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

An Application of One Parameter Families of Elliptic Curves

By

Muhammad Asif

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2017

An Application of One Parameter Families of Elliptic Curves

By

Muhammad Asif

Supervised By

Dr. Umar Hayat

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2017

An Application of One Parameter Families of Elliptic Curves

By

Muhammad Asif

A DISSERTATION SUBMITTED IN THE PARTAL FULFILLMENT OF THE REQUIRMENT

FOR THE DEGREE OF

MASTER OF PHILOSOPHY

in

Mathematics

Supervised By

Dr. Umar Hayat

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2017

Dedicated to

My

Beloved

Parents

Acknowledgements

First of all I am very thankful to my Almighty **Allah** by the blessing of which I completed this thesis.

I am heartily thankful to Dr. Umar Hayat, Assistant Professor in the department of Mathematics, Quaid-i-Azam University, Islamabad, for giving me the opportunity to work under his grand supervision. His good wishes, encouragement and the sharpness of his comments are a part of this work. At the time of difficulties his help came handy that saw me finishing this work without any technical or administrative hitch. My gratitude to him is a living presence in me.

I would also like to convey my sincere gratitude to Prof. Dr. Muhammad Yousaf Malik, Chairman of the department of mathematics, Quaid-i-Azam University, Islamabad.

The following friends of mine have helped and shown affection for me on various occasions during my stay in the campus and I am grateful to them very much. They are: Mr. Fawad Ali, Mr. Ghulam Murtaza, Mr. Muhammad Zeeshan, Mr. Muhammad Shahid, Mr. Ghulam Frid, Mr. Tanveer ul haq, Mr. Muhammad Mubashir, Mr. Iqrar Ansari, Mr. Akhtar Abbas, Mr. Muhammad Irfan Khan, Mr. Irfan Ullah, Mr. Wahid Ullah.

The selfless love and sacrifice of my father Muhammad Lehrasab and mother are the driving force of my education. My father's love is the protective shield of mine that gives me confidence in all my activities and guides me right. If at all I come to this prestigious institute and submit this thesis here now, behind it lies the difficulties with which my father and mother have brought me up and their innocent and deep prayers for me. This thesis is dedicated to my parents.

Finely, I cannot forget the support of my family, especially my brothers Mr. Muhammad Shehzad, Mr. Muhammad Yasir, Mr. Ali Ahmed and my lovely sisters.

Muhammad Asif

Abstract

People from ancient times are using various methods to communicate secretly and now a days we call it cryptography. In modern era there are many secure and sophisticated techniques to transmit data/information. Elliptic curve based cryptography is used from early 80's and is one of the best existing method due to the presence of group law on the points of elliptic curve. The use of group law has many algebraic and geometric advantages when it is used for cryptographic purpose. Elliptic curve cryptography (ECC) provides better security and is more efficient as compare to other public key cryptosystems with identical key size. In this thesis we give a new method for the construction of Substitution box(S-box). We use points lying on the elliptic curve over the finite field to generate S-box. The resistance of the newly generated S-box against common attacks such as linear, differential and algebraic attacks is analyzed by calculating its non-linearity, linear approximation, strict avalanche, bit independence, differential approximation and algebraic complexity. The experimental results are further compared with some of the existing S-boxes presented in [5, 15, 17, 20, 26, 38, 45]. Comparison reveals that the proposed algorithm generates cryptographically strong S-box as compare to some of the other exiting techniques.

Contents

Contents of tables

Chapter 1

Preliminaries

In this chapter, we give some basic concepts of cryptography that will be used in coming chapters of this thesis.

1.1 **Cryptology**. [41]:

It is the science which deals with the subject of secret codes and the mechanisms that are used to construct and decipher these codes. Roughly speaking cryptology is the study of cryptanalysis or cryptography.

1.2 **Cryptosystem**. [31]:

Pair of algorithms which use key for converting plaintext into ciphered form and vice versa is called cryptosystem.

1.3 **Cryptography**. [6]:

It is the study of writing message secretly with the aim of masking the sense of message. In cryptography we study different methods for converting a message into such a complex form that can be inferred by legal person only who has been given secrete key to decrypt that message. If message is catched by unauthorized person, he could not translate it.

1.4 **Cryptanalysis**. [6]:

Cryptanalysis is the art of designing different techniques to decipher the catched (secrete) message without having secrete key worn by sender. This is called “breaking of code.”

Cryptanalysis has a central role in recent cryptosystems. Because without those people who wishes to break our crypto methods, we cannot know we are safe or not. As cryptanalysis is unique way to make sure that our cryptosystem is safe, it is essential unit of cryptology. Cryptography is further divided into three major branches.

(i) Symmetric algorithms:

In this branch of cryptology data is shared between two parties having specific encryption and decryption algorithm and these two parties share secret key between them. From ancient time to 1976, this type of cryptography was used entirely. Still symmetric ciphers are commonly used for encryption of data.

(ii) Asymmetric (public key) algorithms:

Whitfield Diffie, Ralph Merkel and Martin Hellman introduced a completely different form of enciphering scheme in 1976. In asymmetric cryptography user acquires a secret as well as public key. These algorithms can be used for classical data encryption.

(iii) Cryptographic protocol. [6]:

In simple wording cryptographic protocol has to do with the utilization of the cryptographic methods (algorithms). Symmetric and asymmetric algorithms are parts of protocol. The example of cryptographic protocol is Transport Layer Security (TLS) scheme that is used in each web browser. Practically, in most of the applications both the algorithms symmetric and asymmetric are used together. It is called hybrid scheme. The reason is that both these algorithms have their own firmness and deficiencies. The center of our attention is symmetric and asymmetric algorithms.

1.5 Symmetric cryptography. [6]:

Symmetric key cryptography is also called single key or secret key cryptography. Suppose two persons Alice and Bob want to interact through an unassured channel. The term channel means any communication link such as mobile phone, internet or any communication media. The trouble starts with an unacceptable boy, Oscar, having access to the communication link. Such an

illegal listening is referred as eavesdropping. Obviously there may be many topics on which Alice and Bob want to communicate secretly. For example suppose Alice and Bob are business man and they are doing the business of same kind in different places. Alice wants to send data to Bob which contain some strategies for the betterment of their business in coming years. This data should not fall into the hand of their competitors. In such conditions secret key cryptography gives best solution. Alice starts the encryption of the message ' x ' using a secret key ' k ' and as a result a cipher text ' y ' is obtained. Alice sends this cipher text to Bob. Alice also send key to Bob through secure channel. On receiving the cipher text Bob decrypt that message using the key ' k ' as shown in figure 1.1. So decryption is reverse step of encryption. The advantage is that, if we have energetic encryption algorithm then Oscar cannot understand the message because the cipher text occur in random bits to Oscar.

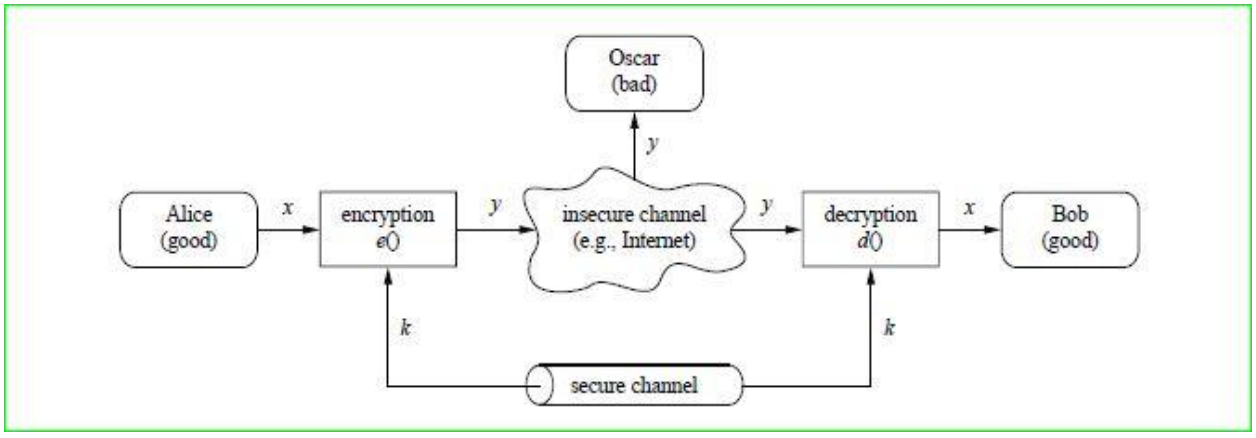


Figure 1.1

The most popular example of symmetric key cryptography is Data Encryption Standard (DES) and Advance Encryption Standard (AES).

A resemblance for symmetric cryptography is shown in figure 1.2. In this figure a safe is shown along with a lock. The key for this lock is given to Alice and Bob only. The encryption of message means placing a message in this safe. To read this message Bob will use his key.

Figure 1.2

1.6 Substitution-box (S-box). [44]:

S-box is a vital part of secret key cryptography which executes substitution. S-boxes are commonly used to vague the interrelation between ciphertext and key. Roughly speaking an S-box gets some number of bits, r, as input and returns some number bits, s, as an output, here r is not always equal to s. In most of the cases, they are selected very carefully so that they can resist the cryptanalytic attacks.

DES consists of 8 S-boxes and these S-boxes are under the intensive study for several years. After the exploration of differential attack the designed criteria of the S-box were published ultimately, showing that S-boxes had been deliberately tuned to enhance protection against this peculiar attack. Researchers have done a lot of research to construct an S-box which can resist against almost all the cryptanalytic attacks.

On October 2000, Rijndael block cipher [10] is adopted by National Institute of Standards and Technology (NIST) as an Advanced Encryption Standard (AES). Nowadays, the

AES is mainly used for data encryption in private key cryptosystem. Other than S-box, all mappings which are being used in the AES are linear transformations resting on Z_2. The only nonlinear part of the AES is the S-box that is important for creating agitation in the data [44]. Many cryptanalysis have studied the structural properties of AES. In [13] there is a formula for Rijndael cipher. Furthermore, it is proved that arithmetic demonstration of the AES is made up of those equalities whose results are not feasible. In [35] another explanation of the AES is given and it is proved that AES is enclosed in another recent cipher. Rosenthal in [42] presented a permutation polynomial of S-box of AES on finite ring. It is realized that the S-box of AES is sparse. So it is clear that the security of AES against different attacks like differential, algebraic and linear attacks [7, 21] is uncertain [34]. Anyhow, still no attack is invented that stunt the default structures of S-box of AES.

1.7 Discrete logarithm problem. [6]:

The generalized form of discrete logarithm problem is given in following.

"For any finite cyclic group G with binary operation $*$ and let cardinality of G is n. Let α be the generator of G and β be any other element of G. Find an integer q such that $\alpha^q = \beta$ where $1 < q < n$".

The discrete logarithm problem over $Z_p^\times$, where p is a prime is given as "Let $Z_p^\times$ be a finite cyclic group of order $p-1$. Further let α be the generator β is any other element of $Z_p^\times$. Find the integer q such that $\alpha^q = \beta \pmod{p}$ where $1 < q < p-1$"

1.8 Drawbacks of symmetric cryptography:

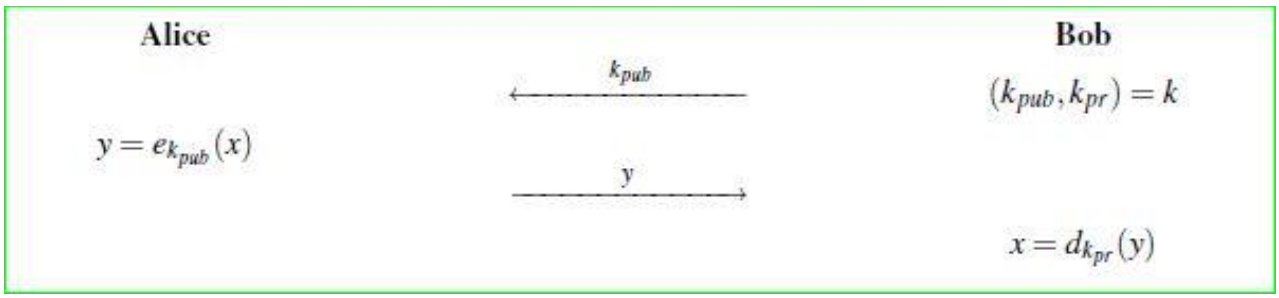
We can observe that in symmetric cryptography the secret key is same which is used for encryption as well as for decryption. The second thing is that encryption function and decryption function are almost identical. Some shortcomings of symmetric key cryptography are discussed below.

1- The key should be settled between two parties by adopting secure channel. But it must be clear that any communication link is not secure. So sending a key securely by channel is not possible.

2- As Alice and Bob possess same key. So symmetric cryptography cannot be adopted for those applications in which we like to avoid cheating by each of two (Alice or Bob). For example in some applications it is necessary to confirm that Alice really sent a specific message, say, an order of laptop. If plan of Alice is changed after some time and we use symmetric cryptography for the sending order of Alice then Alice can claim that Bob has developed the purchase order faithlessly. Preventing from such a situation is referred as nonrepudiation and can be managed by public key cryptography.

1.9 Asymmetric (public key) cryptography:

Asymmetric cryptography rested upon the following idea: "There is no need to keep the encryption key secret. The essential unit is that Bob can only decrypt by applying secret key". To get such a scheme Bob publish his encryption key k_{pub} (called public key) which is familiar to every person. Bob also has a private (secret) key k_{pr} which he will use for decryption. This scheme works just like a mailbox on the street corner. Every person can insert a letter into it, i-e encrypt, but these letters can only be retrieved, decrypted, by that person who have a private (secret) key. A protocol for asymmetric encryption is given below.



By looking at the protocol it is clear that we can communicate by encrypting a message without private channel. So public key cryptography is beautiful scheme for security applications. The most popular example of public key cryptography is RSA and Knapsack cryptosystem.

1.10 Elliptic curve cryptography (ECC). [6]:

ECC is the advanced type of public key cryptography. This type of cryptography is started in mid 1980s. The extent of security of ECC and RSA is same but the advantage of ECC is that, the key size of ECC is very small as compare to the key size of RSA. ECC was individually developed by Neal Koblitz in 1987 and by Victor Miller in 1986. There was a lot of conjectures on the security of ECC During 1990s. But after comprehensive research, it appears today very secure like RSA. The main tool which is used to measure the security of many cryptographic schemes is the key length. Private and academic organizations gives mathematical formulas to calculate the minimum size of key required for security. According to the opinion of many cryptographers, existing systems gives somewhat 128 bits of security. Here the word 128 bits of security does not means the key length is 128 bits. Security is derived from the consolidation of certain algorithm and length of its key. For example using ECC 128 bits of security can be attained by 256 bit keys but on the other hand in RSA 3072 bit keys is needed for the same (128 bits) security. The comparison of security of ECC and RSA is given in the following table.

Security bits	Minimum size (bits) of public keys	
	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

In the Figure 1.10 a comparison between RSA cryptosystem and ECC is shown. It can be observed that in ECC key size is very small as compare to RSA key size but security is much

stronger. Due to these properties ECC is a decent choice for multimedia types of data such as audio, video and images.

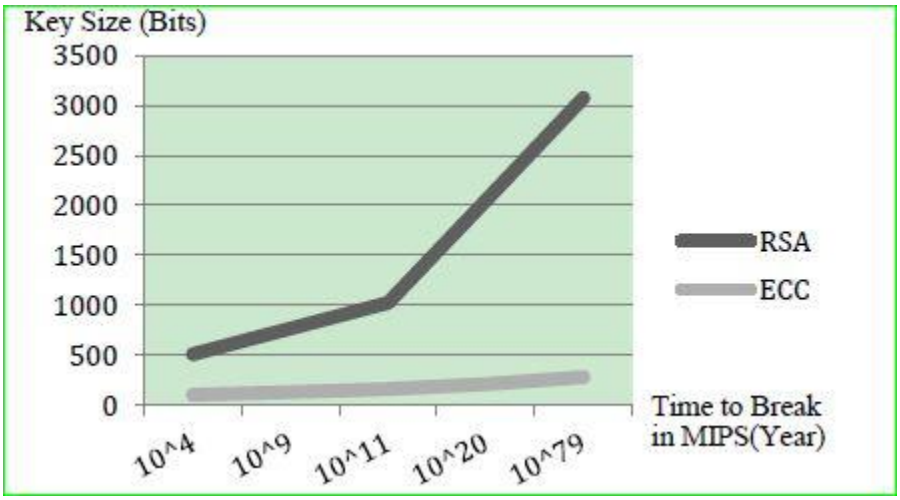


Figure 1.10

With the passage of time key length increases due to the advancement in cryptanalysis. According to the opinion of some experts, AES-256 must be selected for data encryption in place of earlier approved AES-128 protocol. For this purpose if we use elliptic curve then the key length of 128 bits is required but to get the same security level using RSA encryption, we need 15360 bit key, which is unattainable nowadays for embedded systems. From this explanation it is clear that ECC is better algorithm for embedded systems.

If we talk about the performance at the security level of 128 bits, It is observed that ECC is 10-times faster than RSA. This difference increases greatly at the security level of 256 bit where ECC is 50 to 100 times faster than RSA. The key generation of ECC is also 100 to 1000 times faster than RSA. In the following two paragraphs we present uses of elliptic curve cryptography.

Rapid advancement of information technologies has induced the development of internet of things (IoT). In medical field, its use can be implemented to different areas and carry ease to

doctors and patients. The basic communication technology used in IoT is radio-frequency identification (RFID) technology. To fulfill the requirements of its security several authentication schemes have been developed. To give finer security and achievement to RFID authentication scheme, ECC has been used.

Nowadays people are interested to do online transactions. They make association with different organizations like e-library, e-banks or e-stores. They fill out the personal information on the websites of these organizations to attain the service. Organizations share this personal information of people with other organizations to get benefits. Thus personal information of users reaches in those organizations with which he never wants to be connected. So there is an immense threat to privacy of users. There are many techniques to enhance the privacy of users. One of them is private credentials which is an important scheme to preserve the privacy of users. This scheme can be redefined by using ECC because implementation of private credentials becomes much more efficient when we use ECC.

ECC rests on generalized discrete logarithm problem. In most of the cases, if we use ECC instead of RSA we have to perform less computations. First of all we give a brief introduction of mathematics of elliptic curve.

Consider a polynomial $x^2 + y^2 = r^2$ upon set of real numbers. By plotting all the points (x, y) satisfying $x^2 + y^2 = r^2$ we get a circle which is shown in figure 1.3.

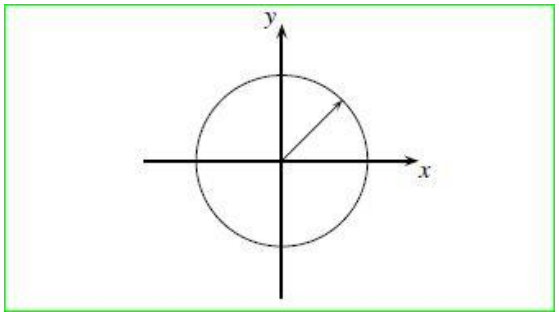


Figure 1.3

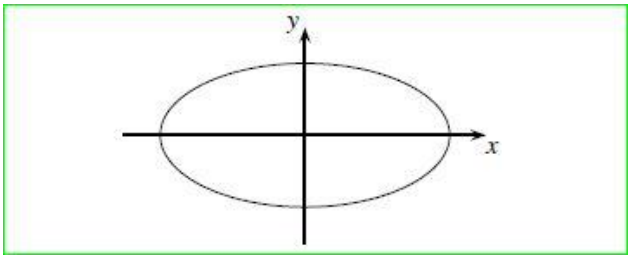


Figure 1.4

Now consider the polynomial $ax^2 + by^2 = c$ over the set of real numbers. It yields an ellipse, shown in figure 1.4.

1.10.1 Elliptic curve:

It is clear from the above two examples that we can form a curve from polynomial equations. The word curve means the set of those points which satisfies the given equation. A certain kind of polynomial ($y^2 = x^3 + ax + b$ where $a, b \in R$) is called elliptic curve. To use it for cryptography we will take a curve over finite field instead of set of real numbers. The most prominent choice for the field is prime field.

1.10.2 Elliptic curve over a finite prime field:

Consider a prime field F_p having p elements, where p is a prime number. For each prime number p there exists exactly one prime field F_p. For any two integers of F_p say a and b, the elliptic curve on field F_p is defined as

$E(F_p) = \{(x, y) \in F_p{}^2 \mid y^2 = x^3 + ax + b \ (mod\ p) and\ a, b, x, y \in F_p\} \cup \{O\}$, provided

$4a^3 + 27b^2 \neq 0 \ (mod\ p)$, here O denotes the infinite point. Number of elements $\#E(Fp)$, in $E(F_p)$ is equal to the number of points lying on elliptic curve over F_p. Hasse theorem [18] gives the bounds of total number of points on elliptic curve so by this theorem

$$p + 1 - 2\sqrt{p} \leq \#E(F_p) \leq p + 1 + 2\sqrt{p}.$$

The expression $4a^3 + 27b^2$ is called the discriminant of elliptic curve. The elliptic curve $y^2 = x^3 - 3x + 3$ over the set of real number is shown in figure 1.5.

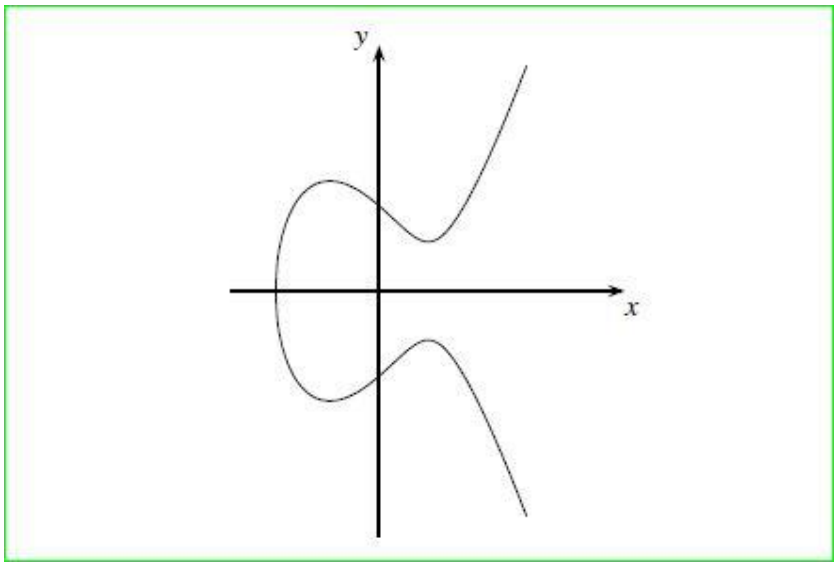


Figure 1.5

From this graph we notice that the elliptic curve is symmetric about x-axis. Further it intersect the x-axis at only one point. This is because if we put y = 0 in the equation of this elliptic curve we get only one real root of cubic equation and two other roots are complex. However there exists some elliptic curves having three intersection points with x-axis. Set of all the points lying on the elliptic curve form an abelian group which is explained in following.

1.11 Group laws of elliptic curves:

Let "+" denotes the addition operation on the group. Addition means for any two given points $P(x, y)$ and $Q(x_1, y_1)$ we need to calculate the third point $R(x_2, y_2)$ such that $P + Q = R$. Fortunately there is a nice geometric explanation of addition of two points on elliptic curve defined over the set of real numbers. We will explain two type of addition below. The first one is addition of two distinct points and the second one is addition of point to itself (points doubling).

1.11.1 Addition of two distinct points:

Consider two distinct points P and Q and let $P + Q = R$. These two points can be added by following rule: Draw a line passing through P and Q and get another intersection point between this line and elliptic curve. Get a mirror of this point about x-axis. The mirrored point is the R (sum of P and Q). Addition of the points P and Q is shown in figure 1.6.

1.11.2 Points doubling:

For any point P of the elliptic curve let $P+P = 2P = R$. To get the point R on elliptic curve we draw a tangent at point P and obtain a point of intersection of this tangent and elliptic curve. Then we mirror that point about x-axis. That mirrored point is R as shown in figure 1.7.

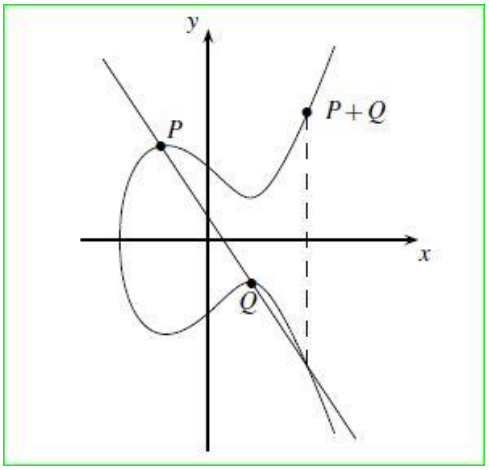


Figure 1.6

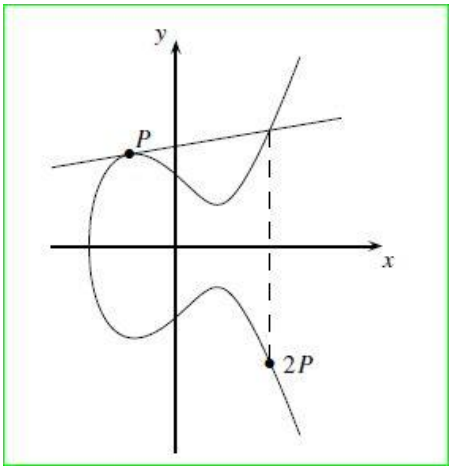


Figure 1.7

Points addition and multiplication is shown above by taking elliptic curve over real field. But if the curve is on prime field then point addition and multiplication is given as following

For any two points $P(x, y)$ and $Q(x_1, y_1)$ on the elliptic curve where $P \neq Q$. Then $P + Q = (x_2, y_2)$, where $x_2 = m^2 - x - x_1$ and $y_2 = m(x - x_2) - y$.

In above formula if $P \neq Q$ then $m = \left(\frac{y_1 - y}{x_1 - x} \right)$ otherwise if $P = Q$ then $m = \left(\frac{3x^2 + a}{2y} \right)$.

Example1: Consider the elliptic curve $y^2 = x^3 + 3x + 72$ and $p = 9$. Points $P(35,9)$ and $Q(15,0)$ lies on it. Then by using above formula we have $P + Q = (78,25)$.

Example2: For the same elliptic curve described in example 1. Let $P = (35,9)$ then $2P = P + P = (0,-1)$.

1.11.3 Point Multiplication:

For any point P on the elliptic curve the operation of multiplication of the point P is defined as repeated addition. $kP = P + P + \ldots\ldots\ldots + P$ k times.

Example3: Consider the elliptic curve $y^2 = x^3 + 2x + 9$ and $p = 37$. For the point $P = (11,17)$ that lies on the elliptic curve, $5P = P + P + P + P + P = (33,9)$.

1.11.4 Identity:

$P + O = P = O + P$ where P is any point of the elliptic curve and O is infinite point. It is also clear from Figure 1.8.

When we join P with O we get a third point $P * O$. Now by joining $P * O$ with O we get the point P again. This shows that O is identity point.

1.11.5 Negatives:

Let $Q(x_1, y_1)$ be any point on elliptic curve then $(x_1, y_1) + (x_1, -y_1) = O$, where $(x_1, -y_1)$ stands for $-Q$ and is called negative of Q as shown in Figure 1.9.

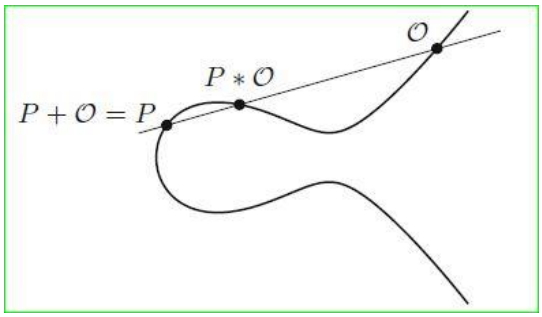


Figure 1.8

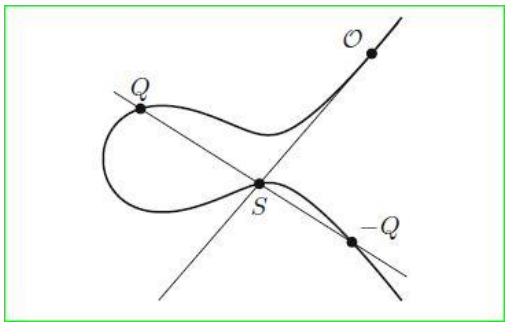


Figure 1.9

So we have defined all the group properties for elliptic curve.

Chapter 2

Rossby Wave Triads and Elliptic Curves

2.1 Introduction

In this chapter we derive the equation of an elliptic curve in weirstrass form from the equations satisfied by rossby triads. Then we will reduce the coefficients appearing in the equation of that elliptic curve according to prime field F_p which will be referred as prime elliptic curve. That prime elliptic curve will be used for construction of S-box in chapter 3. We give an algorithm that how we can use the points of elliptic curve to construct S-box having strong cryptographic properties. First of all we will give the brief introduction on rossby waves in the atmosphere.

2.2 Rossby waves. [3]:

Rossby waves are also called planetary waves. These waves are the natural phenomenon that takes place in the oceans and in the atmospheres of planets that mostly owe their properties to the rotation of the planet.

Rossby waves on earth are an instinctive phenomenon in the atmosphere of the earth that have the main impact on weather. Mathematically these are solutions of those equations which are administrating the dynamics of oceans and atmosphere. The very interesting case of rossby waves is that the component of two waves generates the third wave and the interaction of this third wave with each of them produces the other wave. The non linear interaction of waves is necessarily restricted to three components that transfer energy but do not generate another wave. These three waves are known as resonant triads. Mathematically the set of wave vectors satisfying the following equations is called resonant triad.

$$r_1 + r_2 = r_3 \qquad (1)$$

$$s_1 + s_2 = s_3 \qquad (2)$$

$$t_1 + t_2 = t_3 \qquad (3)$$

Where $t_i = \dfrac{r_i}{r_i^2 + s_i^2}$, $(r_i, s_i) \in Z^2$

So equation (3) can be written as

$$\frac{r_1}{r_1^2 + s_1^2} + \frac{r_2}{r_2^2 + s_2^2} = \frac{r_3}{r_3^2 + s_3^2} \qquad (4)$$

From equation (1) and (2) we have

$$r_2 = r_3 - r_1 \text{ and } s_2 = s_3 - s_1$$

Using these values in equation (4) we have

$$\frac{r_1}{r_1^2 + s_1^2} + \frac{r_3 - r_1}{(r_3 - r_1)^2 + (s_3 - s_1)^2} = \frac{r_3}{r_3^2 + s_3^2}$$

$$\frac{r_1}{r_1^2 + s_1^2} + \frac{r_3 - r_1}{r_3^2 + r_1^2 - 2r_3 r_1 + s_3^2 + s_1^2 - 2s_3 s_1} = \frac{r_3}{r_3^2 + s_3^2}$$

$$\frac{r_1}{r_1^2+s_1^2}+\frac{r_3-r_1}{r_3^2+r_1^2-2r_3r_1+s_3^2+s_1^2-2s_3s_1}-\frac{r_3}{r_3^2+s_3^2}=0$$

Multiplying both sides by $(r_1^2+s_1^2)(r_3^2+r_1^2-2r_3r_1+s_3^2+s_1^2-2s_3s_1)(r_3^2+s_3^2)$ we have

$$\begin{aligned}&r_1(r_3^2+r_1^2-2r_3r_1+s_3^2+s_1^2-2s_3s_1)(r_3^2+s_3^2)+(r_3-r_1)(r_1^2+s_1^2)(r_3^2+s_3^2)\\&-r_3(r_3^2+r_1^2-2r_3r_1+s_3^2+s_1^2-2s_3s_1)(r_1^2+s_1^2)=0\end{aligned}$$

$$\begin{aligned}&(r_1r_3^2+r_1^3-2r_3r_1^2+r_1s_3^2+r_1s_1^2-2r_1s_3s_1)(r_3^2+s_3^2)+(r_3r_1^2+r_3s_1^2-r_1^3-r_1s_1^2)(r_3^2+s_3^2)\\&-(r_3^2+r_1^2-2r_3r_1+s_3^2+s_1^2-2s_3s_1)(r_1^2r_3+s_1^2r_3)=0\end{aligned}$$

$$\begin{aligned}&r_1r_3^4+r_1^3r_3^2-2r_1^2r_3^3+r_1s_3^2r_3^2+r_1s_1^2r_3^2-2r_1s_1s_3r_3^2+r_1r_3^2s_3^2+r_1^3s_3^2-2r_1^2r_3s_3^2+r_1s_3^4+r_1s_1^2s_3^2-2r_1s_3^3s_1+r_3^3r_1^2\\&+r_3^3s_1^2-r_1^3r_3^2-r_1r_3^2s_1^2+r_3r_1^2s_3^2+r_3s_1^2s_3^2-r_1^3s_3^2-r_1s_1^2s_3^2-r_3^3r_1^2-r_1^4r_3+2r_1^3r_3^2-s_3^2r_1^2r_3-s_1^2r_1^2r_3+2s_1s_3r_1^2r_3\\&-r_3^3s_1^2-r_1^2r_3s_1^2+2r_1r_3^2s_1^2-s_1^2s_3^2r_3-s_1^4r_3+2s_1^3s_3r_3=0\end{aligned}$$

After simplification we have

$$\begin{aligned}&r_1r_3^4+r_1s_3^4+r_1s_3^2r_3^2-2r_1^2r_3^3-2r_1^2r_3s_3^2-2r_1s_3^3s_1-2r_1s_1s_3r_3^2+2r_1^3r_3^2+2s_1s_3r_1^2r_3+2r_1r_3^2s_1^2+2s_1^3s_3r_3+r_1s_3^2r_3^2\\&-r_1^4r_3-s_1^2r_1^2r_3-r_1^2r_3s_1^2-s_1^4r_3=0\end{aligned}$$

Multiplying both side by ' –1 ' and rearranging

$$\begin{aligned}&r_1^4r_3+s_1^4r_3+2r_3s_1^2r_1^2-2r_1^3r_3^2-2s_1s_3r_1^2r_3-2r_1r_3^2s_1^2-2s_1^3s_3r_3+2r_1^2r_3^3+2r_1^2r_3s_3^2+2r_1s_3^3s_1+2r_1s_1s_3r_3^2-r_1r_3^4\\&-r_1s_3^4-2r_1r_3^2s_3^2=0\end{aligned}$$

$$r_3(r_1^2+s_1^2)^2-2r_3(r_1^3r_3+s_1s_3r_1^2+r_1r_3s_1^2+s_1^3s_3)+2r_1(r_1r_3^3+r_1r_3s_3^2+s_3^3s_1+r_3^2s_1s_3)-r_1(r_3^4+s_3^4+2r_3^2s_3^2)=0$$

After factorization of 2nd, 3rd and 4th term we have

$$r_3(r_1^2+s_1^2)^2-2r_3(r_1r_3+s_1s_3)(r_1^2+s_1^2)+2r_1(r_3^2+s_3^2)(r_1r_3+s_1s_3)-r_1(r_3^2+s_3^2)^2=0 \qquad (5)$$

Now there are two possibilities either $r_3=0$ or $r_3\neq 0$

A mode (r,s) with $r=0$ is called zonal mode. When $r_3=0$, equation (5) becomes

$$2r_1s_3^2(s_1s_3) - r_1(s_3^4) = 0$$

i-e

$$(2s_1 - s_3)r_1s_3^3 = 0$$

It can be easily solved, so we are not considering this case because resonant interaction with zonal mode is trivial. When $r_3 \neq 0$ then we have four variables in equation (5). Note that (r_3, s_3) and $(-s_3, r_3)$ are two perpendicular vectors in plane. As any two perpendicular vectors in the plane can behaves as basis. So if we know (r_3, s_3) we can generate the other one that is (r_1, s_1) by using following relation.

$$(r_1, s_1) = m(r_3, s_3) + n(-s_3, r_3) \qquad (6)$$

$$\Rightarrow \quad r_1 = mr_3 - ns_3 \quad \text{and} \quad s_1 = ms_3 - nr_3 \qquad (7)$$

$$\Rightarrow \quad m = \frac{r_1 + ns_3}{r_3} \qquad \text{Put in equation (7)}$$

$$s_1 = \left(\frac{r_1 + ns_3}{r_3} \right) s_3 + nr_3$$

$$\Rightarrow \quad s_1r_3 = r_1s_3 + n(s_3^2 + r_3^2)$$

$$\Rightarrow \quad n = \frac{s_1r_3 - r_1s_3}{s_3^2 + r_3^2}$$

Now

$$m = \frac{r_1 + \left(\frac{s_1r_3 - r_1s_3}{s_3^2 + r_3^2} \right) s_3}{r_3}$$

$$m = \frac{r_1(s_3^2 + r_3^2) + s_1 r_3 s_3 - r_1 s_3^2}{r_3(s_3^2 + r_3^2)}$$

After simplification

$$m = \frac{r_1 r_3 - s_1 s_3}{s_3^2 + r_3^2}$$

Now consider

$$m^2 + n^2 = \frac{r_1^2 r_3^2 + s_1^2 s_3^2 + 2 r_1 r_3 s_1 s_3}{(s_3^2 + r_3^2)^2} + \frac{s_1^2 r_3^2 + r_1^2 s_3^2 - 2 r_1 r_3 s_1 s_3}{(s_3^2 + r_3^2)^2}$$

$$m^2 + n^2 = \frac{r_1^2 r_3^2 + s_1^2 s_3^2 + s_1^2 r_3^2 + r_1^2 s_3^2}{(s_3^2 + r_3^2)^2}$$

After simplification we have

$$m^2 + n^2 = \frac{(s_1^2 + r_1^2)}{(s_3^2 + r_3^2)}$$

$$\Rightarrow \qquad s_1^2 + r_1^2 = (m^2 + n^2)(s_3^2 + r_3^2) \tag{8}$$

Equation (5) is

$$r_3(r_1^2 + s_1^2)^2 - 2r_3(r_1 r_3 + s_1 s_3)(r_1^2 + s_1^2) + 2r_1(r_3^2 + s_3^2)(r_1 r_3 + s_1 s_3) - r_1(r_3^2 + s_3^2)^2 = 0$$

Dividing both sides by r_3 we have

$$(r_1^2 + s_1^2)^2 - 2(r_1 r_3 + s_1 s_3)(r_1^2 + s_1^2) + 2\frac{r_1}{r_3}(r_3^2 + s_3^2)(r_1 r_3 + s_1 s_3) - \frac{r_1}{r_3}(r_3^2 + s_3^2)^2 = 0$$

Now dividing both sides by $(r_3^2+s_3^2)^2$ we have

$$\frac{(r_1^2+s_1^2)^2}{(r_3^2+s_3^2)^2}-2(r_1r_3+s_1s_3)\frac{(r_1^2+s_1^2)}{(r_3^2+s_3^2)^2}+2\frac{r_1}{r_3}\frac{(r_1r_3+s_1s_3)}{(r_3^2+s_3^2)}-\frac{r_1}{r_3}=0$$

Using the value of m and equation (8) we have

$$\left(m^2+n^2\right)^2-2m(m^2+n^2)+(2m-1)(m-\frac{s_3}{r_3}n)=0 \qquad (9)$$

Here we discuss two separate cases.

Case1

When $m=0$

Equation (9) becomes

$$n^4+\frac{s_3}{r_3}n=0$$

Here we reject the solution $n=0$ because it produce a triad which is generated by collinear modes. So $n\neq 0$ then $n^3=-\frac{s_3}{r_3}$

but n is rational number. So we can say that in this case the non trivial triad is possible only when $\frac{s_3}{r_3}$ is pure cubic rational.

Case2

When $m\neq 0$ provided $\frac{s_3}{r_3}$ is not a pure cubic rational. We use following transformations.

Let $\lambda = \frac{n}{m}$ put in (9)

$$\left(m^2 + \lambda^2 m^2\right)^2 - 2m\left(m^2 + \lambda^2 m^2\right) + \left(2m-1\right)\left(m - \frac{s_3}{r_3} m\lambda\right) = 0$$

$$m^4 + \lambda^4 m^4 + 2m^4\lambda^2 - 2m^3 - 2m^3\lambda^2 + 2m^2 - 2m^2\lambda\frac{s_3}{r_3} - m + \frac{s_3}{r_3} m\lambda = 0$$

Dividing both sides by m we have

$$m^3\left(1+\lambda^2\right)^2 - 2m^2\left(1+\lambda^2\right) + \left(2m-1\right)\left(1 - \frac{s_3}{r_3}\lambda\right) = 0$$

Multiplying both sides by $1+\lambda^2$ we have

$$m^3\left(1+\lambda^2\right)^3 - 2m^2\left(1+\lambda^2\right)^2 + \left(2m-1\right)\left(1 - \frac{s_3}{r_3}\lambda\right)\left(1+\lambda^2\right) = 0$$

Now put $\gamma = m\left(1+\lambda^2\right)$

$$\gamma^3 - 2\gamma^2 + \left\{2\gamma - \left(1+\lambda^2\right)\right\}\left(1 - \frac{s_3}{r_3}\lambda\right) = 0 \qquad (10)$$

Using $D = \frac{1}{1 - \frac{s_3}{r_3}\lambda}$, $x_1 = \gamma D$, $y_1 = \lambda D$ equation (10) becomes

$$\frac{x_1^3}{D^3} - 2\frac{x_1^2}{D^2} + \left(2\frac{x_1}{D} - 1 - \frac{y_1^2}{D^2}\right)\left(\frac{1}{D}\right) = 0$$

Multiplying both side by D^3

$$x_1^3 - 2Dx_1^2 + 2Dx_1 - D^2 - y_1^2 = 0$$

$$\Rightarrow y_1^2 = x_1^3 - 2Dx_1^2 + 2Dx_1 - D^2 \qquad (11)$$

Put $a = -2D, b = 2D, c = -D^2$

So equation (11) becomes

$$y_1^2 = x_1^3 + ax_1^2 + bx_1 + c \qquad (12)$$

Suppose charF≠2, 3

Put $x = x_1 + \frac{a}{3}, y = y_1$

So equation (12) becomes

$$y^2 = \left(x - \frac{a}{3}\right)^3 + a\left(x - \frac{a}{3}\right)^2 + b\left(x - \frac{a}{3}\right) + c$$

$$= x^3 - \frac{a^3}{27} - ax^2 + \frac{a^2 x}{3} + ax^2 + \frac{a^3}{9} - \frac{2xa^2}{3} + bx - \frac{ba}{3} + c$$

$$y^2 = x^3 + \left(\frac{a^2}{3} - \frac{2a^2}{3} + b\right)x + \frac{a^3}{9} - \frac{ba}{3} - \frac{a^3}{27} + c$$

$$= x^3 + \left(\frac{a^2 - 2a^2 + 3b}{3}\right)x + \frac{3a^3 - 9ab - a^3 + 27c}{27}$$

$$= x^3 + \left(\frac{3b - a^2}{3}\right)x + \frac{2a^3 - 9ab + 27c}{27}$$

After putting values of a, b and c we have

$$y^2 = x^3 + \left(\frac{6D - 4D^2}{3} \right) x + \frac{-16D^3 + 36D^2 - 27D^2}{27}$$

After simplification

$$y^2 = x^3 + \frac{6D - 4D^2}{3} x + \frac{-16D^3 + 9D^2}{27} \qquad (13)$$

If we fix some value of D in equation (13) we will get the elliptic curve in weirstrass form. For Example by putting $D = -4$ we have

$$y^2 = x^3 + \frac{-88}{3} x + \frac{1168}{27} \qquad (14)$$

Which is elliptic curve in weirstrass form. Now by choosing a specific prime p and converting the coefficients of equation (14) according to the prime field F_p we get a prime elliptic curve. For example if we choose a prime 2861 and reducing the coefficients of equation (14) according to the field F_{2861} we get

$$y^2 = x^3 + 1878x + 785$$

This prime elliptic curve is used in the construction of S-box which is explained in chapter 3.

Chapter 3

Construction of S-box Using Concept of Elliptic Curves

3.1 S-box construction technique

A simple technique for generation of cryptographically strong S-boxes is discussed in this section. The construction technique is based on elliptic curve over a prime field F_p. The proposed algorithm consists of four main steps which are given below:

Step1. Choose two distinct elements a and b from prime field F_p, where p is large prime. We are selecting large p so that the corresponding elliptic curve EC has at least 256 ordered pairs. We have calculated the lower bound of p for proposed algorithm by using Hasse's Theorem which is $p > 289$.

Step2. Generate the elliptic curve $E_p(a,b)$ by using the equation:

$$y^2 = x^3 + ax + b \pmod{p}.$$

Step3. Let $E_{p,x}(a,b)$ denotes the set of *x-coordinate* of all ordered pairs of $E_p(a,b)$. Now, apply modulo 256 on $E_{p,x}(a,b)$ to get $E_{p,x}^{256}(a,b)$. This operation is used to restrict the values of $E_{p,x}(a,b)$ in the range 0-255.

Step4. Finally, an S-box S_a^b is generated by selecting first 256 distinct integers of $E_{p,x}^{256}(a,b)$.A flowchart of the proposed technique is presented in Figure 1.The proposed algorithm is implemented on $E_{2861}(1878,785)$ and S_{1878}^{785} is generated which is presented in Table 1. The points of $E_{2861}(1878,785)$ are shown in Figure 2.

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

Table 1: S-box S_{1878}^{785} generated by proposed algorithm over the EC $E_{2861}(1878,785)$

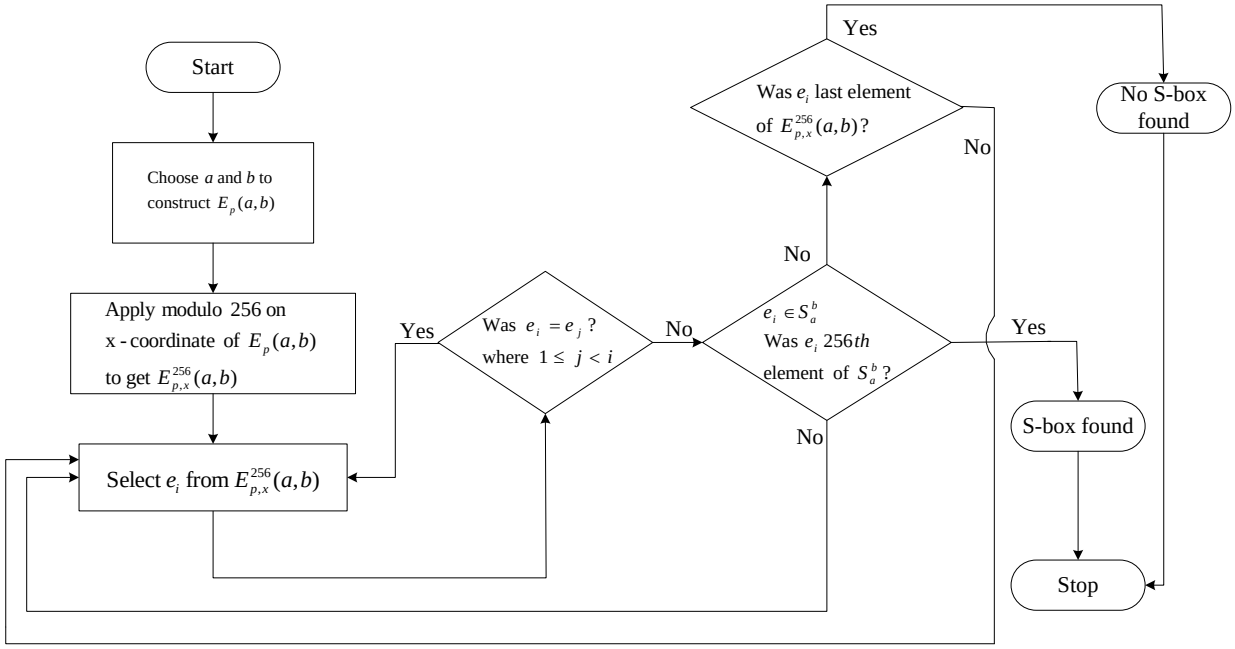


Figure 1: Flowchart of proposed technique

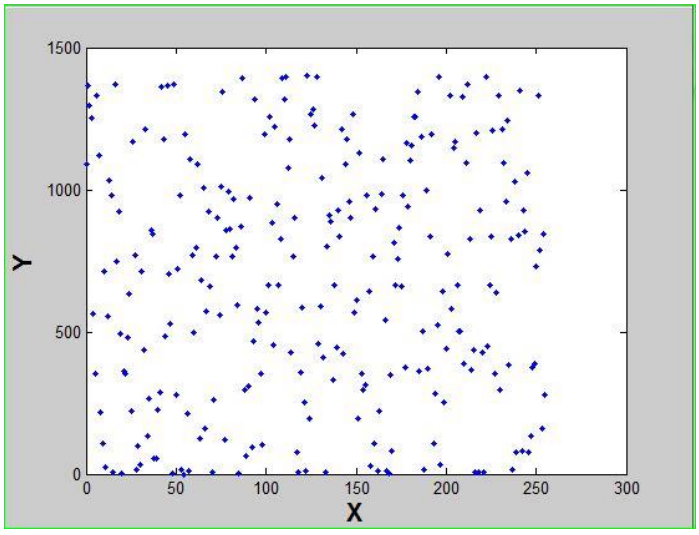


Figure 2: Points of $E_{2861,x}(1878, 785)$

3.2 Analysis and comparison

We applied security performance tests including non-linearity test, linear approximation probability, strict avalanche criterion, bit independence criterion, differential approximation probability and algebraic complexity test on the S-box S_{1878}^{785} generated by the proposed algorithm. These tests are implemented to investigate the efficiency of the proposed technique. A brief introduction to these tests and their experimental results are presented in this section. A comparison of results of S_{1878}^{785} with some of the prevailing S-boxes generated by other construction techniques is also presented in this section.

3.2.1 Bijective

The step 4 of the proposed algorithm ensures that all newly developed S-boxes are bijective.

3.2.2 Non-linearity (NL)

The concept of non-linearity is introduced in [52] to quantify the confusion creation ability of an S-box. For a given S-box $S: GF(2^8) \to GF(2^8)$, NL is measured by calculating the distance $\delta(S)$ of S to affine functions over $GF(2^8)$:

$$\delta(S) = \min_{\alpha,\, w, \beta} \#\left\{x \in GF(2^8) \middle| \alpha \cdot S(x) \neq \beta \cdot x \oplus w\right\},$$

Where $\alpha \in GF(2^8)$, $w \in GF(2)$, $\beta \in GF(2^8) \setminus \{0\}$ and "$\cdot$" denotes the dot product over $GF(2)$. The optimal value of non-linearity of a bijective S-box over $GF(2^8)$ is 120. It is also noticed in [52], that an S-box with maximum non-linearity may not satisfies other cryptographic criterion. Furthermore, the study in [52] suggests that an S-box with nearly optimal NL and satisfying other security test is of special interest. We calculated the non-linearity of the S-box S_{1878}^{785} generated by the proposed algorithm. The result of this test is 100.

3.2.3 Linear approximation probability (LAP)

In [33], linear approximation probability of an S-box is introduced. This calculates the probability of obtaining a linear approximation of a given S-box. LAP of an S-box depends upon the coincidence of input bits with output bits. The mathematical expression of LAP is given below:

$$N(a,\ \beta)=\#\left\{x\in GF(2^8)\,\middle|\,\alpha\cdot x=\beta\cdot S(x)\right\}-2^{n-1},$$
$$LAP(S)=\frac{1}{2^n}\left\{\max_{\alpha,\ \beta}\ \left|N(a,\ \beta)\right|\right\},$$

where $\alpha\in GF(2^8)$, $\beta\in GF(2^8)\setminus\{0\}$ and "$\cdot$" denotes the dot product over $GF(2)$.

We applied LAP test on S_{1878}^{785}. The LAP of S_{1878}^{785} is 0.0547.

3.2.4 Strict avalanche criterion (SAC)

This criterion is developed in [50] by combining the concepts of avalanche effect and completeness. The probability of change in output bits when a single input bit is inverted is calculated in this test. SAC of an S-box is calculated with an 8×8 dependence matrix whose entries are calculated by:

$$\left\{\frac{1}{2^n}\left[w\left(S_i(x+\alpha_j)+S_i(x)\right)\right]\middle|\,\alpha_j\in GF(2^8), w(\alpha_j)=1 \text{ and } 1\le i,\ j\le 8\right\},$$

Where $w(\alpha_j)$ is the number of non-zero bits in α_j. SAC is satisfied if all entries of dependence matrix are closer to 0.5. The SAC result S_{1878}^{785} is presented in Table 2.The minimum value of SAC is 0.4219 while its maximum value is 0.5938.

0.5312	0.5312	0.4844	0.5000	0.4687	0.4687	0.4844	0.5937
0.4531	0.4688	0.5938	0.5000	0.4844	0.5312	0.5000	0.5000

0.5469	0.5000	0.4844	0.5000	0.5156	0.5000	0.4688	0.4688
0.5469	0.4688	0.4844	0.5312	0.5000	0.5312	0.4844	0.5156
0.4844	0.4688	0.4531	0.4531	0.5156	0.4844	0.4844	0.5468
0.5312	0.5156	0.4844	0.4531	0.4375	0.4844	0.5000	0.4375
0.4688	0.5000	0.4219	0.4844	0.5156	0.5312	0.50000	0.4844
0.5625	0.5469	0.4688	0.5156	0.5938	0.4844	0.5625	0.5312

Table 2: Strict avalanche results of S_{1878}^{785}

3.2.5 Bit independence criterion (BIC)

BIC is also proposed in [50] to analyze the independence between pair of output bits when an input bit is complemented. BIC of pair of output bit A and B is calculated by finding correlation coefficient of A and B. The minimum and maximum value of BIC of S_{1878}^{785} are 0.4688 and 0.5293 respectively. The BIC results are given in Table 3.

---	0.4688	0.5098	0.5000	0.4863	0.5156	0.5176	0.4785
0.4687	---	0.5195	0.4844	0.4824	0.4902	0.4883	0.4805
0.5098	0.5195	---	0.5293	0.4805	0.5078	0.5078	0.5039
0.5000	0.4844	0.5293	---	0.4844	0.5254	0.4785	0.4785
0.4863	0.4824	0.4805	0.4844	---	0.5000	0.5195	0.4785
0.5156	0.4902	0.5078	0.5254	0.5000	---	0.5098	0.5000
0.5176	0.4883	0.5078	0.4785	0.5195	0.5098	---	0.4766
0.4785	0.4805	0.5039	0.4785	0.4785	0.5000	0.4766	---

Table 3: BIC of S_{1878}^{785}

3.2.6 Differential approximation probability (DAP)

Differential approximation probability is presented in [11] to find the probability effect of a specific difference in the input bit on the difference of the resultant output bits. The mathematical expression for DAP of an S-box S is given below:

$$DAP(S) = \max_{\Delta x, \Delta y} \left\{ \#\left\{ x \in GF(2^8) \middle| S(x+\Delta x) - S(x) = \Delta y \right\} \right\},$$

where $\Delta x, \Delta y \in GF(2^8)$. We applied DAP test on the proposed S-box and the result is given in Table 4. The DAP of S_{1878}^{785} is 0.0391.

0.0234	0.0312	0.0391	0.0312	0.0312	0.0312	0.0234	0.0312	0.0234	0.0312	0.0312	0.0234	0.0234	0.0312	0.0234	0.0312
0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0312	0.0312	0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0312	0.0312
0.0312	0.0312	0.0234	0.0234	0.0234	0.0312	0.0312	0.0234	0.0312	0.0234	0.0234	0.0312	0.0312	0.0234	0.0312	0.0234
0.0234	0.0312	0.0234	0.0234	0.0312	0.0391	0.0234	0.0156	0.0312	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234	0.0234
0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0234	0.0234	0.0156	0.0234	0.0234	0.0234	0.0312	0.0312	0.0234
0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0234
0.0234	0.0390	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0156	0.0234	0.0234	0.0234	0.0312	0.0234
0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0234	0.0312	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234
0.0234	0.0312	0.0156	0.0234	0.0234	0.0234	0.0234	0.0234	0.0312	0.0312	0.0234	0.0312	0.0234	0.0312	0.0234	0.0234

0.0 234	0.0 234	0.0 234	0.02 34	0.03 12	0.0 312	0.0 312	0.0 156	0.0 312	0.0 234	0.0 234	0.0 312	0.0 234	0.0 234	0.0 312	0.0 234
0.0 234	0.0 234	0.0 234	0.02 34	0.02 34	0.0 234	0.0 391	0.0 391	0.0 234	0.0 234	0.0 312	0.0 234	0.0 312	0.0 234	0.0 312	0.0 234
0.0 234	0.0 312	0.0 234	0.02 34	0.03 12	0.0 312	0.0 312	0.0 312	0.0 234	0.0 234	0.0 312	0.0 156	0.0 234	0.0 234	0.0 312	0.0 234
0.0 234	0.0 312	0.0 312	0.02 34	0.02 34	0.0 234	0.0 234	0.0 234	0.0 312	0.0 234	0.0 234	0.0 234	0.0 312	0.0 234	0.0 312	0.0 234
0.0 234	0.0 234	0.0 312	0.03 90	0.02 34	0.0 234	0.0 234	0.0 234	0.0 234	0.0 234	0.0 234	0.0 234	0.0 156	0.0 312	0.0 234	0.0 234
0.0 234	0.0 312	0.0 312	0.02 34	0.02 34	0.0 234	0.0 391	0.0 312	0.0 234	0.0 234	0.0 234	0.0 234	0.0 234	0.0 234	0.0 234	0.0 234
0.0 234	0.0 312	0.0 234	0.02 344	0.02 344	0.0 391	0.0 234	0.0 312	0.0 234	0.0 234	0.0 312	0.0 234	0.0 312	0.0 234	0.0 234	0.0 234

Table 4: DAP of S_{1878}^{785}

3.2.7 Algebraic Complexity (AC)

Linear polynomial for an S-box is defined in [28]. The algebraic complexity of an S-box is measured by the number of non-zero terms in its linear polynomial expression. In Table 5, coefficients of polynomial corresponding to S_{1878}^{785} are presented. The AC of S-box S_{1878}^{785} generated by the proposed algorithm is 255.

0	238	101	176	255	34	86	90	193	221	207	45	63	116	145	39
233	101	178	45	58	240	165	244	89	201	199	179	182	121	206	249
190	106	85	75	201	178	152	142	37	106	174	154	92	136	229	121
168	84	228	249	72	153	28	9	122	246	130	192	90	87	78	238
12	193	178	53	71	72	87	189	148	81	121	187	58	42	231	93
172	30	76	158	124	98	202	244	123	64	31	169	31	211	180	66

83	124	254	111	134	48	18	75	195	120	206	168	201	241	22	242
102	175	77	195	247	179	29	18	36	230	117	136	91	243	107	186
41	12	17	163	83	41	170	14	52	229	219	188	25	145	5	72
2	24	197	43	157	158	3	93	200	224	157	118	237	105	105	39
82	172	62	60	203	173	182	22	152	53	233	17	118	50	130	207
152	175	178	149	138	102	197	245	194	112	85	74	10	195	26	94
127	191	203	16	43	11	230	201	84	4	106	42	60	40	27	212
222	142	155	137	233	120	86	238	221	31	206	99	169	18	254	203
141	179	196	255	253	55	80	193	4	4	112	192	3	94	83	131
142	253	137	128	218	109	222	29	223	182	61	135	32	213	72	54

Table 5: AC of S_{1878}^{785}

The former tests are also applied on some of the well know S-boxes presented in [5, 15, 17, 20, 26, 38, 45] to compare the efficiency of proposed algorithm with other S-box generation algorithms based on different mathematical structures. The results are presented and compared in Table 6.

S-box	Bijective	NL	LAP	SAC(Max)	SAC(Min)	BIC(Max)	BIC(Min)	DAP	AC
[45]	Yes	108	0.156	0.502	0.406	0.503	0.47	0.046	255
[20]	Yes	98	0.0352	0.5781	0.4453	0.5156	0.4922	0.046	256
[15]	Yes	103	0.0352	0.5703	0.4414	0.5039	0.4961	0.0391	255
[5]	Yes	102	0.078	0.6094	0.3750	0.5215	0.4707	0.0391	254
[25]	Yes	104	0.109	0.593	0.39	0.499	0.454	0.0469	255
[38]	Yes	106	0.0469	0.5938	0.4375	0.5313	0.4648	0.0391	251
[17]	Yes	100	0.125	0.593	0.493	0.476	0.0137	0.0391	255
S_{1878}^{785}	Yes	100	0.0547	0.5937	0.4219	0.5293	0.4688	0.0391	255

Table 6: Comparison of S_{1878}^{785} with other S-boxes

Table 6 shows that the NL of S-boxes in [17& 20] is less than or equal to the NL of the S-box constructed by the proposed algorithm. The LAP of S_{1878}^{785} is less than that of the S-boxes presented in [5, 17, 26, 45]. This fact reveals that the S_{1878}^{785} creates high confusion in the data and hence higher resistance against linear attack [33] as compared to [5, 17, 26, 45]. The SAC and BIC results of S_{1878}^{785} and other S-boxes used in Table 6 are almost the same. Thus, the S-box generated by the proposed technique and S-boxes presented in Table 6 create diffusion in the data of equal magnitude. The DAP of S_{1878}^{785} is less than or equal to the DAP of S-boxes [5, 15, 17, 20, 26, 38, 45]. Thus, proposed encryption technique generates S-box high resistance against differential cryptanalysis [11] as compared to the others. The AC of S_{1878}^{785} is maximum which shows that it is secure against algebraic attacks [7, 39, 47].

3.3 Conclusion:

A novel S-box construction technique is presented in this thesis. The proposed algorithm uses the x*-coordinate* of ordered pairs of an elliptic curve $E_p(a,b)$ over prime field F_p for the generation of cryptographically strong S-box S_b^a, where p is a prime greater than 289, a and b belong to finite field F_p. Several tests are applied on newly developed S-box S_b^a to analyze its cryptographic strength. Furthermore, cryptographic properties of S_b^a are compared with some of the existing prevailing S-boxes. Experimental results showed that the proposed algorithm is capable of generating S-boxes with high resistance against linear, differential and algebraic attacks. The S-box generated by the proposed technique depends upon the selection of p, a and b. In other words, by changing either p, a or b, we will get another S-box.

Bibliography:

[1] Amara M and Siad A, Elliptic Curve Cryptography and its Applications, 7th International Workshop on Systems, Signal Processing and their Applications, pp. 247–250, May (2011).

[2] Brown DRL. SEC 1: Elliptic Curve Cryptography. Certicom Corp (2009).

[3] Bustamante MD, Hayat U. Complete classification of discrete resonant Rossby/drift wave triads on periodic domains. Commun. Nonlinear Sci. Numer. Simulat. 18 (2013) 2402-2419.

[4] Caragiu M, Johns RA, Gieseler J, Quasi-random structures from elliptic curves. J.Algebra, Number Theory Appl. 6, 561–571, 2006.

[5] Chaos G, A novel heuristic method for obtaining S-boxes, Chaos, Solitons and Fractals 36 (2008) 1028–1036.

[6] Chiristof P. Understanding Cryptography "A Textbook for Students and Practitionars."

[7] Courtois NT and Josef P, Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, ASIACRYPT 2002, LNCS 2501, pp. 267–287, 2002.

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

[9] Daemen J and Rijmen V, AES Proposal: Rijndael (Version 2). NIST AES website csrc.nist.gov/encryption/aes, 1999.

[10] Daemen J and Rijmen V. The Design of RIJNDAEL: AES the Advanced Encryption Standard. Springer- Verlag: Berlin, 2002.

[11] Eli Biham Adi Shamir, Differential Crypt analysis of DES-like Cryptosystems, Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 2-21, 1991.

[12] Farashahi RR, Schoenmakers B, Sidorenko A. Efficient pseudorandom generators based on the DDH assumption. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 426–441. Springer, Heidelberg (2007).

[13] Ferguson N, Schroeppel R, Whiting D. A simple algebraic representation of Rijndael. In Selected Areas in Cryptography SAC01, LNCS2259, 2001; 103–111.

[14] Gong G, Berson TA, Stinson DR. Elliptic curve pseudorandom sequence generators. Selected areas in cryptography (Kingston, ON, 1999), pages 34-48. Springer, Berlin, 2000.

[15] Guoping T, Xiaofeng L, Yong C, A novel method for designing S-boxes based on chaotic maps, Chaos, Solitons and Fractals 23 (2005) 413–419.

[16] Hao Y, Longyan L, Yong W, An S-box Construction Algorithm based on Spatiotemporal Chaos, 2010 International Conference on Communications and Mobile Computing.

[17] Hussain I, Shah T, Gondal MA, Khan WA, Mehmood H. A group theoretic approach to construct cryptographically strong substitution boxes. Neural Computing and Applications 2012.doi:10.1007/s00521-012-0914-5.

[18] Hussain I, Azam NA, Shah T. Stego optical encryption based on chaotic S-box transformation. Optics and Laser Technology 2014; 61:50–56.

[19] Hussain I, Azam NA, Shah T, Stego optical encryption based on chaotic S-box transformation, Optics & Laser Technology 61 (2014) 50–56.

[20] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers. IEEE Trans Circuits Syst–I 48 (2001) 163–70.

[21] Jakobsen T, Knudsen LR. The interpolation attack on block ciphers. In Fast Software

Encryption, LNCS 1267, 1997; 28–40.

[22] Jung HC, Seongtaek C and Choonsik P, S-boxes with Controllable Nonlinearity, EUROCRYPT'99, LNCS 1592, pp. 286{294, 1999.

[23] Khan M, Azam NA. Right translated AES Gray S-box, Security and Network Communication, 2014, doi:10. 1002/sec.1110.

[24] Khan M, Azam NA. S-boxes based on Affine mapping and orbit of power function, 3 D Research 2015, 10.1007/s13319-015-0043-x.

[25] Khan M, Shah T, Syeda IB, Construction of S-box based on chaotic Boolean functions and its application in image encryption, Neural Comput&Applic (2016) 27:677–685 DOI 10.1007/s00521-015-1887-y.

[26] Kim J, Phan RCW. Advanced differential-style cryptanalysis of the NSA's skipjack block cipher, Cryptologia 33(2009) 246–270.

[27] Kumar D, Suneetha C and Chandrasekhar A. present an algorithem for encryption of data using elliptic curve in International Journal of Distributed and Parallel Systems(IJDPS) Vol.3,NO.1, January 2012.

[28] Lidl R, Niederreiter H. Introduction to Finite Fields and their Applications (2nd edn.). Cambridge University Press: Cambridge, England, 1994.

[29] Liu J, Wai B, Cheng X, Wang X. An AES S-box to increase complexity and cryptographic analysis. Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Taiwan, 2005; 724–728.

[30] Maurer UM., Wolf S. The Diffie–Hellman Protocol. In "Towards a Quarter-Century of Public Key. Cryptography", Kluwer Academic Publishers, pp. 147–171, Boston (2000).

[31] Menezes, A.; Oorschot, P. van; Vanstone, S. Handbook of Applied Cryptography (5th ed.).

[32] Miller V, "Uses of elliptic curves in cryptography," *Advances in Cryptology–Crypto'85*, pp. 417-426, 1986.

[33] Mitsuru M, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 386-397, 1994.

[34] Murphy S and Robshaw MJ. Comments on the security of the AES and the XSL technique. Electronics Letters 2003; 39:26–38.

[35] Murphy S and Robshaw MJ. Essential algebraic structure within the AES. Proceedings of the 22th Annual International Cryptology, Springer-Verlag, 2002; 1–16.

[36] Neal K, Alfred M and Scott V, The State of Elliptic Curve Cryptography, Designs, Codes and Cryptography, vol. 19, issue 2–3, pp. 173–193, (2000).

[37] Neal K, Elliptic Curve Cryptosystems, Mathematics of Computation, vol. 48, issue 177, pp. 203–209, January (1987).

[38] Neural YW, Li Y, Min L and Sihong S, A method for designing S-box based on chaotic neural network, 2010 Sixth International Conference on Natural Computation (ICNC 2010).

[39] Nicolas C, Alexander K, Jacques P and Adi S, Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations, International Conference on the Theory and Application of Cryptographic Techniques EUROCRYPT 2000: Advances in Cryptology-EUROCRYPT 2000 pp 392-407.

[40] Omar R and Zbigniew K, On Pseudo-Random Number Generators Using Elliptic Curves and Chaotic Systems, Appl. Math. Inf. Sci. 9, No. 1, 31-38 (2015).

[41] Rivest and Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical Computer Science. **1**. Elsevier.

[42] Rosenthal J. A polynomial description of the Rijndael Advanced Encryption Standard. Journal of Algebra and its Applications 2003; 2:223–236.

[43] Scott A. Vansfone, Elliptic Curve Cryptography. The Answer to Strong, Fast Public-Key Cryptography for Securing Constrained Environments, Information Security Technical Report, vol. 2, no. 2, pp. 78–87, (1997).

[44] Shannon CE 'Communications Theory of Secrecy Systems", Bell Sys. Tech.Journal.Vol. 20.pp.656-715. 1949.

[45] Shi XY, Xiao H, You XC and Lam KY. A method for obtaining cryptographically strong

8 × 8 S-boxes. International Conference on Information Network and Application 1997; 2:689–693.

[46] Stinson D.R. Cryptography Theory And Practice. 3th edition, Chapman & Hall/CRC, New York (2006).

[47] Thomas J and Lars RK, The Interpolation Attack on Block Ciphers, International Workshop on Fast Software Encryption (FSE) 1997: Fast Software Encryption pp 28-40.

[48] Tran MT, Bui DK and Doung AD. Gray S-box for advanced encryption standard. International Conference on Computational Intelligence and Security 2008; 1:253–258.

[49] Wang Y, Wong KW, Li C and Li Y. A novel method to design S-box based on chaotic map and genetic algorithm. Physics Letters A 2012; 376:827–833.

[50] Webster AF and Tavares SE, ON THE DESIGN OF S-BOXES, Advances in Cryptology - CRYPT0 '85, LNCS 218, pp. 523-534, 1986.

[51] Williams S, Cryptography and Network Security, Prentice Hall, 4th Edition, (2000).

[52] Willi M and Othmar S, Nonlinearity Criteria For Cryptographic Functions, Advances in Cryptology - EUROCRYPT ‘89, LNCS 434, pp. 549-562, 1990.

[53] Yong W, Kwok-WoW , Changbing L and Yang L, A novel method to design S-box based on chaotic map and genetic algorithm, Physics Letters A 376 (2012) 827–833.