ &= (x^6 + x^5 + x^3)(x^7 + x^6 + x^4 + x) \mod M \\ &= x^{13} + x^{11} + x^6 + x^4 \mod M \\ &= x^5 + x^2 + x + 1 \mod M \\ &= 00100111 \text{ (in 8-bit binary form)} \\ &= 39 \text{ (in decimal form)} \\ &= 27 \text{ (in Hexadecimal form)} \end{aligned}$$

$$\begin{aligned}
x_2 &= r_1(r_2 + x_1) \mod M \\
&= (x^6 + x^5 + x^3)(x^7 + x^6 + x^4 + x^5 + x^2 + x + 1) \mod M \\
&= x^{13} + x^{10} + x^7 + x^4 + x^3 \mod M \\
&= x^6 + 1 \mod M \\
&= 01000001 \text{ (in 8-bit binary form)} \\
&= 65 \text{ (in decimal form)} \\
&= 41 \text{ (in Hexadecimal form)}
\end{aligned}$$

We get a random sequence $\{x_n\} = \{x_0, x_1, \ldots, x_{254}\}$ of 255 elements. It's decimal representation are

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

Now the missing element is $GF(2^8) \setminus \{x_n\} = 173$.

So, appending 173 into resulting sequence $\{x_n\}$, we get the following S-box containing 256 elements in decimal form:

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

Table 3.1: S-Box 1

Example 3.1.8. Let us choose

$x_0 = x, \quad r_1 = x^7 + x^4 + x^3 + x^2 + x, \quad$ and $\quad r_2 = x^6 + x^3 + x^2 + 1 \quad$ in $\quad GF(2^8)$.

Then using (3.4) we get:

$$\begin{aligned} x_1 = r_1(r_2 + x_0) &\mod M \\ &= (x^7 + x^4 + x^3 + x^2 + x)(x^6 + x^3 + x^2 + 1) \mod M \\ &= x^{13} + x^7 + x^5 + x^3 + x \mod M \\ &= x^7 + x^6 + x^2 + x \mod M \\ &= 11000110 \text{ (in 8-bit binary form)} \\ &= 198 \text{ (in decimal form)} \\ &= C6 \text{ (in Hexadecimal form)} \end{aligned}$$

$$\begin{aligned} x_2 = r_1(r_2 + x_1) &\mod M \\ &= (x^7 + x^4 + x^3 + x^2 + x)(x^6 + x^3 + x^2 + 1 + x^7 + x^6 + x^2 + x) \mod M \\ &= x^{14} + x^{11} + x^9 + x^6 + x^4 + x \mod M \\ &= x^6 + x^5 + x^4 + x + 1 \mod M \\ &= 01110011 \text{ (in 8-bit binary form)} \\ &= 115 \text{ (in decimal form)} \\ &= 73 \text{ (in Hexadecimal form)} \end{aligned}$$

similarly, the process continues.

We get a random sequence $\{x_n\} = \{x_0, x_1, \ldots, x_{50}\}$ of 51 elements. It's decimal

representation are

$$\begin{array}{lllllllllll}
\{2, & 198, & 115, & 125, & 239, & 205, & 229, & 197, & 160, & 11, & 29, \\
64, & 65, & 223, & 34, & 163, & 216, & 107, & 178, & 204, & 123, & 56, \\
33, & 112, & 174, & 153, & 63, & 104, & 97, & 186, & 137, & 181, & 133, \\
106, & 44, & 49, & 250, & 67, & 146, & 169, & 208, & 46, & 124, & 113, \\
48, & 100, & 190, & 19, & 210, & 99, & 247\} & & & &
\end{array}$$

Hence $\{x_n\}$ is the periodic sequence of 51 elements. We cannot generate S-box from this sequence of 51 elements.

Example 3.1.9. Let us choose
$x_0 = x, \quad r_1 = x^2, \quad$ and $\quad r_2 = x^3 \quad$ in $\quad GF(2^8)$.
Then using (3.4) we get:

$$\begin{aligned}
x_1 &= r_1(r_2 + x_0) \quad \text{mod } M \\
&= (x^2)(x^3 + x) \quad \text{mod } M \\
&= x^5 + x^3 \quad \text{mod } M \\
&= 00101000 \text{ (in 8-bit binary form)} \\
&= 40 \text{ (in decimal form)} \\
&= 28 \text{ (in Hexadecimal form)} \\
x_2 &= r_1(r_2 + x_1) \quad \text{mod } M \\
&= (x^2)(x^3 + x^5 + x^3) \quad \text{mod } M \\
&= x^7 \quad \text{mod } M \\
&= 10000000 \text{ (in 8-bit binary form)} \\
&= 128 \text{ (in decimal form)} \\
&= 80 \text{ (in Hexadecimal form)}
\end{aligned}$$

similarly, the process continues.

We get a random sequence $\{x_n\} = \{x_0, x_1, \ldots, x_{254}\}$ of 255 elements. It's decimal

representation are

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

Now the missing element is $GF(2^8) \setminus \{x_n\} = 69$.

So, appending 69 into resulting sequence $\{x_n\}$, we get the following S-box containing 256 elements in decimal form:

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

Table 3.2: S-Box 2

For a fixed $x_0 = x$ and varying r_1, r_2 over all elements in $GF(2^8)$, Algorithm (3.1.6) generated $32,640$ different S-boxes. That is out of $256 \times 256 = 65,536$ possibilities, only $32,640$ sequences having length 255 and hence can be used to create corresponding S-boxes. Since x_0 can be chosen in 256 different ways, there are a total of $256 \times 32,640 = 8,355,840$ possible S-boxes that can be generated from logistic map equation (3.4) for a fixed irreducible polynomial M. Further, there are 30 irreducible polynomial of degree 8. Continuing in this way, the possible number of chaotic S-boxes that can be generated from (3.4) and with all possible irreducible polynomial is $30 \times 256 \times 32,640 = 250,675,200$. Many software tools are available for the analysis of S-boxes but we have used the software tool **SET** [43].

3.2 Analysis of S-boxes using SET

Boolean function and S-boxes plays an important role for non-linear elements in stream and block cipher. Non-linear elements and their properties are important for security. In case of boolean function, text file are defined in form of truth table. In case of S-boxes text file are defined in decimal or hexadecimal format. Performance is more important when some one is interested in calculating the properties of AES s-box or someone is using a program as a script go through a number of s-boxes. All small functions which are frequently used are inclined and it helps to improve the execution speed of the tool. Every function is computed which help the researchers when they are examining the tool or adding new functionality. An extensive documentation containing information about all function and instruction about their use is a part of secure code package to comfort the user.

S-Box Evaluation Tool (**SET**) [43] is a tool used for the analysis of non-linear elements and their properties. For this, we firstly install the Microsoft visual studio, then create a text file. After this, we compile and run the program which give us the properties of S-Boxes. Its properties like non-linearity [1], correlation immunity [30], absolute indicator [30], sum of the square indicator [30], algebraic degree

[32], algebraic immunity [1], transparency order [13] are discussed in **Chapter** (2). Although, some properties are not being used frequently but yet we consider them important because they make us able to collect as much data on S-boxes or boolean function as possible. Now we give some examples for the construction of S-boxes and analyzed their properties.

3.2.1 AES S-box

We start with AES S-box given in Table (1.1). Its decimal representation is given in the following table:

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

TABLE 3.3: AES S-box b

Now using S-box Evaluation Tool SET [43], we observe the following output for the properties of AES S-box.

- S-Box is balanced.
- Non-linearity (NL_f) is 112.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 44.
- Sum of Square Indicator (σ_h) is 148720.
- Algebraic Degree (deg_h) is 8.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.859.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 0.

3.2.2 S-box generated by logistic map equation

From now on, we fix a irreducible polynomial M of degree 8 over $GF(2)$:

$$M = x^8 + x^6 + x^5 + x^4 + 1$$

Now using Logistic map equation (3.4), the resulting S-boxes are $32,640$ and varying x_0 over $GF(2^8)$. We have randomly selected 50 chaotic S-boxes from $32,640$ S-boxes. Of these 50 S-boxes, 18 S-boxes together with the value of x_0 and the corresponding outputs from SET [43] are given below:

Example 3.2.1. Let us choose

1. $x_0 = x^2$

   using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

TABLE 3.4: S-Box 3

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 100.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 72.
- Sum Of Square Indicator (σ_h) is 214912.

- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.816.
- Number of Fixed Points (F_p) is 1.
- Number of Opposite Fixed Points (OF_p) is 1.

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

Table 3.5: S-Box 4

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum Of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.818.
- Number Of Fixed Points (F_p) is 0.
- Number Of Opposite Fixed Points (OF_p) is 0.

2. $x_0 = M - x^8$

   using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

Table 3.6: S-Box 5

the corresponding output is:

- S-Box is balanced.
- Non-Linearity $(NL_f)$is 96.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 96.
- Sum of Square Indicator (σ_h) is 260608.
- Algebraic Degree $(deg_h)$is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.820.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 1.

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

Table 3.7: S-Box 6

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree is (deg_h) 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.819.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 0.

3. $x_0 = x + 1$

using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

TABLE 3.8: S-Box 7

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.

- Transparency Order (T_G) is 7.829.
- Number of Fixed Points (F_p) is 1.
- Number of Opposite Fixed Points (OF_p) is 3.

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

Table 3.9: S-Box 8

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 92.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 247168.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.826.
- Number of Fixed Points (F_p) is 1.
- Number of Opposite Fixed Points (OF_p) is 0.

4. $x_0 = x^7$

   using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

Table 3.10: S-Box 9

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 96.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 96.
- Sum of Square Indicator (σ_h) is 260608.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.820.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 2.

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

Table 3.11: S-Box 10

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.830.
- Number of Fixed Points (F_p) is 2.
- Number of Opposite Fixed Points (OF_p) is 0.

5. $x_0 = x^3 + x^2 + 1$

   using (3.4), total number of S-boxes generated are $32,640$. we choose some S-boxes from $32,640$ S-Boxes and check its properties.

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

Table 3.12: S-Box 11

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.

- Transparency Order (T_G) is 7.816.
- Number of Fixed Points (F_p) is 1.
- Number of Opposite Fixed Points (OF_p) is 1.

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

TABLE 3.13: S-Box 12

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 96.
- Correlation Immunity (CI) is 0.
- Absolute Indicator $(\Delta_h)$is 96.
- Sum of Square Indicator (σ_h) is 260608.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.829.
- Number of Fixed Points (F_p) is 3.
- Number of Opposite Fixed Points (OF_p) is 2.

6. $x_0 = x^5 + x^4$

   using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

Table 3.14: S-Box 13

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 100.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 72.
- Sum of Square Indicator (σ_h) is 206080.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.824.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 0.

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

Table 3.15: S-Box 14

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.812.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 1.

7. $x_0 = x$

using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

TABLE 3.16: S-Box 15

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 100.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 88.
- Sum of Square Indicator (σ_h) is 214528.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.

- Transparency Order (T_G) is 7.782.
- Number of Fixed Points (F_p) is 1.
- Number of Opposite Fixed Points (OF_p) is 1.

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

Table 3.17: S-Box 16

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.830.
- Number of Fixed Points (F_p) is 1.
- Number of Opposite Fixed Points (OF_p) is 2..

8. $x_0 = 1$

   using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

Table 3.18: S-Box 17

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 100.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 88.
- Sum of Square Indicator (σ_h) is 214528.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.770.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 0.

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

Table 3.19: S-Box 18

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.829.
- Number of Fixed Points (F_p) is 1.
- Number of Opposite Fixed Points (OF_p) is 0.

Similarly if we fix another irreducible polynomial M of degree 8 over $GF(2)$:

$$M = x^8 + x^5 + x^3 + x + 1$$

Now using Logistic map equation (3.4), the resulting S-boxes are $32,640$ and varying x_0 over $GF(2^8)$,

Example 3.2.2. Let us choose $x_0 = x$
using (3.4), total number of S-boxes generated are $32,640$. Select some S-boxes from $32,640$ and check their properties.

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

TABLE 3.20: S-Box 19

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 102.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 80.
- Sum of Square Indicator (σ_h) is 217600.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.831.
- Number of Fixed Points (F_p) is 0.
- Number of Opposite Fixed Points (OF_p) is 3.

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

TABLE 3.21: S-Box 20

the corresponding output is:

- S-Box is balanced.
- Non-Linearity (NL_f) is 96.
- Correlation Immunity (CI) is 0.
- Absolute Indicator (Δ_h) is 96.
- Sum of Square Indicator (σ_h) is 212608.
- Algebraic Degree (deg_h) is 7.
- Algebraic Immunity (AI) is 4.
- Transparency Order (T_G) is 7.812.
- Number of Fixed Points (F_p) is 4.
- Number of Opposite Fixed Points (OF_p) is 1.

Above examples shows that if we fix a irreducible polynomial M investigated in [31], then the total number of S-boxes generated are $32,640$. Similarly if we fix a remaining 29 irreducible polynomial then the total number of S-boxes generated are $32,640$.

3.2.3 Comparison of different S-boxes

For all $r_1, r_2, x_0 \in GF(2^8)$ then we can generate $256 \times 32,640 = 8,355,840$ S-boxes. The analysis and comparison of 50 random S-boxes from $8,355,840$ S-boxes are given below in the table:

NL_f	$C.I$	$\triangle_h$	σ_h	deg_h	AI	T_G	F_p	OF_p
100	0	88	214528	7	4	7.760	1	1
100	0	88	214528	7	4	7.763	1	3
100	0	88	214528	7	4	7.759	1	0
100	0	88	214528	7	4	7.786	0	1
92	0	80	247168	7	4	7.812	2	4
100	0	88	214528	7	4	7.786	1	1
100	0	88	214528	7	4	7.791	2	1
96	0	96	260608	7	4	7.827	1	0
100	0	80	216448	7	4	7.826	1	1
100	0	80	216448	7	4	7.839	0	2
100	0	88	214912	7	4	7.846	1	0
100	0	88	214528	7	4	7.755	0	0
102	0	80	217600	7	4	7.825	1	0
96	0	96	260608	7	4	7.823	0	1
100	0	88	214528	7	4	7.758	3	0
100	0	88	214912	7	4	7.835	1	0
96	0	96	260608	7	4	7.819	0	1
100	0	80	216448	7	4	7.832	1	0
100	0	88	214528	7	4	7.772	3	1

NL_f	$C.I$	$\triangle_h$	σ_h	deg_h	AI	T_G	F_p	OF_p
96	0	96	260608	7	4	7.837	2	3
100	0	88	214912	7	4	7.830	0	1
96	0	96	260608	7	4	7.820	0	1
96	0	96	212608	7	4	7.821	1	1
100	0	88	214528	7	4	7.782	1	1
102	0	80	217600	7	4	7.832	0	0
96	0	96	212608	7	4	7.830	1	1
100	0	88	214528	7	4	7.768	2	2
96	0	96	260608	7	4	7.820	2	2
92	0	80	247168	7	4	7.827	2	2
96	0	96	212608	7	4	7.828	1	1
102	0	80	217600	7	4	7.819	0	0
100	0	88	214912	7	4	7.809	0	1
100	0	72	214912	7	4	7.817	0	0
102	0	80	217600	7	4	7.825	1	0
100	0	88	214912	7	4	7.805	1	1
100	0	80	216448	7	4	7.819	0	2
100	0	88	214528	7	4	7.754	1	1
100	0	88	216528	7	4	7.790	0	0
102	0	80	217600	7	4	7.830	0	0
96	0	96	212608	7	4	7.824	0	0
96	0	96	212608	7	4	7.833	0	0
100	0	88	214912	7	4	7.825	1	1
96	0	96	260608	7	4	7.813	0	0
96	0	96	212608	7	4	7.830	0	3
100	0	88	214528	7	4	7.782	0	1
92	0	80	247168	7	4	7.815	2	1
96	0	96	260608	7	4	7.832	3	2
100	0	72	206080	7	4	7.814	1	3
100	0	88	214528	7	4	7.758	0	0
100	0	88	214528	7	4	7.768	1	2

From the above table ,we analyzed that all of the S-boxes are balanced. Highest non-linearity of these S-Boxes is 102. Low number of fixed and opposite fixed point is 0. Algebraic degree is 7 which remains same for all S-boxes, Algebraic immunity is 4 which remains same for all S-boxes. Correlation immunity is 0.

3.2.4 Conclusion and Future work

In this thesis, we have proposed an algorithm for the generation of S-boxes using logistic map equations (3.4) defined over $GF(2^8)$. Such logistic maps over the finite field $GF(2^8)$ can be used to generate a random sequence of size 255. We observed that by adding a missing element in this sequence, we can generate an AES-like chaotic S-box of size 256. Our proposed Algorithm (3.1.6) can be used to generate $30 \times 256 \times 32,640 = 250,675,200$ chaotic S-boxes. Finally, properties of 50 randomly choosen S-box are studied and analyzed using S-box evaluation tool (SET). These S-boxes passes all of the cryptographic properties which are important criterion for strong chaotic S-boxes to produce more confusion to the encryption process. To conclude our work, it is worth mentioning that we have obtained results that lead to the robustness and efficiency of an S-box. These chaotic S-boxes can also be used the encryption of digital images.

Appendix A

Field Elements $GF(2^8)$

A.1 Finite Field Elements over Irreducible Primitive Polynomial

Consider another primitive polynomial $m(x) = x^8 + x^6 + x^3 + x^2 + 1$ and β be the root of $m(x) = 0$. Then all the polynomials of degree less than 8 can uniquely be expressed as some power of β. Since $(+)$ and $(-)$ operations are same in $GF(2^8)$, so

$$x^8 + x^6 + x^3 + x^2 + 1 = 0$$
$$x^8 = x^6 + x^3 + x^2 + 1 \mod m(x)$$

S. No	Decimal	polynomial	Binary	Exponential
0	0	0	00000000	0
1	1	1	00000001	1
2	2	x	00000010	β
3	4	x^2	00000100	β^2
4	8	x^3	00001000	β^3
5	16	x^4	00010000	β^4
6	32	x^5	00100000	β^5
7	64	x^6	01000000	β^6
8	128	x^7	10000000	β^7
9	77	$x^6 + x^3 + x^2 + 1$	01001101	β^8
10	154	$x^7 + x^4 + x^3 + x$	10011010	β^9
11	121	$x^6 + x^5 + x^4 + x^3 + 1$	01111001	β^{10}
12	242	$x^7 + x^6 + x^5 + x^4 + x$	11110010	β^{11}
13	169	$x^7 + x^5 + x^3 + 1$	10101001	β^{12}
14	31	$x^4 + x^3 + x^2 + x + 1$	00011111	β^{13}
15	62	$x^5 + x^4 + x^3 + x^2 + x$	00111110	β^{14}
16	124	$x^6 + x^5 + x^4 + x^3 + x^2$	01111100	β^{15}
17	248	$x^7 + x^6 + x^5 + x^4 + x^3$	11111000	β^{16}
18	189	$x^7 + x^5 + x^4 + x^3 + x^2 + 1$	10111101	β^{17}
19	55	$x^5 + x^4 + x^2 + x + 1$	00110111	β^{18}
20	110	$x^6 + x^5 + x^3 + x^2 + x$	01101110	β^{19}
21	220	$x^7 + x^6 + x^4 + x^3 + x^2$	11011100	β^{20}
22	245	$x^7 + x^6 + x^5 + x^4 + x^2 + 1$	11110101	β^{21}
23	167	$x^7 + x^5 + x^2 + x + 1$	10100111	β^{22}
24	3	$x + 1$	00000011	β^{23}
25	6	$x^2 + x$	00000110	β^{24}
26	12	$x^3 + x^2$	00001100	β^{25}
27	24	$x^4 + x^3$	00011000	β^{26}
28	48	$x^5 + x^4$	00110000	β^{27}
29	96	$x^6 + x^5$	01100000	β^{28}
30	192	$x^7 + x^6$	11000000	β^{29}

S. No	Decimal	polynomial	Binary	Exponential
31	205	$x^7 + x^6 + x^3 + x^2 + 1$	11001101	β^{30}
32	215	$x^7 + x^6 + x^4 + x^2 + x + 1$	11010111	β^{31}
33	227	$x^7 + x^6 + x^5 + x + 1$	11100011	β^{31}
34	139	$x^7 + x^3 + x + 1$	10001011	β^{32}
35	91	$x^6 + x^4 + x^3 + x + 1$	01011011	β^{33}
36	182	$x^7 + x^5 + x^4 + x^2 + x$	10110110	β^{34}
37	33	$x^5 + 1$	00100001	β^{35}
38	66	$x^6 + x$	01000010	β^{36}
39	132	$x^7 + x^2$	10000100	β^{37}
40	69	$x^6 + x^2 + 1$	01000101	β^{38}
41	138	$x^7 + x^3 + x$	10001010	β^{39}
42	89	$x^6 + x^4 + x^3 + 1$	01011001	β^{40}
43	178	$x^7 + x^5 + x^4 + x$	10110010	β^{41}
44	41	$x^5 + x^3 + 1$	00101001	β^{42}
45	82	$x^6 + x^4 + x$	01010010	β^{43}
46	164	$x^7 + x^5 + x^2$	10100100	β^{44}
47	5	$x^2 + 1$	00000101	β^{45}
48	10	$x^3 + x$	00001010	β^{46}
49	20	$x^4 + x^2$	00010100	β^{47}
50	40	$x^5 + x^3$	00101000	β^{48}
51	80	$x^6 + x^4$	01010000	β^{49}
52	160	$x^7 + x^5$	10100000	β^{50}
53	13	$x^3 + x^2 + 1$	00001101	β^{52}
54	26	$x^4 + x^3 + x$	00011010	β^{53}
55	52	$x^5 + x^4 + x^2$	00110100	β^{54}
56	104	$x^6 + x^5 + x^3$	01101000	β^{55}
57	208	$x^7 + x^6 + x^4$	11010000	β^{56}
58	237	$x^7 + x^6 + x^5 + x^3 + x^2 + 1$	11101101	β^{57}
59	151	$x^7 + x^4 + x^2 + x + 1$	10010111	β^{58}
60	99	$x^6 + x^5 + x + 1$	01100011	β^{59}

S. No	Decimal	polynomial	Binary	Exponential
61	198	$x^7 + x^6 + x^2 + x$	11000110	β^{60}
62	193	$x^7 + x^6 + 1$	11000001	β^{61}
63	207	$x^7 + x^6 + x^3 + x^2 + x + 1$	11001111	β^{62}
64	211	$x^7 + x^6 + x^4 + x + 1$	11010011	β^{63}
65	235	$x^7 + x^6 + x^5 + x^3 + x + 1$	11101011	β^{64}
66	155	$x^7 + x^4 + x^3 + x + 1$	10011011	β^{65}
67	123	$x^6 + x^5 + x^4 + x^3 + x + 1$	01111011	β^{66}
68	246	$x^7 + x^6 + x^5 + x^4 + x^2 + x$	11110110	β^{67}
69	161	$x^7 + x^5 + 1$	10100001	β^{68}
70	15	$x^3 + x^2 + x + 1$	00001111	β^{69}
71	30	$x^4 + x^3 + x^2 + x$	00011110	β^{70}
72	60	$x^5 + x^4 + x^3 + x^2$	00111100	β^{71}
73	120	$x^6 + x^5 + x^4 + x^3$	01111000	β^{72}
74	240	$x^7 + x^6 + x^5 + x^4$	11110000	β^{73}
75	173	$x^7 + x^5 + x^3 + x^2 + 1$	10101101	β^{74}
76	23	$x^4 + x^2 + x + 1$	00010111	β^{75}
77	46	$x^5 + x^3 + x^2 + x$	00101110	β^{76}
78	92	$x^6 + x^4 + x^3 + x^2$	01011100	β^{77}
79	184	$x^7 + x^5 + x^4 + x^3$	10111000	β^{78}
80	61	$x^5 + x^4 + x^3 + x^2 + 1$	00111101	β^{79}
81	122	$x^6 + x^5 + x^4 + x^3 + x$	01111010	β^{80}
82	244	$x^7 + x^6 + x^5 + x^4 + x^2$	11110100	β^{81}
83	165	$x^7 + x^5 + x^2 + 1$	10100101	β^{82}
84	7	$x^2 + x + 1$	00000111	β^{83}
85	14	$x^3 + x^2 + x$	00001110	β^{84}
86	28	$x^4 + x^3 + x^2$	00011100	β^{85}
87	56	$x^5 + x^4 + x^3$	00111000	β^{86}
88	112	$x^6 + x^5 + x^4$	01110000	β^{87}
89	224	$x^7 + x^6 + x^5$	11100000	β^{88}
90	141	$x^7 + x^3 + x^2 + 1$	10001101	β^{89}

S. No	Decimal	polynomial	Binary	Exponential
91	87	$x^6+x^4+x^2+x+1$	01010111	β^{90}
92	174	$x^7+x^5+x^3+x^2+x$	10101110	β^{91}
93	17	x^4+1	00010001	β^{92}
94	34	x^5+x	00100010	β^{93}
95	68	x^6+x^2	01000100	β^{94}
96	136	x^7+x^3	10001000	β^{95}
97	93	$x^6+x^4+x^3+x^2+1$	01011101	β^{96}
98	186	$x^7+x^5+x^4+x^3+x$	10111010	β^{97}
99	57	$x^5+x^4+x^3+1$	00111001	β^{98}
100	114	$x^6+x^5+x^4+x$	01110010	β^{99}
101	228	$x^7+x^6+x^5+x^2$	11100100	β^{100}
102	133	x^7+x^2+1	10000101	β^{101}
103	71	x^6+x^2+x+1	01000111	β^{102}
104	142	$x^7+x^3+x^2+x$	10001110	β^{103}
105	81	x^6+x^4+1	01010001	β^{104}
106	162	x^7+x^5+x	10100010	β^{105}
107	9	x^3+1	00001001	β^{106}
108	18	x^4+x	00010010	β^{107}
109	36	x^5+x^2	00100100	β^{108}
110	72	x^6+x^3	01001000	β^{109}
111	144	x^7+x^4	10010000	β^{110}
112	109	$x^6+x^5+x^3+x^2+1$	01101101	β^{111}
113	218	$x^7+x^6+x^4+x^3+x$	11011010	β^{112}
114	249	$x^7+x^6+x^5+x^4+x^3+1$	11111001	β^{113}
115	191	$x^7+x^5+x^4+x^3+x^2+x+1$	10111111	β^{114}
116	51	x^5+x^4+x+1	00110011	β^{115}
117	102	$x^6+x^5+x^2+x$	01100110	β^{116}
118	204	$x^7+x^6+x^3+x^2$	11001100	β^{117}
119	213	$x^7+x^6+x^4+x^2+1$	11010101	β^{118}
120	231	$x^7+x^6+x^5+x^2+x+1$	11100111	β^{119}

S. No	Decimal	polynomial	Binary	Exponential
121	131	x^7+x+1	10000011	β^{120}
122	75	x^6+x^3+x+1	01001011	β^{121}
123	150	$x^7+x^4+x^2+x$	10010110	β^{122}
124	97	x^6+x^5+1	01100001	β^{123}
125	194	x^7+x^6+x	11000010	β^{124}
126	201	$x^7+x^6+x^3+1$	11001001	β^{125}
127	223	$x^7+x^6+x^4+x^3+x^2+x+1$	11011111	β^{126}
128	243	$x^7+x^6+x^5+x^4+x+1$	11110011	β^{127}
129	171	$x^7+x^5+x^3+x+1$	10101011	β^{128}
130	27	x^4+x^3+x+1	00011011	β^{129}
131	54	$x^5+x^4+x^2+x$	00110110	β^{130}
132	108	$x^6+x^5+x^3+x^2$	01101100	β^{131}
133	216	$x^7+x^6+x^4+x^3$	11011000	β^{132}
134	253	$x^7+x^6+x^5+x^4+x^3+x^2+1$	11111101	β^{133}
135	183	$x^7+x^5+x^4+x^2+x+1$	10110111	β^{134}
136	35	x^5+x+1	00100011	β^{135}
137	70	x^6+x^2+x	01000110	β^{136}
138	140	$x^7+x^3+x^2$	10001100	β^{137}
139	85	$x^6+x^4+x^2+1$	01010101	β^{138}
140	170	$x^7+x^5+x^3+x$	10101010	β^{139}
141	25	x^4+x^3+1	00011001	β^{140}
142	50	x^5+x^4+x	00110010	β^{141}
143	100	$x^6+x^5+x^2$	01100100	β^{142}
144	200	$x^7+x^6+x^3$	11001000	β^{143}
145	221	$x^7+x^6+x^4+x^3+x^2+1$	11011101	β^{144}
146	247	$x^7+x^6+x^5+x^4+x^2+x+1$	11110111	β^{145}
147	163	x^7+x^5+x+1	10100011	β^{146}
148	11	x^3+x+1	00001011	β^{147}
149	22	x^4+x^2+x	00010110	β^{148}
150	44	$x^5+x^3+x^2$	00101100	β^{149}

S. No	Decimal	polynomial	Binary	Exponential
151	88	$x^6 + x^4 + x^3$	01011000	β^{150}
152	176	$x^7 + x^5 + x^4$	10110000	β^{151}
153	45	$x^5 + x^3 + x^2 + 1$	00101101	v^{152}
154	90	$x^6 + x^4 + x^3 + x$	01011010	β^{153}
155	180	$x^7 + x^5 + x^4 + x^2$	10110100	β^{154}
156	37	$x^5 + x^2 + 1$	00100101	β^{155}
157	74	$x^6 + x^3 + x$	01001010	β^{156}
158	148	$x^7 + x^4 + x^2$	10010100	β^{157}
159	101	$x^6 + x^5 + x^2 + 1$	01100101	β^{158}
160	202	$x^7 + x^6 + x^3 + x$	11001010	β^{159}
161	217	$x^7 + x^6 + x^4 + x^3 + 1$	11011001	β^{160}
162	255	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	11111111	β^{161}
163	179	$x^7 + x^5 + x^4 + x + 1$	10110011	β^{162}
164	43	$x^5 + x^3 + x + 1$	00101011	β^{163}
165	86	$x^6 + x^4 + x^2 + x$	01010110	β^{164}
166	172	$x^7 + x^5 + x^3 + x^2$	10101100	β^{165}
167	21	$x^4 + x^2 + 1$	00010101	β^{166}
168	42	$x^5 + x^3 + x$	00101010	β^{167}
169	84	$x^6 + x^4 + x^2$	01010100	β^{168}
170	168	$x^7 + x^5 + x^3$	10101000	β^{169}
171	29	$x^4 + x^3 + x^2 + 1$	00011101	β^{170}
172	58	$x^5 + x^4 + x^3 + x$	00111010	β^{171}
173	116	$x^6 + x^5 + x^4 + x^2$	01110100	β^{172}
174	232	$x^7 + x^6 + x^5 + x^3$	11101000	β^{173}
175	157	$x^7 + x^4 + x^3 + x^2 + 1$	10011101	β^{174}
176	119	$x^6 + x^5 + x^4 + x^2 + x + 1$	01110111	β^{175}
177	238	$x^7 + x^6 + x^5 + x^3 + x^2 + x$	11101110	β^{176}
178	145	$x^7 + x^4 + 1$	10010001	β^{177}
179	111	$x^6 + x^5 + x^3 + x^2 + x + 1$	01101111	β^{178}
180	222	$x^7 + x^6 + x^4 + x^3 + x^2 + x$	11011110	β^{179}

S. No	Decimal	polynomial	Binary	Exponential
181	241	$x^7 + x^6 + x^5 + x^4 + 1$	11110001	β^{180}
182	175	$x^7 + x^5 + x^3 + x^2 + x + 1$	10101111	β^{181}
183	19	$x^4 + x + 1$	00010011	β^{182}
184	38	$x^5 + x^2 + x$	00100110	β^{183}
185	76	$x^6 + x^3 + x^2$	01001100	β^{184}
186	152	$x^7 + x^4 + x^3$	10011000	β^{185}
187	125	$x^6 + x^5 + x^4 + x^3 + x^2 + 1$	01111101	β^{186}
188	250	$x^7 + x^6 + x^5 + x^4 + x^3 + x$	11111010	β^{187}
189	185	$x^7 + x^5 + x^4 + x^3 + 1$	10111001	β^{188}
190	63	$x^5 + x^4 + x^3 + x^2 + x + 1$	00111111	β^{189}
191	126	$x^6 + x^5 + x^4 + x^3 + x^2 + x$	01111110	β^{190}
192	252	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2$	11111100	β^{191}
193	181	$x^7 + x^5 + x^4 + x^2 + 1$	10110101	β^{192}
194	39	$x^5 + x^2 + x + 1$	00100111	β^{193}
195	78	$x^6 + x^3 + x^2 + x$	01001110	β^{194}
196	156	$x^7 + x^4 + x^3 + x^2$	10011100	β^{195}
197	117	$x^6 + x^5 + x^4 + x^2 + 1$	01110101	β^{196}
198	234	$x^7 + x^6 + x^5 + x^3 + x$	11101010	β^{197}
199	153	$x^7 + x^4 + x^3 + 1$	10011001	β^{198}
200	127	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	01111111	β^{199}
201	254	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$	11111110	β^{200}
202	177	$x^7 + x^5 + x^4 + 1$	10110001	β^{201}
203	47	$x^5 + x^3 + x^2 + x + 1$	00101111	β^{202}
204	94	$x^6 + x^4 + x^3 + x^2 + x$	01011110	β^{203}
205	188	$x^7 + x^5 + x^4 + x^3 + x^2$	10111100	β^{204}
206	53	$x^5 + x^4 + x^2 + 1$	00110101	β^{205}
207	106	$x^6 + x^5 + x^3 + x$	01101010	β^{206}
208	212	$x^7 + x^6 + x^4 + x^2$	11010100	β^{207}
209	229	$x^7 + x^6 + x^5 + x^2 + 1$	11100101	β^{208}
210	135	$x^7 + x^2 + x + 1$	10000111	β^{209}

S. No	Decimal	polynomial	Binary	Exponential
211	67	$x^6 + x + 1$	01000011	β^{210}
212	134	$x^7 + x^2 + x$	10000110	β^{211}
213	65	$x^6 + 1$	01000001	β^{212}
214	130	$x^7 + x$	10000010	β^{213}
215	73	$x^6 + x^3 + 1$	01001001	β^{214}
216	146	$x^7 + x^4 + x$	10010010	β^{215}
217	105	$x^6 + x^5 + x^3 + 1$	01101001	β^{216}
218	210	$x^7 + x^6 + x^4 + x$	11010010	β^{217}
219	233	$x^7 + x^6 + x^5 + x^3 + 1$	11101001	β^{218}
220	159	$x^7 + x^4 + x^3 + x^2 + x + 1$	10011111	v^{219}
221	115	$x^6 + x^5 + x^4 + x + 1$	01110011	β^{220}
222	230	$x^7 + x^6 + x^5 + x^2 + x$	11100110	β^{221}
223	129	$x^7 + 1$	10000001	β^{222}
224	79	$x^6 + x^3 + x^2 + x + 1$	01001111	β^{223}
225	158	$x^7 + x^4 + x^3 + x^2 + x$	10011110	β^{224}
226	113	$x^6 + x^5 + x^4 + 1$	01110001	β^{225}
227	226	$x^7 + x^6 + x^5 + x$	11100010	β^{226}
228	137	$x^7 + x^3 + 1$	10001001	β^{227}
229	95	$x^6 + x^4 + x^3 + x^2 + x + 1$	01011111	β^{228}
230	190	$x^7 + x^5 + x^4 + x^3 + x^2 + x$	10111110	β^{229}
231	49	$x^5 + x^4 + 1$	00110001	β^{230}
232	98	$x^6 + x^5 + x$	01100010	β^{231}
233	196	$x^7 + x^6 + x^2$	11000100	β^{232}
234	197	$x^7 + x^6 + x^2 + 1$	11000101	β^{233}
235	199	$x^7 + x^6 + x^2 + x + 1$	11000111	β^{234}
236	195	$x^7 + x^6 + x + 1$	11000011	β^{235}
237	203	$x^7 + x^6 + x^3 + x + 1$	11001011	β^{236}
238	219	$x^7 + x^6 + x^4 + x^3 + x + 1$	11011011	β^{237}
239	251	$x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$	11111011	β^{238}
240	187	$x^7 + x^5 + x^4 + x^3 + x + 1$	10111011	β^{239}

S. No	Decimal	polynomial	Binary	Exponential
241	59	$x^5+x^4+x^3+x+1$	00111011	β^{240}
242	118	$x^6+x^5+x^4+x^2+x$	01110110	β^{241}
243	236	$x^7+x^6+x^5+x^3+x^2$	11101100	β^{242}
244	149	$x^7+x^4+x^2+1$	10010101	β^{243}
245	103	$x^6+x^5+x^2+x+1$	01100111	β^{244}
246	206	$x^7+x^6+x^3+x^2+x$	11001110	β^{245}
247	209	$x^7+x^6+x^4+1$	11010001	β^{246}
248	239	$x^7+x^6+x^5+x^3+x^2+x+1$	11101111	β^{247}
249	147	x^7+x^4+x+1	10010011	β^{248}
250	107	$x^6+x^5+x^3+x+1$	01101011	β^{249}
251	214	$x^7+x^6+x^4+x^2+x$	11010110	β^{250}
252	225	$x^7+x^6+x^5+1$	11100001	β^{251}
253	143	$x^7+x^3+x^2+x+1$	10001111	β^{252}
254	83	x^6+x^4+x+1	01010011	β^{253}
255	166	$x^7+x^5+x^2+x$	10100110	β^{254}

Bibliography

[1] B. Ann. Cryptographic properties of Boolean functions and S-boxes. Diss. phd thesis-2006, 2006.

[2] E. Brow: Elliptic Curve Cryptography, Math 189A; Algebraic Geometry, December 2010.

[3] S. Bruce, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, and M. Stay. “The Twofish teams final comments on AES Selection.” AES round 2 (2000).

[4] C. Claude “Vectorial Boolean functions for cryptography.” Boolean models and methods in mathematics, computer science, and engineering 134 (2010): 398-469

[5] C. Claude. “Boolean functions for cryptography and error correcting codes.” Boolean models and methods in mathematics, computer science, and engineering 2 (2010): 257.

[6] S. Claude E. “Communication theory of secrecy systems.” Bell Labs Technical Journal 28.4 (1949): 656-715..

[7] T. R. Core. “R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. 2013.” (2014).

[8] A. Cubero, J. Antonio, and P. J. Zufiria “ A c++ class for analysing vector boolean functions from a cryptographic perspective.” In: Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT), pp. 19 (July 2010).

[9] S. S. Deva, and C. P. Arya. "Algebraic Construction and Cryptographic Properties of Rijndael Substitution Box." Defence Science Journal 62.1 (2012): 32-37.

[10] S. Douglas. "Advanced encryption standard." Rivier Academic Journal 6.2 (2010): 1-14.

[11] D. Eastlake and P. Jones.US secure hash algorithm 1 (SHA1) (No. RFC 3174).

[12] L.Edward N. "Deterministic nonperiodic flow." Journal of the atmospheric sciences 20.2 (1963): 130-141.

[13] P. Emmanuel. "DPA attacks and S-boxes." International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2005.

[14] F. Eric, and F. R. Ferard, F. Rodier "On the nonlinearity of Boolean functions. Proceedings of WCC2003, Workshop on coding and cryptography. 2003.

[15] P. J. et al. "A novel method for designing dynamical key-dependent s-boxes based on hyperchaotic system." International Journal of Advancements in Computing Technology 4.18 (2012): 282-289

[16] O. Fatih, and A. B. Ozer. "A method for designing strong S-Boxes based on chaotic Lorenz system." Physics Letters A 374.36 (2010): 3733-3738.

[17] B. Feng, R. H. Deng, W. Geiselmann, C. Schnorr, R. Steinwandt, and H. Wu. "Cryptanalysis of two sparse polynomial based public key cryptosystems." International Workshop on Public Key Cryptography. Springer Berlin Heidelberg, 2001.

[18] L. Frdric. "The boolfun Package: Cryptographic Properties of Boolean Functions." (2012).

[19] J. Goce, and L. Kocarev. "Chaos and cryptography: block encryption ciphers based on chaotic maps." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48.2 (2001): 163-169.

[20] T. Guoping, X. Liao, and Y. Chen. “A novel method for designing S-boxes based on chaotic maps.” Chaos, Solitons , Fractals 23.2 (2005): 413-419

[21] C. Guo, Y. Chen, and X. Liao. ”An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps.” Chaos, Solitons , Fractals 31.3 (2007): 571-579.

[22] N. James, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback. “Report on the development of the Advanced Encryption Standard (AES).” Journal of Research of the National Institute of Standards and Technology 106, no. 3 (2001): 511.

[23] S. Jennifer, X. M. Zhang, and Y. Zheng. (1993, December). Systematic generation of cryptographically robust S-boxes. In Proceedings of the 1st ACM Conference on Computer and Communications Security (pp. 171-182). ACM.

[24] D. Joan, and V. Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science , Business Media, 2013.

[25] B. Johannes, and J. Seifert. “Fault based cryptanalysis of the advanced encryption standard (AES).” International Conference on Financial Cryptography. Springer Berlin Heidelberg, 2003.

[26] B. C. Juan.“ Galois field in cryptography.” University of Washington.(2012).

[27] K. Kazys, and J. Kazlauskas“Key-dependent S-box generation in AES block cipher system” Informatica, 20(1) 2009, 23-34.

[28] M. Kreuzer, Team: Applied Computations in Computer Algebra, v 1.8.0, June 2012

[29] K. R. A1. E. B2. Lars. “Serpent: A proposal for the advanced encryption standard.” First Advanced Encryption Standard (AES) Conference, Ventura, CA. 1998.

[30] B. Linda “ Heuristic optimization of boolean functions and substitution boxes for cryptography”. Diss. Queensland University of Technology, 2005.

[31] M. Mahalinga V., KN .H. Bhat, and R. Murali. "Generation of large set of binary sequences derived from chaotic functions with large linear complexity and good cross correlation properties." Proc. IEEE International Workshop on Microelectromechanical Systems (MEMS97). 2010

[32] S. Martin. "On cryptographic properties of random Boolean functions." Journal of Universal Computer Science 4.8 (1998): 705-717.

[33] D. Mona, and K. Manochehri. "A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key." World Applied Sciences Journal 28.12 (2013): 2003-2009.

[34] W. Neal R. "The Laws of Cryptography with Java Code." Available online at Neal Wagners home page (2003). The Finite Field $GF(2^8)$

[35] C. Nicolas T. "An improved dierential attack on full GOST. The New Codebreakers. Springer Berlin Heidelberg, 2016. 282-303.

[36] S. N. Paul. Cryptography: an introduction. Vol. 5. New York: McGraw-Hill, 2003.

[37] T. Petr. "A new method for generating high non-linearity s-boxes." Radioengineering (2010).

[38] S. Rashmi, and S. Kumar. "Elgamals algorithm in cryptography." International Journal of Scientific , Engineering Research 3.12 (2012): 1-4.

[39] R. Ronald. "The MD5 message-digest algorithm." (1992).

[40] S. Shivkumar and G. Umamaheswari. "Performance Comparison of Advanced Encryption Standard (AES) and AES key dependent S-box-Simulation using MATLAB." Process Automation, Control and Computing (PACC), 2011 International Conference on. IEEE, 2011.

[41] R. Ronald L., A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[42] W. A. Stein: Sage Mathematics Software (Version 5.10). The Sage Development Team (2013), http://www.sagemath.org

[43] P. Stjepan, L. Batina, D. Jakobovi, B. Ege, and M. Golub. “S-box, SET, match: a toolbox for S-box analysis.” In IFIP International Workshop on Information Security Theory and Practice, pp. 140-149. Springer Berlin Heidelberg, 2014.

[44] W. Xingyuan, and Q. Wang. “A novel image encryption algorithm based on dynamic S-boxes constructed by chaos.” Nonlinear Dynamics 75.3 (2014): 567-576.

[45] S. William. Cryptography and network security: principles and practices. Pearson Education India, 2006.

[46] W. Xingyuan, and J. Zhao. “An improved key agreement protocol based on chaos.” Communications in Nonlinear Science and Numerical Simulation 15.12 (2010): 4052-4057.