CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

A New Generalized Signcryption Scheme Based on Elliptic Curves

by

Sakina Syed

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

in the

Faculty of Computing
Department of Mathematics

2023

Dedicated to My Father and Mother(Late)

CERTIFICATE OF APPROVAL

A New Generalized Signcryption Scheme Based on Elliptic Curves

by

Sakina Syed

(MMT213015)

THESIS EXAMINING COMMITTEE

S.No	Examiner	Name	Organization
(a)	External Examiner	Dr. Shabieh Farwa	COMSATS, Wah cantt
(b)	Internal Examiner	Dr. Muhammad Afzal	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
December, 2023

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
December, 2023

Dr. M. Abdul Qadir
Dean
Faculty of Computing
December, 2023

Author's Declaration

I, **Sakina Syed** hereby state that my MPhil thesis titled "**A New Generalized Signcryption Scheme Based on Elliptic Curves**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MPhil Degree.

(Sakina Syed)

Registration No:MMT213015

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A New Generalized Signcryption Scheme Based on Elliptic Curves**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MPhil Degree, the University reserves the right to withdraw/revoke my MPhil degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Sakina Syed)

Registration No:MMT213015

Acknowledgement

On completion of my research project, I would like to thank all those people who made this thesis possible and an unforgettable experience for me. Foremost, I would like to acknowledge and give my warmest thanks to my supervisor **Dr. Rashid Ali** who made this work possible. His guidance and advice carried me through all the stages of writing my thesis. I am very thankful for his patience, motivation, enthusiasm, continuous advice and encouragement throughout the course of this thesis. Beside this, I would also like to express my appreciation to the head of the Mathematics department **Dr. Muhammad Sagheer**. His commitment to providing a conducive and innovative learning environment has enriched my academic experience significantly. However, the most profound gratitude goes to my family, who have been my pillars of strength.

This thesis is dedicated from the depths of my heart to my beloved mother(Late) and father.

In closing, I offer my sincere gratitude to all those mentioned above and to the Almighty God for the blessings and opportunities that have brought me to this moment. May His blessings continue to enrich the lives of all who have contributed to this journey, and may our collective endeavors continue to bear fruit in the pursuit of knowledge and understanding.

(Sakina Syed)

Registration No:MMT213015

Abstract

In the field of cryptography, signcryption is a modren technique that performs the digital signatures and provides the security requirements of encryption in single logical step. This new technique helps to reduce the computational cost and it is more efficient as compared to other signature-then-encryption techniques. Previously, many signcryption schemes were introduced and each of them provides different level of security attributes like, confidentiality, authentication, integrity, non-repudiation, authentication, unforgeability and forward secrecy. In this thesis we first reviewe the recently proposed signcryption scheme based on elliptic curve, then it is extended to new generalized signcryption scheme based on elliptic curve. The proposed scheme provides some extra features, it has felexibilty to perform signatures only or encryption only. Due to rapid increase in cryptographic attacks, security of the cryptographic scheme is essential requirement. Our proposed scheme provides the high level of resistance againts the cryptographic attacks. The security analysis and cost analysis of the proposed scheme is also presented to show the efficiency of the scheme when user has to work with a single mode.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advanced Encryption Standard
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDH	ECDH Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GSC	Generalized Signcryption
GCD	Greatest Common Divisor
S− DES	Simplified Data Encryption Standard
IFP	Integer Factorization Problem
PKC	Public Key Cryptography

Symbols

C	Ciphertext Message
K^*	Session key of both sender and receiver
H	One Way Hash Function
M	Plaintext Message
G	Base Point of Elliptic Curve
$\mathcal{O}$	Point at Infinity
q	Large Prime Number
$\mathbb{F}$	Finite Field
$\mathbb{Z}$	Set of Integers
$\mathbb{R}$	Set of Real Numbers
$\mathbb{C}$	Set of Complex Numbers

Chapter 1

Introduction

In this chapter, we will discuss the development and improvement in the field of cryptography. Also present our modification and contribution.

The term "cryptography" is the combination of two Greek words kryptos and graphein which imply secret and writing respectively. Cryptography [1] is the science which deals with the study of secret communication, generating and breaking secret codes. It also deals with the study of cryptanalysis and cryptology. Cryptanalysis is an art of breaking secret codes and secret communication even without having any secret key. The first examples of cryptography may be found in the ancient worlds of Greece, Rome, and Egypt. Latest cryptography not only has confidentiality of data and information but also deals the security attributes of integrity, authentication, unforgeability, non-repudiation, public verification and forward secrecy. Cryptography now a day is extremely used in many fields and aspects of human life for example, e-commerce, online voting system, online cash payment system, digital signature, smart phones, ATM machines, credit cards, transaction of money through digital apps in banks [2]. There are two main branches of cryptography namely, the "Private (symmetric) Key Cryptography" and the "Public (asymmetric) Key Cryptography".

In symmetric key cryptography, we only use one key for both encryption and decryption while in asymmetric key cryptography, we use two different related keys where one is known as secret key or private key and other is public key.

The cryptographic schemes which are based on symmetric key cryptography are DES[3], Tripple DES [4], AES [5]. The cryptographic schemes which are based on asymmetric key cryptography are Elliptic curve cryptography [6], ELGamal [7] and RSA [8].

In cryptographic field ECC [6] and RSA [8] are widely used because of its smaller key size with strong security. Because of this benefit (ECC) [6] has less storage requirements and provides more secure encryption as compared to RSA [8]. The basic tools on which cryptography is based are digital signatures and encryption that provides confidentiality, authentication, and integrity. In order to have both confidentiality and authentication of single message or document, the traditional appraoch was signature-then-encryption technique. In this approach the task is performed in such a manner that first apply a digital signature on a document and then encrypt the document for transmission over an unsecured network. The main disadvantage of this technique was, it has more computational cost and less efficient. In 1997, Zheng [9] proposed a new cryptographic technique named as "Signcryption" scheme. It combines the function of digital signature and encryption in one step. This new proposed scheme (signcryption) has decreased the computatoinal cost and increased the efficiency of scheme as compared to signature-then-encryption. In modren cryptographic fields EEC based signcryption scheme are widely used because of their security, low computational cost, less storage requirements and more efficiency. Signcryption schemes provides the following security attributes.

- Confidentiality
- Authentication
- Non repudiation
- Integrity
- Unforgeability

Forward secrecy and availibilty are two more security attributes depending on the requirements of the user.

There are different varients of signcryption, including blind signcryption, certificateless signcryption, generalized signcryption. Blind signcryption is used to shield the sender's identity and privacy from other users, particularly in electronic currency payment and voting systems. Certificateless signcryption is a variation of ID-based signcryption. Mostly Certificate authority and key generation center are based on certificateless signcryption. Generalized signcryption is an extension of signcryption. There are three modes of generalized signcrytption. One is signature only mode, encryption only mode, and signcrytption mode.

Security attacks on cryptographic algorithm are increasing day by day. There are some attacks that concern with cryptosystem.

- Known Plaintext Attack
- Man in the Middle Attack
- Choosen Plaintext Attack
- Forgery Attack
- Cipheretext Only Attack

1.1 Literature review

In 1985 Koblitz [10] proposed Elliptic curve cryptography. Zheng [9] proposed a new cryptographic scheme in 1997 named "signcryption". This scheme performed both digital signatures and encryption in one logical single step. It has less computational cost and more efficient. It is the scheme which is replaced by Signature-then-Encryption scheme. Zheng and Imai [11] applied ECC in signcryption scheme and proposed a new scheme which is based on elliptic curve cryptography. This scheme is more secure because its security is dependent on ECDLP [12], where ECDLP is more secure and unbreakable in modern cryptography. It has approximately 58% computational cost and 40% communication cost. Later on Bao and Deng [13] gave extension and modification to Zheng's scheme.

Because they thought that Zheng's scheme does not provides the authenticity without secret key of the sender. So, the scheme improved by Bao and Deng [13] provides the authenticity without using secret key of sender or in other words a receiver can verify the signature without secret key of sender. After this, Gamage [14] proposed the signcryption scheme which provides the authenticity to anyone to verify the sender's signature but this facility was only available in firewalls. Jung [15] pointed out that Zheng's signcryption scheme does not provides a forward secrecy. In 2005 Hwang et al [16] proposed elliptic curve discreate logrithm problem (ECDLP), also proposed elliptic curve Diffie Helman problem (ECDHP) [17] which is based on signcryption scheme with addtional feature of forward secrecy and public verification. In general, confidentiality, integrity, authentication, unforgeability, non-repudiation, forward secrecy, and public verification are compared in terms of security attributes. For more different varients of signcryption we suggested [19–21]. In 2006 a new cryptographic signcryption scheme was proposed by Han and Yang [22] named "Generalized Signcryption (GSC)". After this Wang [23] provides the security attributes of the generalized signcryption. In 2010, Yu et al [24] proposed an identity-based GSC system and a security model. Kush-wah and Lal simplified the system's security model [23] and recommended a more powerful GSC identity-based system in 2011. In the traditional model, Wei et al [25] proposed an identity-based GSC scheme and in 2015, he proposed extension for big data protection. In 2016, Zhou et al [26] provides extension of GSC, and presented two new schemes named as, generalized proxy signcryption and generalized signcryption and suggested a concrete scheme. Farshim et al [27] proposed a certificateless lightweight certification.

1.2 Thesis Contribution

In this thesis we extended the ECC based signcryption scheme of Zhang et al [28] into new Gerneralized Signcryption. This scheme [28] based on elliptic curves for secure and authenticated message transmission, which provides both digital signature and encryption with less computaional cost as compared to Signature-than-

Encryption scheme. This scheme provides the security because its security based on the ECDLP and ECDHP, which are more secure currently. The scheme provides integrity, message confidentiality, forward secrecy, availibilty, unforgeability, verification, and non-repudiation security attributes. The computational time of this scheme is little bit higher than the Zheng and Imai scheme [11] and Zhang et al [28] scheme but it is more secure. Our proposed scheme provides double functions when we required both confidentiality and authenticity seperatly performs a single function without any additional calculations . The proposed scheme provides all the security attributes and it is uneffected by various known attacks.

1.3 Thesis layout

- In Chapter 1, introduction, comprehensive literature of cryptography, elliptic curve cryptography, signcryption, generlized signcryption and cryptananlysis is presented.
- In Chapter 2, mathematical and cryptographic background is presented.
- In Chapter 3, Zhang et al [28] proposed scheme is reviewed also presented its scheme and its security analysis.
- In Chapter 4, we modified Zhang et al [28] proposed scheme and presented its generalized signcryption scheme.
- In Chapter 5, security analysis of proposed generalized signcryption scheme is presented and comparison of its cost analysis with existing cryptographic schemes.
- In Chapter 6, conculsion as well as future work of the modified scheme is presented .

Chapter 2

Preliminaries

The fields of number theory and algebra play a vital role in the development of cryptography. In this chapter we will present some basic definitions from number theory and algebra. Also present the contribution of mathematical background in the field of cryptography. In order for the readers to have a thorough understanding of cryptographic field, some basic definitions and tools from cryptographic background will be presented.

2.1 Mathematical Background

Definition 2.1.1.

"A group $\mathbb{G}$ is a non empty set denoted by pair $(\mathbb{G}, *)$ under binary operation $*$ on $\mathbb{G}$ satisfies the following axioms.

1. **Closure:** If the elements $s, t \in \mathbb{G}$, then $s * t$ is also in $\mathbb{G}$.
2. **Associativity:** $s * (t * u) = (s * t) * u$ for all s, t, u in $\mathbb{G}$.
3. **Identity element:** An element e in $\mathbb{G}$ such that $s * e = e * s = s$ for all s in $\mathbb{G}$ where e is the identity element of $\mathbb{G}$.

4. **Inverse element:** For s in $\mathbb{G}$ there is an element $s^{'}$ in $\mathbb{G}$ such that $s * s^{'} = s^{'} * s = e$. A group $\mathbb{G}$ is called Abelian if it satisfies the following additional property $s * t = t * s$ for all s, t in $\mathbb{G}$" [1].

Definition 2.1.2.

$\mathbb{G}$ is a cyclic group if every element of $\mathbb{G}$ is a power s^k (k is an integer) of a fixed element s in $\mathbb{G}$. The element s is said to generate the group $\mathbb{G}$ [1].

Example 2.1.3. Here are some examples of a group and a cyclic group.

1. Set of real numbers $\mathbb{R}$, set of complex numbers $\mathbb{C}$, set of intergers $\mathbb{Z}$ all are group under binary operation + and also known as abelian group.

2. A set $X = \{1, -1, i, -i\}$ is cyclic group under addition where $-i$ or i is the generating element of group X.

Definition 2.1.4.

"A nonempty set $(\mathbb{F}, +, *)$ together with binary operations '$+$' and '$*$' is called a field $\mathbb{F}$, if the following properties hold:

1. $\mathbb{F}$ is abelian under addition.

2. The non zero elements of $\mathbb{F}$ form an abelian group under multiplication .

3. Multiplication is distributed over addition in $\mathbb{F}$" [29].

Example 2.1.5. Here are examples of field.

1. "Set of complex numbers $\mathbb{C}$ and set of real numbers $\mathbb{R}$ are field.

2. Set of integers $\mathbb{Z}$ is not a field, because inverses of all integers except 1 and -1 do not exist".

Definition 2.1.6.

Galois field is a field that consists of a finite number of elements. Galois fields are either prime fields or prime power fields. The set of integers under $\mod p$ denoted by $\mathbb{Z}_p$ is field. Galois field or finite field was first introduced by "Evariste Galois" in 1905 [30].

Example 2.1.7. Suppose, we have Galois field $GF(7)$ which has 7 elements only $\{0, 1, \ldots 6\}$. The addition and multiplication operation in this field are performed under modulo 7 which means that result of any operation will always be less than 7.

$$8 + 3 \equiv 4 \mod 7$$

also

$$8 * 3 \equiv 3 \mod 7$$

Definition 2.1.8.

"Ring denoted by $(R, +, *)$ is a set of elements together with two binary operations addition $+$ and multiplication $*$ that satisfies the following properties:

1. $(R, +)$ is an abelian group.
2. $(R, *)$ is associative.
3. $(*)$ is distributive with respect to $+$, i.e. for all $a, b, c \in R$
4. Left and right distributive laws hold in $\mathbb{R}$

   i.e. $a * (b + c) = ab + ac, (b + c)a = ba + ca$"" [31].

Example 2.1.9. Following are the examples of rings.

"Set of integers $\mathbb{Z}$ under usual addition $+$ and multiplication $*$ is a ring.

Let $Z_v = \{0, 1, 2 \ldots v - 1\}$ and $v > 0$ and $v \in \mathbb{Z}^+$ is a ring under addition and multiplication modulo v" [31].

Theorem 2.1.10.

"Fermat's theorem states that, if p is prime and a is a positive integer not divisible by p then $a^{p-1} - 1 \equiv 0 \mod p$" [1].

Definition 2.1.11.

"Given $x, y \in Z_p$ such that $x^n = y \mod p$ then finding n is known as discrete logarithm problem" [32].

Definition 2.1.12.

When given composite number $N = x_1 * y_1$ then decomposition of an integer N or findind integers x_1 and y_1 is complicated, this complexity is known as integer factorization problem (IFP). It is an earlier problem. This provides the fundamental building block for many cryptographic methods, including RSA encryption system.

Division Algorithm

Suppose we have two integers s and t then there exsist two unique integers q_1 and r_1 such that;

$$s = q_1 t + r_1$$

Here q_1 is quotient and $0 \leqslant r_1 < t$ is remainder. If $r_1 = 0$ then t divides s.

Definition 2.1.13.

Finding multiplicative inverse of an integers is easy in a small field. We construct a Caleys table to obtain the multiplicative inverses of integers. But multiplicative inverse of any integer $u \in \mathbb{F} \mod m$ is possible if $\gcd(u, m) = 1$ otherwise it is not possible. In the section below the Extented Euclidean algorithm to compute the inverses of integers is given.

Algorithm 2.1.14.

To compute the greatest common divisor, one should repeating the process of division algorithm again and again. This process is known as Euclidean Algorithm.

To calculate the gcd of the integers ℓ and m, we will perform the following steps.

Input: Two integers ℓ and m

Output: gcd(ℓ,m)

1. If we have $\ell = 0$ then $\gcd(\ell, m) = m$, since $\gcd(0, m) = m$ and stop.
2. If $m = 0$ then $\gcd(\ell, m) = m$, since $\gcd(\ell, 0) = m$ and stop.
3. Write $\ell = Q * m + r$ where Q is quotient and r is reminder.
4. Find $\gcd(m, r)$, since $\gcd(\ell, m) = \gcd(m, r)$ [1]

Algorithm 2.1.15.

The above algorithm is transferred as follows and compute modular inverse of integers ℓ and m.

Input: Two integers ℓ and m

Output: gcd(ℓ,m)

1. "Set $(\ell_1, \ell_2, \ell_3) = (1, 0, m)$ and $(m_1, m_2, m_3) = (0, 1, b)$
2. If $m_3 = 0$ then returns $\ell_3 = \gcd(m, b)$ no inverse of element b exist.
3. Now check if $m_3 = 1$ then return $m_3 = \gcd(m, b)$ $B_2 = b^{-1} \mod m$
4. Now divide ℓ_3 and m_3 set the quotient $Q = \ell_3$ div m_3
5. Now let we take (n_1,n_2, n_3) = ($\ell_1 - Q * m_1$, $\ell_2 - Q * m_2$, $\ell_3 - Q * m_3$)
6. Set $(\ell_1, \ell_2, \ell_3) = (m_1, m_2, m_3)$
7. Set $(m_1, m_2, m_3) = (n_1, n_2, n_3)$
8. Go to step number 2".

2.2 Elliptic Curve over $\mathbb{F}_p$

The equation of the form with additional point $\mathcal{O}$ at infinity.

$$E : y^2 = x^3 + ax + b \mod p \tag{2.1}$$

select integers a and b from finite field $\mathbb{F}_p$. If the discriminant $4a^3 - 27b^2 \neq 0$ then curve is said to be smooth and this curve is known as an Elliptic curve.

The Elliptic curve $E_p(a, b)$ is based on all those points which statisfy the equation (2.1). The elements of $E_p(a, b)$ also form a cyclic group and generated by base point G. A small non negative integer n is known as order of G such that $nG{=}\mathcal{O}$ or infinity. Suppose we have an elliptic equation and its graphical representation is shown in the figure below

$$y^2 = x^3 + 0x - 4 \mod 251$$

Figure 2.1 illustrates the elliptic curve points of elliptic equation

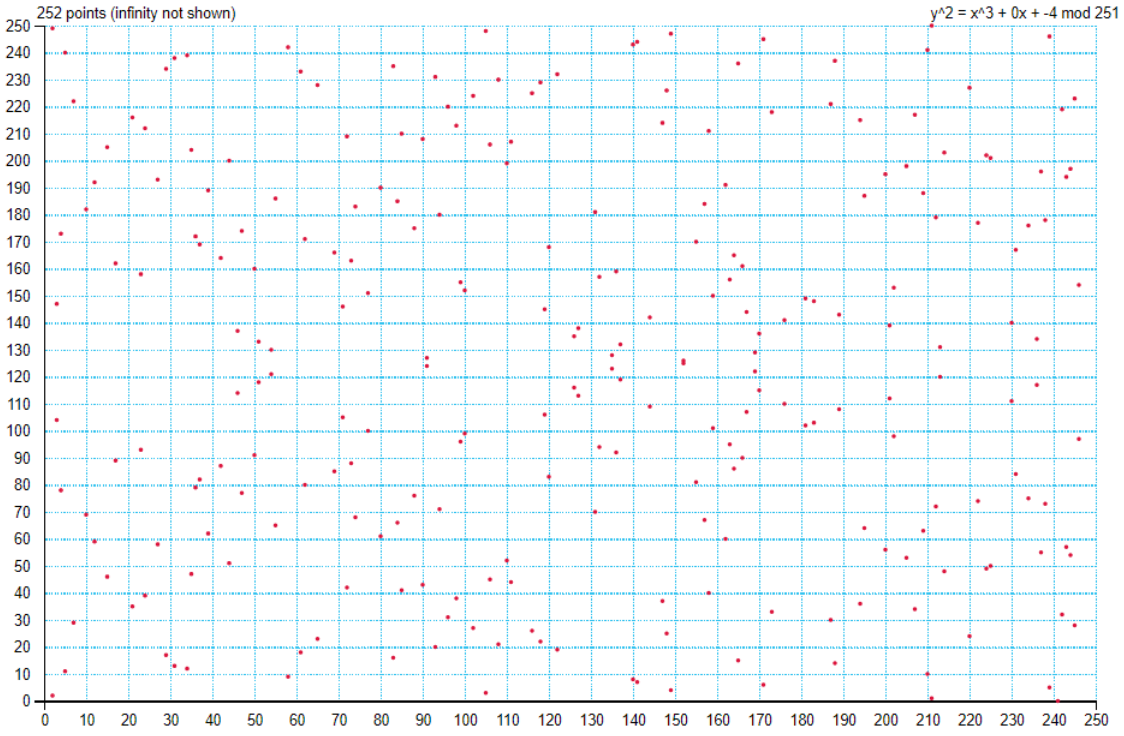


FIGURE 2.1: Elliptic curve over $E_{251}(0, -4)$

Point Addition

Suppose we have two points, $P(x_1, y_1)$ and $Q(x_2, y_2)$, on an elliptic curve E. The addition of P and Q is $R(x_3, y_3)$ as shown in Figure 2.2

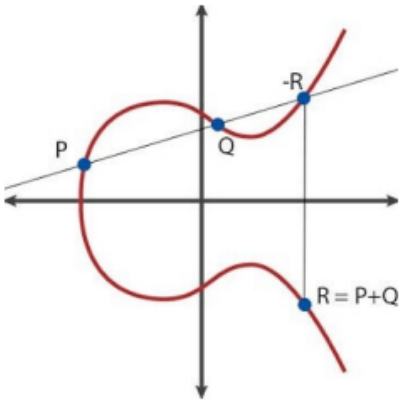


FIGURE 2.2: Elliptic Curve Point Addition

The following steps must be followed in order to add such points.

1. A straight line is passed from points P and Q of elliptic curve E .
2. At any third point, the straight line intersects the curve, say at R of elliptic curve E.
3. The addition of P and Q is negative to third point $-R$.

Let the sum of the points P and Q is $R(x_3, y_3)$ where the coordinates x_3 and y_3 are given as

$$x_3 = m^2 - x_1 - x_2 \mod p.$$
$$y_3 = m(x_1 - x_3) - y_1 \mod p.$$

Here

$$m = \frac{y_2 - y_1}{x_2 - x_1} \mod p.$$

Point Doubling

Now we explain the point doubling operation on elliptic curve. Suppose we have point $P(x_1, x_2)$ on elliptic curve E. To add a point P to itself as $P + P = 2P$, we perform the following actions:

1. Draw a tangent at point $P(x_1, y_1)$ which intersects the curve at the second point of elliptic curve E.

2. The next step is to simply take S which is negative of second point and it is used as the point doubling.

The coordinates of point doubling are calculated as $S = 2P = (x_2, y_2)$

$$x_2 = m^2 - 2x_1.$$
$$y_2 = m(x_1 - x_2) - y_1.$$

Where,

$$m = \frac{3x_1^2 + a}{2y_1}.$$

Point at Infinity

The similar approach can be applied to the addition of P to $-P$. We are aware that $-P$ is effectively an extension of P. So, as a straight line departs from them, it gets closer to infinity. To identify a specific infinity-bound point that is known as a point towards infinity and is denoted by $\mathcal{O}$.

Example 2.2.1. Let us consider the curve over $\mathbb{F}_{11}$, that is,

$$y = x^3 + x + 6 \mod 11.$$

For elliptic curve points addition on $E_{11}(1, 6)$ let $P(3, 5)$ and $Q(7, 9)$ are any two points on elliptic curve E, then formula provide us new points $R(x_3, y_3)$ as shown in Table 2.1. Calculate slope s by

$$\begin{aligned} s &= \frac{9-5}{7-3} \mod 11. \\ &= \frac{4}{4} \Rightarrow 1 \mod 11. \\ s &= 1 \mod 11. \end{aligned}$$

TABLE 2.1: Points on Elliptic Curve

x	y^2	y_1	y_2	$P(x,y)$	$Q(x,y)$
0	6	–	–	–	–
1	8	–	–	–	–
2	5	4	7	(2,4)	(2,7)
3	3	5	6	(3,5)	(3,6)
4	8	–	–	–	–
5	4	2	9	(5,2)	(5,9)
6	8	–	–	–	–
7	4	2	9	(7,2)	(7,9)
8	9	3	8	(8,3)	(8,8)
9	7	–	–	–	–
10	4	2	9	(10,2)	(10,9)

$$x_3 = s^2 - x_1 - x_2. \tag{2.2}$$

Put value of s in Equation 2.2

$$y_3 = s(x_1 - x_3) - y_1. \tag{2.3}$$

$$\begin{aligned} x_3 &= 1^2 - 3 - 7 \mod 11. \\ &= -9 \mod 11. \\ x_3 &= 2 \mod 11. \end{aligned}$$

Put the value of x_1 and x_3 in Equation 2.3

$$\begin{aligned} y_3 &= 1(3-2) - 5 \mod 11. \\ y_3 &= -4 \mod 11. \\ y_3 &= 7 \mod 11. \end{aligned}$$

So, $R(x_3, y_3) = (2, 7)$ is the addition of points. Now let us add a point $P(3, 5)$ into itself.

$$\begin{aligned} s =& \frac{3x^2 + a}{2y_1} \Rightarrow \frac{3(3^2) + 1}{2(5)} \mod 11. \\ =& \frac{3(9) + 1}{10} \mod 11. \\ =& \frac{14}{5} \mod 11. \\ =& 14(5)^{-1} \mod 11. \\ =& 14(6) \mod 11. \\ s =& 7 \mod 11. \end{aligned}$$

Now use values of s

$$\begin{aligned} x_3 =& s^2 - 2x_1. \\ x_3 =& 7^2 - 2(3) \mod 11. \\ =& 49 - 6 \mod 11. \\ =& 43 \mod 11. \\ x_3 =& 10 \mod 11. \\ y_3 =& 7(3 - 10) - 5. \\ y_3 =& 7(-7) - 5. \\ =& -49 - 5 \mod 11. \\ y_3 =& 10 \mod 11. \end{aligned}$$

So we have

$$2P = (10, 10)$$

2.3 Cryptographic Background

The field of cryptology known as cryptography involves the safe transmission of information such that it cannot be read or altered by a third party. The original

message is transformed by the sender. Cryptography focuses on building and analyzing such procedures that keep the general public or outsiders from reading private messages. It involves the use of mathematical and computational methods to transform information into a form that is unintelligible to unauthorized users, and then back into its original form for authorized users. **Types of cryptography**

There are two types of cryptographic scheme.

1. Cryptography with Symmetric key
2. Cryptography with Asymmetric key

2.3.1 Cryptography with Symmetric key

Private key cryptography is another name for a symmetric key encryption. Usually, it uses a key that you can trade with a reliable third party. In early crytographic schemes, it was the only method of message transmission. In cryptography with symmetric key same key is used for both encryption and decryption. The main benifit of this cryptographic scheme was fastest and simple communication but disadvantage of this scheme was it relies on each participent that involves in communication to keep the keys confidential. The well defined examples of this scheme are DES [3], AES [5]. A symmetric key cryptography model [1] is shown in Figure 2.3.

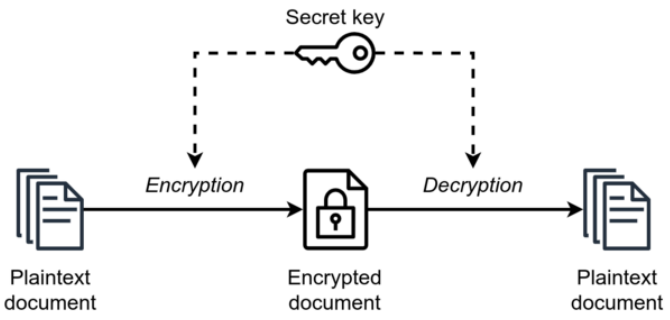


FIGURE 2.3: Symmetric Encryption Model

There are some drawbacks of symmetric key cryptography.

- **Key sharing:** The issue with key distribution arises when n people are conversing with each other. The integrity of the entire communication will be harmed if one individual reveals the key.
- **Authentication:** One of the primary issues is authentication. If Ayeza and Babar interact, how can Ayeza establish that Babar sent the message and vice versa.

2.3.2 Cryptography with Asymmetric Key

Diffie and Martin Hellman [33] introduced the public key cryptography in 1976. They proposed a new mechanism which is based on two different keys.

1. Publick Key
2. Private Key

Where public key is known to everybody, while private key is kept secret, it is also known as secret key. This scheme is known as Asymmetric key cryptography. The main advantage of this scheme is to overcome the key sharing issues and disadvantage of this scheme is complex and slow computations. The examples of cryptography with public key or Asymmetric key cryptography are Elliptic curve cryptography [6], EL-Gamal [7] and RSA [8]. The encryption process of this scheme is based on six components.

To create the ciphertext C, the sender encrypts the plaintext M using the recipient's public key PU and an encryption algorithm E. The receiver then applies the matching decryption method D to the ciphertext using his private key PR, which is known only to him. As a result,$M = D(Sk, C)$ and $C = E(Pk, M)$ [1]. The model of Public key encryption is illusterated in Figure 2.4 An important factor in Asymmetric key cryptography is authentication. A certificate Authority (CA) is a reliable third party among the owner of public key and party that depends upon certificate. It provides the authentication to the person that involved in communication to assure that the specific key is related to person who claimed it.

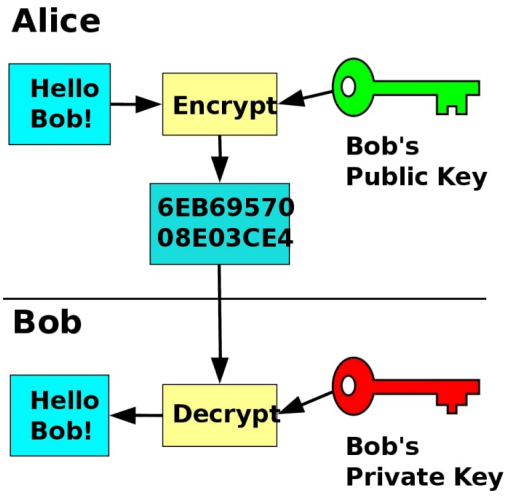


FIGURE 2.4: Asymmetric key Encryption Model

2.3.3 One Way Trapdoor Function

Trapdoor functions are one-way functions with an additional constraint. A one-way function is one for which calculation in the opposite manner is much more difficult than evaluation in the precise same direction. A function is referred to be a trapdoor one-way function when the restriction that computing in the opposite direction is relatively easy upon revelation of some additional (trapdoor) information is present.

Trapdoor one-way functions were first described by Diffie and Hellman [17], who also examined its implications for the advancement of public-key cryptography, paralleling the theoretical development of one-way functions. The full potential of trapdoor one-way functions was successfully realised in the proposal for public-key cryptography and the development of digital signature techniques. When it is given M and a function $f(M)$, it is difficult to find a message $M^{'} \neq M$ such that $f(M^{'}) = f(M)$.

As explained below, the idea of a one-way trapdoor function makes it possible to practically design a public key cryptography.

- The basis of public key cryptosystems is a trapdoor one-way function. The public key offers information on a particular instance of the function, but

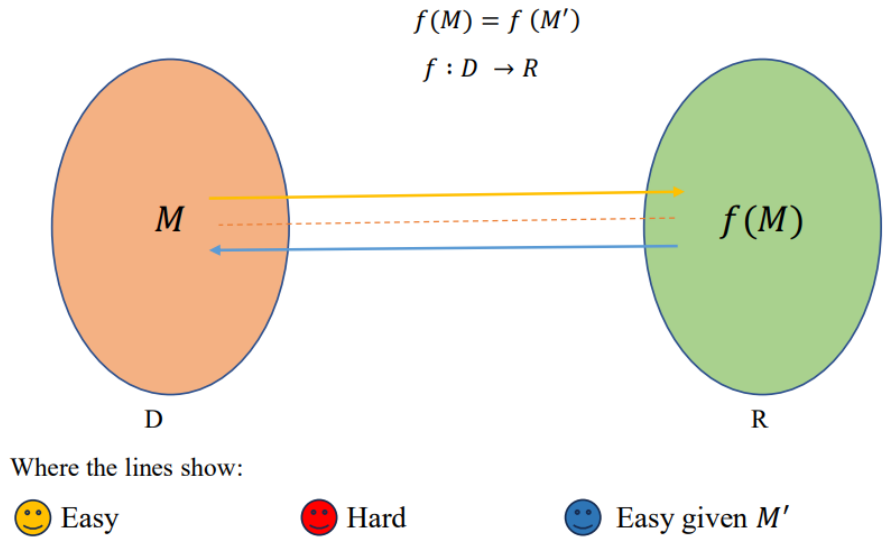


FIGURE 2.5: Oneway Trapdoor Function

the private key serves as the trapdoor.

- Trapdoor function is also used in factorization of a very large integer that is the product of two large prime numbers. Selecting and verifying two large prime numbers and multiplying them is easy. But factoring the resulting product is hard task. This is the basis for RSA encryption [8] known as integer factorization problem.

- To secure digital signature for the future use, use the trapdoor one-way function. Because, inverse function that is used to compute the signatures will take large amount of time, Due to this it is infesible for an attacker to compute the signature.

- Although no function has been demonstrated to be one-way, all viable public-key cryptosystems are built on top of such functions. Because, theoretically it is feasible to create an algorithm that quickly computes the inverse function without a trapdoor.

2.3.4 Hash function

A string of characters with a variable length is known as "message". A "hash function" which is mathematical function simply converts this data or string into

a string with a fixed number of characters known as a hash value or just a"hash". Since even a small change to the message will give output that is completely unique hash, hashing is important for verifying the legitimacy of data. Hashing is convenient to certify the authenticity of a chunck of data [34]. Mathematically, if given a hash function h and value of t then it is easy to calculate $h(t)$ but with given $h(t)$ it is hard to calculate the value of t. The result of hash function is named as hash value. Computing a hash value is easy but difficult to reverse. As shown in Figure 2.6 There are following important properties of hash function.

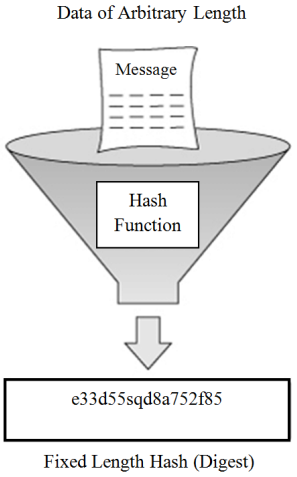


FIGURE 2.6: Hash function

1. **Efficiency:** For any given input in the hash function, the hash value or output is smoothly computed.

2. **Pre-image resistance:** It is impossible to determine the associated input value for any given output or hash value in the hash function.

3. **Collision resistance:** If input x_1 is provided, it is impossible to obtain an other input x_2, resulting in a situation where both inputs set the same value.

4. **Sensitivity:** Small change in input data creates a major change in output data.

   The hash functions that are commonly used are secure hash algorithm, SHA [35], SHA-1 [36], SHA-256 [37], SHA-3 [38], MD5 [39]. Comparison of different hash functions described in Table 2.2 below.

TABLE 2.2: Comparison of Cryptographic Hash Functions

Algorithem	Output size	Block size	Message size	Rounds	Collision
SHA	160	512	$2^{64}-1$	80	yes
SHA-1	160	512	$2^{64}-1$	80	2^{63} Attack
SHA-256	256	512	$2^{64}-1$	64	No
SHA-224	224	512	$2^{64}-1$	64	No
SHA-512	512	1024	$2^{128}-1$	80	No
SHA-384	384	1024	$2^{128}-1$	80	No

Types of Hash Functions

There are two types of hash functions.

1. **Keyed Hash function**

   The keyed hash function requires the message and the secret key to return an output called one way keyed hash value.

2. **Unkeyed Hash Function**

   The only type of input required by the unkeyed hash function is a message, and it outputs a hash value devoid of any secret key.

2.3.5 Elliptic Curve Discrete Logarithm Problem

Given an ellpitic curve $y^2 = x^3 + ax + b^2 \mod p$ and a base point P, we will calculate $Q' = kP$ through $k-1$ iterative point additions. Fast algorithms for this task exist. It is hard to compute k when the point Q' is known. This is known as an Elliptic Curve Discrete logarithm Problem (ECDLP). The security of any cryptographic scheme relies on ECDLP.

2.3.6 Diffie-Hellman Key Exchange based on Eliptic Curve

To communicate securely, Ayeza and Babar must disclose their keys to encrypt and decrypt the messages. Exchanging of keys over a public network without compromising security was first intoduced by Diffie and Hellman [33] in 1976. A

cyclic group of elliptic curve points is used to create the scheme, and the safety of the system depends on how challenging it is to overcome ECDLP. The Diffie-Hellman key exchange protocol is appllied to exchange keys between Ayeza and Babar in the following method.

1. Ayeza and Babar mutually selects an elliptic curve E over a finite field $\mathbb{F}_p$ with base point of elliptic curve G of curve E.
2. Ayeza selects a random number $n_A \in \{1, 2, 3, \ldots n-1\}$ as her secret key and compute her public key as $P_A = n_A G$.
3. Babar choose his private key $n_B \in \{1, 2, 3, \ldots n-1\}$ and calculates his public key $P_B = n_B G$.
4. They both share their public keys P_A and P_B with each other.
5. Ayeza computed $P_{AB} = n_B n_A$ where P_{AB} is used to find n_A and n_B as session key security.

Example 2.3.1. Let Ayeza wishes to send a message $m = 23$ to Babar. So, they must share their keys to encode and decode a message. Ayeza and Babar mutually selects an elliptic curve $y_2 = x^2 - 4 \mod 257$ that is equalvalent to $E_{257}(0, -4)$, where $G = (2, 2)$ is the base point of order $n = 129$. That is, $129(2, 2) = \mathcal{O}$ and this elliptic curve contains 258 points.

1. Ayeza selects secret key $n_A = 101$ and compute public key as

$$P_A = n_A G = 101(2, 2) = (197, 167).$$

2. Babar selects secret key $n_B = 17$ and compute public key as

$$P_B = n_B G = 17(2, 2) = (80, 56).$$

3. They both exchange their $P_A = (197, 167)$ and $P_B = (556, 631)$ with each other publically.

4. Ayeza computed $P_{AB} = n_A n_B = 17(101) = 175 \mod 257$ is used to find $n_A = 101$ and $n_B = 17$ as session key security.

2.3.7 Digital Signature

A digital signature is a mathematical formula applies to confirm the legitimacy of digital messages or documents. In the presence of a genuine digital signature, a recipient has a very high level of confidence that the message has been generated by a recognized sender (authenticity) and was not altered while in route (integrity), provided that the requirements are met. The majority of cryptographic protocols include digital signatures as a basic component. They are commonly used in financial transactions, software distribution, contract management, and other circumstances where it is critical to spot fraud or tampering.

In asymmetric cryptography, digital signatures are used. Frequently, they extend the security and verification of messages received across an unsafe channel. When used appropriately, a digital signature gives the recipient assurance that the message came from the specified sender. Traditional handwritten signatures are equivalent to digital signatures in many ways, however correctly implemented digital signatures are harder to forge than the handwritten physical signatures. Digitally signatures can be formulated by using idea of asymmetric key cryptography. In this context, digital signature systems are cryptographically designed and require adequate implementation to be effective. Additionally, they can offer non-repudiation, which prevents the signers from being able to claim they did not sign a message while yet maintaining the secrecy of their private key [40].

Properties of Digital Signature

Follows are the properties of digital signature.

1. **Authenticity:** Only authorized user has access to original signatures and message.

2. **Unforgeability:** A valid signature for the related message can only be provided by the signer. This ensures that the forged signatures are not possible.

3. **Non-re-usability:** A signature from one document cannot be used on another.

4. **Non-repudiation:** The signer of a document with a valid signature cannot deny their signature.

5. **Integrity:** Make sure the information has not been changed.

2.4 Signcryption

Signcryption is a public-key primitive in cryptography that combines the capabilities of digital signature with encryption. They were considered as significant but separate components of many cryptographic systems up until 1997. In public key systems, the traditional method is to sign a communication digitally, then encrypt it (signature, then encryption). However, this approach can have two drawbacks. First, it is inefficient and expensive, and second, no random strategy can provide security. Signcryption is a relatively recent cryptographic technique that seeks to merge the digital signature and encryption operations in a single logical step, as opposed to the traditional signature-then-encryption systems. Additionally, it can drastically lower the overheads associated with communication and computing. Rather than signing and encrypting separately, a more efficient approach, signcryption combines the benefits of digital signatures and encryption methods. In 1997, Zheng [9] presented the first signcryption technique. It saves 58% of computational costs and 40% of transmission costs when compared to the traditional elliptic curve based signature. Various alternative signcryption systems have also been put forth over the years, each scheme comes with its own set of issues and constraints in addition to provide varying degrees of security and computational costs. A signcryption method is often made up of the three methods key creation, signcryption, and un-signcryption. While signcryption is frequently a probabilistic

process and unsigncryption is nearly surely deterministic, key generation creates a pair of keys for every user [9].

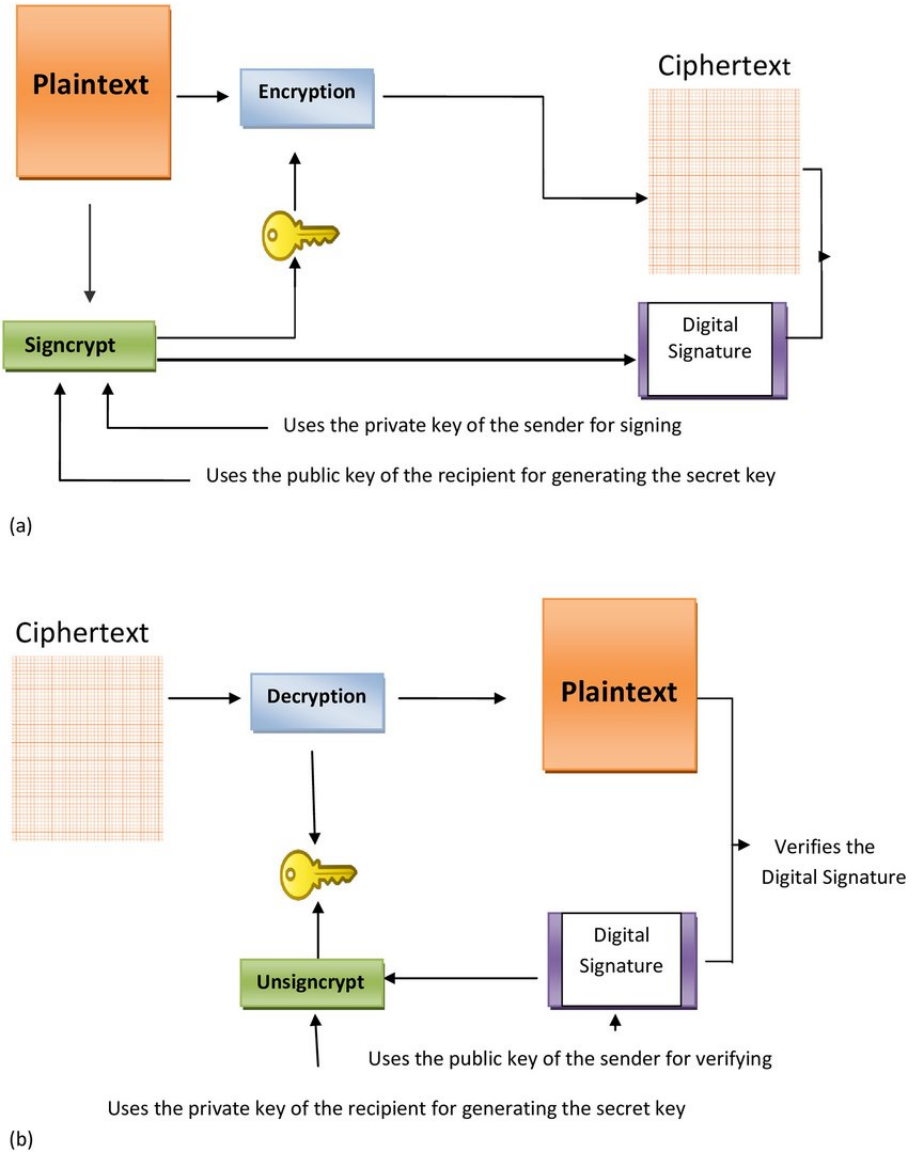


FIGURE 2.7: Model of Signcryption

Security attributes

- **Confidentiality:** It should be computationally impossible for an attacker to extract even a small portion of the content of a signcrypted text without knowing the sender's and receiver's private keys.
- **Unforgeability:** A clever attacker shouldn't be able to produce an authentic signcrypted text that the unsigncryption algorithm can accept by disguising themselves as an honest sender due to computational limitations.

- **Non-repudiation:** The signcrypted text should be conveyed, and the recipient should be able to show the sender's identity to a third party (such as a judge). Because of this, the sender's previously signed and encrypted texts cannot be disputed.

- **Integrity:** The message received should be authentic and delivered by the sender, and the recipient should be able to confirm this.

- **Public verifiability:** Without knowing private key of sender or receiver, anyone may check to see if the signed text is a real or not.

- **Forward secrecy:** No body should be able to read or decrypt the plaintext even secret key is exposed. In a standard signature encryption method in the unlikely scenario that the long-term secret key is compromised, all previously issued signatures become invalid. Forward secrecy appears to be a crucial component of such systems, as more cryptographic computation are often performed on unprotected devices like cell phones, the risk of key exposure is increasing.

  In the next section presented Zheng's [9] signcryption scheme

2.4.1 Zheng's Signcryption Scheme

The concept of signcryption was first put forth by Zheng [9]. It is a earliest cryptographic scheme that executes encryption with public key and digital signatures into one logical operation at a significantly lower computational cost. Zheng's approach allows the recipient to verify signatures either directly (using his private key) or indirectly (without releasing the recipient's private key). In the following section we take a concise look of this scheme.

Global Setting

Algorithm 2.4.1. Key Generation

1. Ayeza choose private key $n_A \in \{1, 2, 3, \ldots q-1\}$ and compute her public key $P_A = r^{n_A} \mod q$.

TABLE 2.3: Global Setting

m	original message or plaintext
q	any big prime number
p	any big prime factor of $q-1$
r	randomly choosen number from $\{1, 2, 3. \ldots q-1\}$
h	one way hash function to get 128-bit hash values
H_k	Keyed hash function
E	private key encryption algorithm
D	private key decryption algorithm

2. Babar choose private key $n_B \in \{1, 2, 3, \ldots q-1\}$ and compute his public key $P_B = r^{n_B} \mod q$

Algorithm 2.4.2. Signcryption

We have given input plaintext m secret key n_A of Ayeza (sender) and public key P_B of Babar (receiver) and after signcryption, we get an output ciphertext c and signatures s , as mentioned in the below algorithm 2.4.2.

Input:(m, n_A, P_B)

Output:(c, s)

1. Ayeza choose an integer $r \in \{1, 2, 3, \ldots q-1\}$
2. Ayeza use public key of Bob P_B, the random integer r and one way hash function h to compute

$$u = h(P_B * r) \mod q$$

3. She distributes 128 bits into two equal 64-bits. They can be numbered as u_1 and u_2
4. Ayeza use public key encryption scheme E with key u_1 to encrypt the message m. It will give ciphertext

$$c = E_{u_1}(m) \mod q$$

5. She use second key u_2, message m and one way keyed hash H_k value to compute value of α.

$$\alpha = H_k u_2(m) \mod q$$

6. Ayeza computed signature parameter s by using α, the secret key n_A, the large prime number q and α

$$s = \frac{r}{\alpha + n_A} \mod q$$

7. Ayeza have a values of (c,α,s). In order to compute the task she send these values to Babar.

After signcryption we have output (c,α,s). Now for unsigncryption we have input (n_B, P_A, c, s), where n_B is the secret key of Babar, P_A is public key of Ayeza, c is the ciphertext and s is a signature.

Algorithm 2.4.3. Unsigncryption

Input:(n_B, P_A, c, s)

Output:m

1. Babar recieves cihpertext c, keyed hash value $\alpha = H_k u_2(m)$ and signatures value s. Babar also uses the values r which is random integer and s, his secret key n_B, Ayeza's public key P_A and q to calculate a hash value of 128 bits.

$$u = h(P_A.r^{\alpha})^s n_B \mod q$$

   then 128 bit string hash value is distributed into two equal bits portion that gives him (u_1, u_2) where each (u_1 and u_2) are 64 bit keys. So by this both Babar and Ayeza have same key pair.

2. Babar use key u_1 to decrypt the cipheretext c, then he will get message m

$$m = D_{u_1}(c)$$

3. Babar will verify the calculation

$$\alpha = H_k u_2(m)$$

If both results of signcryption and unsigncryption matches then it verifies that Ayeza send signcryption result securly over public network and Babar successfully performed unsigncryption. No attacker or third party altered generated results during transmission.

2.5 Different varients of Signcryption

In cryptographic field different varients of signcryption scheme are proposed. Every signcryption scheme has different level of security attributes and performance efficiency. In next section two different schemes based on signcryption are presented.

2.5.1 Identity Based Signcryption

In cryptography for secure comunication over public network, three types of security is important, confidentiality, integrity, and authentication. A type of public key encryption called identity-based encryption [41] allows users to create their own public keys using well-known unique identifiers, like email addresses, and has a trusted third-party server construct the corresponding private keys from the public keys. This eliminates the requirement for distributing public keys before sharing encrypted data. The recipient's unique identifier can be used by the sender to create a public key and encrypt the contents. The PKG (public key generation) first provides a master public key accessible while maintaining the corresponding master private key (sometimes referred to as the master key) to apply this encryption technique. Any party can determine a public key matching to an identity given the master public key by combining the master public key into a known identity value (such as an email address). The PKG generates the requested private key using its master private key after receiving a request from the owner of the identity that was utilized to generate the public key.

2.5.2 Blind Sincryption Scheme

Before discussing blind signcryption, we are discussing blind signatures which was first introduced by chaum [42] . Any blind signature scheme must satisfy the two main properties which are blindness and untraceability. Blindness property allows that the message is transmitted between a user and a signer where message contents remain unknown to signer. On the other hand untraceability property

ensures that signer can not identify any kind of message-signature pair later, even if signature is disclosed to public. Chaum [42] signature scheme is based on integer fractorization problem (IFP). There are many Blind signcryption schemes and these are typically based on four phases, which are mentioned below.

- Pre-request Phase
- Key Generation Phase
- Blind Signcryption Phase
- Unblind Signcryption Phase

The sender (Ayeza), the recipient (Babar), and the signer are the three participants in the scheme. A Signer signs received communication without reviewing the original message's content. Suppose Ayeza wants to transmits a message to Babar over public network. First Ayeza blinds the message and then send it to the signer. Signer signs the message without knowning the message contents and send back it to Ayeza. Ayeza transmits a signcrypted text to Babar after unblinding the blind signature.

2.6 Gernalized Signcryption

Messages does not always need to be confidential and authentic. Depending on the communication, simply signing or only encrypting may be required. When compared to standard signcryption, the latter two circumstances can only provide one of the specific parties. Because there is no longer a specific party with key pairs, traditional signcrytion will stop. Zheng [9] proposed a signcryption scheme and ElGamal encryption in applications to resolve this issue. The three primitives of signing, encrypting, and signcrypting must all be implemented by applications. In some applications such as embedded devices and ubiquitous computing, the method is, nevertheless, impractical. A signcryption that is more adaptable and practical is known as generalised signcryption [22]. When both confidentiality

and authenticity are needed at once, it provides two functions, and when just confidentiality or authenticity is needed, it only gives one function encryption or signature without any modifications or additional calculations. In specific situations, a generalised signcryption scheme will be comparable to a signature scheme or an encryption method.

Therefore, there are three scenarios: signature encryption, signature only, and encryption only. The three cases identification is a significant issue. In public key configurations, the information about a specific sender is needed in order to complete the authentication procedure. An information about recipient's public key and secret key is needed to perform the encryption process. The knowledge about both parties is needed in order to do the signcryption operation. Therefore, the operator's identity can be utilised to differentiate between the three scenarios.

2.7 Cryptanalysis

The study of ciphertext and cryptosystems is known as cryptanalysis, which aims to security analysis of developed techniques for weakening or breaking them. Secure hashing, digital signatures, and other cryptographic techniques are the focus of cryptanalysts, who, for example, attempt to interpret ciphertexts without being aware of the plain-text source, encryption key, or method that was used to encrypt them. While cryptanalysis aims to detect weaknesses in cryptographic algorithms or otherwise undermine them, cryptographers make use of cryptanalyst's research findings to strengthen or replace outdated techniques. Cryptography, which focuses on creating encryption cyphers and made better other techniques, it encircle both cryptanalysis and cryptography.

It is conceivable for researchers to devise techniques of attack that entirely destroy an encryption method, making it trivially simple to decrypt ciphertext encoded with that algorithm without the encryption key. When cryptanalytic output point out infirmity in the design or implementation of the technique, the total number of keys are turn down that are tried on target ciphertext. An encryption algorithm may be completely defeated by attack techniques created by researchers, making

it trivially viable to decipher ciphertext encrypted using that algorithm without the encryption key. When cryptanalyts find out errors in the structure or implementation of the algorithm, the number of keys that have to be checked on the target ciphertext might be reduced.

2.7.1 Types of Attacks

There are different types of attacks. Some of them are discussed below. For further details on these attacks we reffer [43–46].

2.7.2 Ciphertext Only Attack

In this attack model, the attacker has only the knowledge of more than one encrypted messages without any knowledge of corresponding plaintext data, in all practical ciphertext only attacks , an attacker has still some knowledge of plaintext contents. For instance, the attacker may be aware of language in which plaintext is written. In many developed systems, standard protocol data and messages are common part of plaintext which can be guessed.

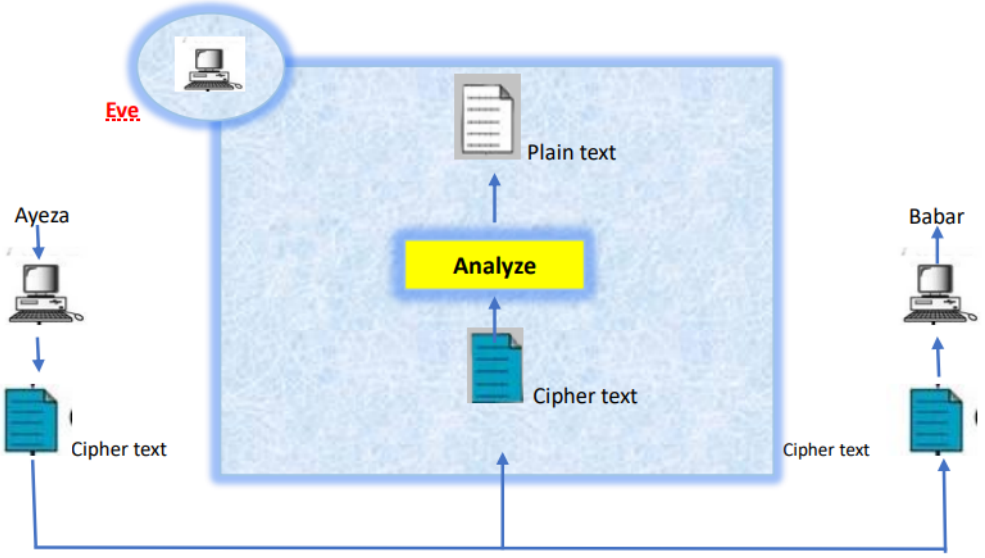


FIGURE 2.8: Cipheretext Only Attack

2.7.3 Known Plaintext Attack

An attacker could have approach to any or every bit of the ciphertext of plaintext in a known plaintext attack. The goal of an attacker in this scenario is to locate the encryption key and decrypt the ciphertext to recover to message. In this way, he can use it to decrypt all messages that were originally encrypted. A known plaintext attack, called linear cryptanalysis, approximates the operation of a block cipher using a linear function. The ability to decipher or infer a portion or the full of an encrypted message, as well as the format for the original plaintext, is a prerequisite for known plaintext attacks.

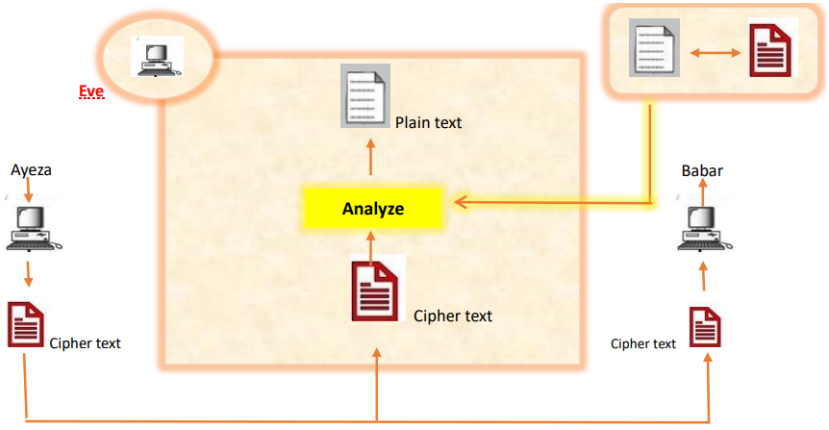


FIGURE 2.9: Known Plaintext Attack

2.7.4 Choosen Plaintext Attack

In a choosen plaintext attack, the interpreter is either in possession of the necessary encryption tools or is conversant with their workings. The interpreter can encrypt the selected plaintext with the selected algorithm to discover more about the key.

2.7.5 Choosen Ciphertext Attack

In this type of attack an attacker can gathere information by obtaining decryptions of choosen ciphertexts. The basic aim of attacker is to obtain the secret key. So

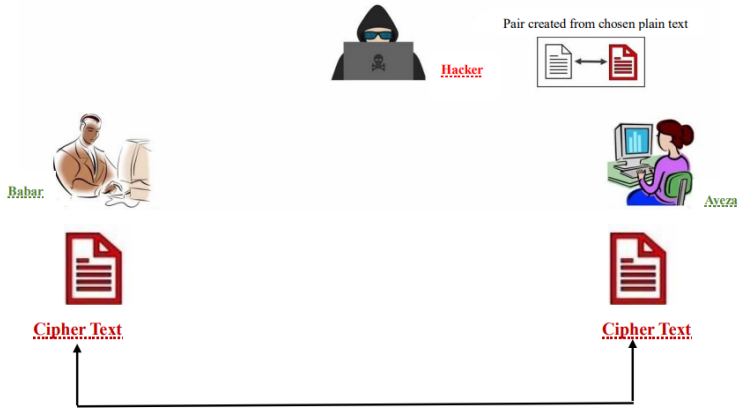


FIGURE 2.10: Choosen Plaintext Attack

he use all gathered data to recover the secret key which is used to decrypt the plaintext. Mostly this attack model is applicable in public key cryptography.

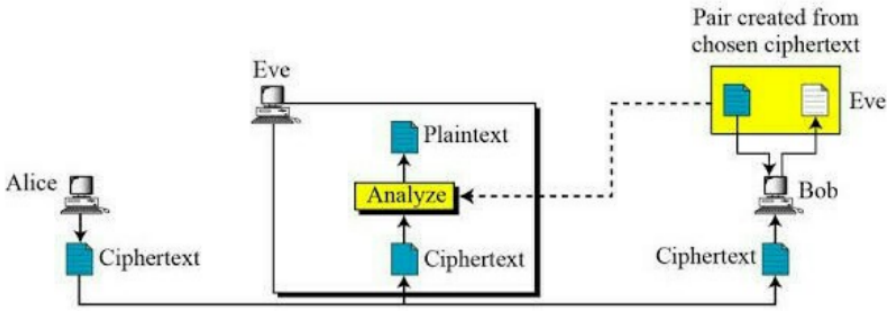


FIGURE 2.11: Choosen Ciphertext Attack

2.7.6 Brute Force Attack

In this type of attack an attacker uses trials and error method to crack the password or secret key. Attacker tries all possible keys and passwords to decrypt the ciphertext which is correct. In this attack model, Special designed computers and devices are used to break the cryptosystem. Time required to break the cryptosystem depends upon the size of key which is used to encrypt the message. This attack model is presented in Figure 2.12.

FIGURE 2.12: Brute Force Attack

2.7.7 Forgery Attack

In this type of attack attacker firsty intercepts the network communication between sender and receiver to alter the original message with his own choice and creates a fake digital signatures by using public parameters in such a way, the unsigncryption algorithm correctly verifies it. After verification of the fake digital signatures, receiver accept the message and belives that message is not tempered during transmission and sent by authorized person. So in this way, attacker transmits any message of his own choice successfully with having knowledge of sender and receiver.

2.7.8 Side Channel Attack

Data from the system that is used for encryption and decryption of the message is collected during a side-channel attack. Successful side-channel attacks make use of information other than the ciphertext generated by the encryption method, such as information on how quickly a system answers to particular queries, total power the encrypting system injest, or how much electromagnetic radiation emited by the system.

2.7.9 Man-in-the-Middle Attacks

When a third party learns how to enter the communication room between two parties who are interacting with one other and want to exchange keys for encrypted communication using the asymmetric or public keys, this is known as a man-in-the-middle attack. The attacker performs a key exchange with every single one of the original parties while the parties think they are exchanging keys with each other. The keys of an attacker are ultimately used by the two parties.

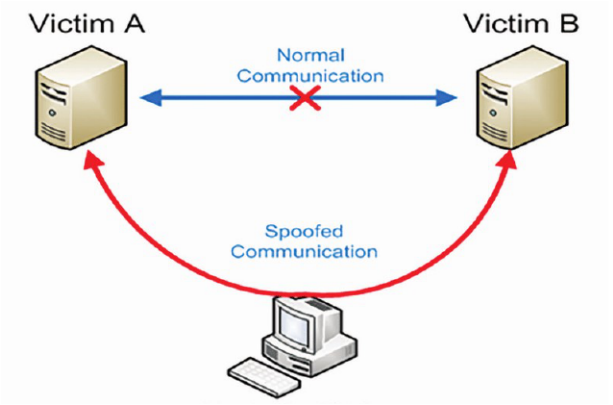


FIGURE 2.13: Man-in-the middle attack

2.8 Elliptic Curve Cryptography

Crtptography with public key that involves elliptic curve is called elliptic curve cryptogrphy (ECC), and it is based on the algebraic structure of elliptic curves over finite fields. ECC allows for smaller keys to achieve equal security compared to non-EC encryption (based on plain Galois fields) [47].

Applications for elliptic curves include key agreement, digital signatures, and pseudo-random number generators. By coupling a symmetric encryption method with a key agreement, they may be used for encryption secretly.

The use of an ellpitic curves in cryptography was first suggested by Neal Koblitz and Victor Saul Miller in 1985. An Elliptic Curve Discrete Logarithm problem (ECDLP) is the foundation of the ECC [6] . This tendency will undoubtedly

continue as more people desire gadgets to keep their belongings safe as keys get bigger, putting a strain on the scarce mobile resources. Knowing ECC in its context is important because the main advantage of ECC [6] is that, for key sizes currently in use, it is simply stronger than RSA [8] and ELGamal [7].

RSA [8] keys must get longer to outlast an attacker's computer capability. It makes sense to implement ECC [6] in order to guarantee high standards of both efficiency and security. In comparison of other public key cryptosystem like RSA [8] and ELGamal [7], ECC uses smaller key size with the same level of security. The comparison of ECC [6] with RSA [8] is presented in the Table 2.4 below [48].

TABLE 2.4: Comparison of ECC wirh RSA

Bits of Security	RSA and DH Key size	ECC Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

.

Elliptic Curve Cryptosystem

Asymmetric key cryptography uses the elliptic curve approach. Each user must have a unique public key and private key for secure communication.

Global Settings

The global parameters that involved in communication between sender and receiver.

1. Consider elliptic curve group $E_q(a, b)$, where q is a prime integer and a, b are parameters of elliptic curve.

2. G is the base point such that $nG = \mathcal{O}$. where n is the prime number and $\mathcal{O}$ is point at infinity.

Key Generation Phase

1. Sender chooses the randomly secret key $n_a \in \{1, 2, \ldots n-1\}$ and calculate public key as $\mathbb{P}_a$=n_aG.

2. Receiver chooses the secret key $n_b < n$ and computes the public key as $\mathbb{P}_b = n_bG$.

Encryption Phase

1. The sender uses the ECC scheme to send a message m to the receiver. For this m is converted into a elliptic curve point $\mathbb{P}_m$.

2. Sender select a random integer k and calculates the ciphertext C_m as the elliptic curve pair of points using receiver's public key $\mathbb{P}_b$ as follows.

$$C_m = (kG, \mathbb{P}_m + k\mathbb{P}_b) \mod q.$$

Decryption Phase

After receiving ciphertext C_m, message will be decrypted back into original form by multiplying kG with private key of the receiver n_B and then add the result into second ciphertext pair $(\mathbb{P}_m + k\mathbb{P}_b)$

$$\begin{aligned}\mathbb{P}_m + k\mathbb{P}_b - n_b(kG) &= \mathbb{P}_m + k(\mathbb{P}_b) - k(\mathbb{P}_b) \mod q \\ &= \mathbb{P}_m.\end{aligned}$$

which is plaintext, so receiver gets the same value.

Example 2.8.1. Consider the elliptic curve group $E_{257}(0,-4)$ given by $\mod 257$.

$$y^2 = x^3 - 4 \mod 257.$$

that is equalvalent to $E_{257}(0,-4)$. Let $G = (2,2)$ be the basepoint of an elliptic curve. Total number of points are 258 and order of G is 129 where $129(2,2) = \mathcal{O}$. Let private key of receiver is $n_b = 101$ and his public key is $\mathbb{P}_b = n_b G = 101(2,2) = (197,167)$.

A sender wishes to send a message to receiver that is encrypted in an elliptic point $\mathbb{P}_m = (112,26)$. Sender chooses random integer $k = 41$ and computes

$$\begin{aligned} k\mathbb{P}_b &= 41(197,167) = (68,84) \mod 257 \\ kG &= 41(2,2) = (136,128) \mod 257 \\ \mathbb{P}_m + k(\mathbb{P}_b) &= (112,26) + (68,84) = (246,174) \mod 257. \end{aligned}$$

sender sends the ciphertext to receiver,

$$\begin{aligned} C_m &= \{c_1, c_2\} = \{kG, \mathbb{P}_m + k(\mathbb{P}_b)\} \mod 257 \\ C_m &= \{(136,128),(246,174)\} \mod 257. \end{aligned}$$

then receiver receives the ciphertext and decrypt the ciphertext

$$\begin{aligned} \mathbb{P}_m &= \{\mathbb{P}_m + K(\mathbb{P}_b) - K(\mathbb{G} * n_b)\} \mod 257 \\ &= \{(112,26) + (68,84) - 41(197,167)\} \mod 257 \\ &= \{(112,26) + (68,84) - (68,84)\} \mod 257 \\ \mathbb{P}_m &= (112,26) \mod 257. \end{aligned}$$

Simplified Data Encryption Standard (S-DES)

S-DES is a symmetric key encryption. This technique is divided into three phases. A Key Generation phase, Encrytpion phase and Decryption phase. A 10 bit key is

converted into two 8 bit and shared these keys between both sender and receiver.

P10 is a permutation, LS-1 is a circular left shift of 1 bit position, LS-2 is a circular left shift of 2 bit positions. P8 is another permutation.A Figure 2.14 is illustrates the S-DES Algorithm below.

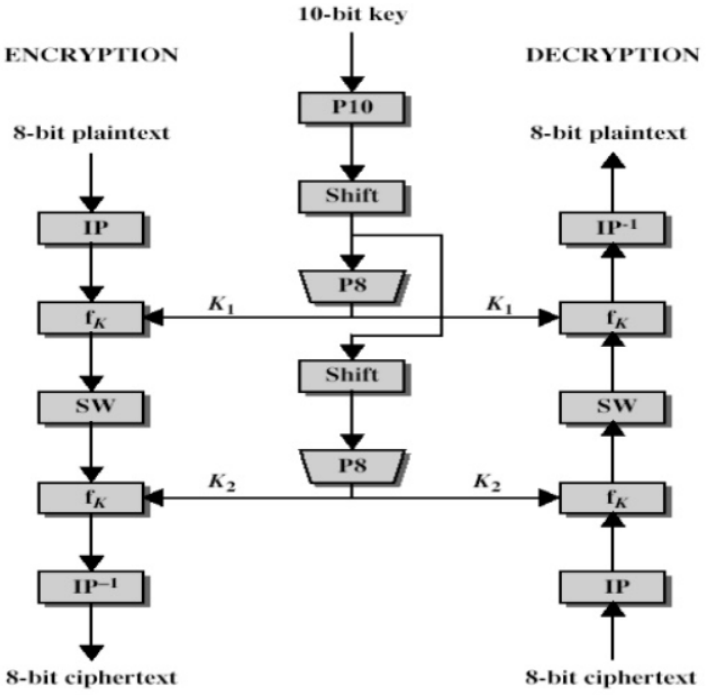


FIGURE 2.14: S-DES Algorithm

In this chapter, mathematical and cryptographic background are presented. In mathematical background some basic defintions and examples like groups, field, galois field, ring, Fermats theorem, division algorithm, and elliptic curves are presented. In cryptographic background, types of cryptogtraphy, one way trapdoor function, hash function, ECDLP, digital signature, signcryption, Zheng's signcryption scheme, different varients of signcryption scheme, types of attacks, elliptic curve cryptography and generalized signcryption scheme are presented.

Chapter 3

Signcryption Scheme Based on Elliptic Curves

In this chapter, we review the signcryption scheme of Zhang et al [28]. This scheme is based on elliptic curve cryptography. Section 3.1 presents a detailed review of the signcryption scheme. This scheme has four phases like setup, key generation, signcryption and unsigncryption. After this in Section 3.1.3 presents the pictorial view of the whole scheme. This scheme has resistance againts the multiple cryptographic attacks so, Section 3.2 presents the security analysis of the scheme and the chapter is concluded with the security analysis of the scheme.

3.1 ECC Based Signcryption Scheme

In this section, signcryptoin scheme based on Elliptic Curve is reviewed, which was proposed by Zhang et al [28]. The signcryption is divided into four phases.

1. Setup
2. Key Generation
3. Signcryption
4. Unsigncryption

3.1.1 Setup

In this scheme, $GF(q)$ is a finite field, where q is the order of the finite field, also q is a large prime number and its length is ℓ bits. Let $E_q(a, b)$ be an elliptic curve with parameters $a, b \in GF(q)$. Let G be the base point of the elliptic curve $E_q(a, b)$. G_1 is an elliptic curve cyclic multiplication group of order q which is generated by base point G. M is a plaintext and plaintext space is $\{0, 1\}^\ell$. Two hash functions $\{H_1, H_2\}$ are used for the security of the scheme, where H_1 hash function applies on values from G_1 and its resulting values will be fixed bit string of length ℓ and H_2 is a second hash function which applies on variable bit string of length $\{*\}$ and its resulting values will be in Z_q. These parameters on which both sender and receiver are agreed are presented in below Table 3.1.

TABLE 3.1: Setup

q	large prime number
G	base point of elliptic curve
$GF(q)$	a finte field of order q
$\mathcal{O} = nG$	order of base point G here n is large prime number
G_1	cyclic multiplication group of order q based on elliptic curve
$H_1 : G_1 \longrightarrow \{0, 1\}^\ell$	a hash function
$H_2 : \{0, 1\}^* \longrightarrow \mathbb{Z}_q$	a hash function

Keygeneration

The second phase of the signcryption scheme is keygeneration. Both sender and receiver generate their private and public keys by using procedure which is described below.

1. The sender randomly choose his secret key x_S and generates his public key as

$$Y_S = x_S G.$$

2. The receiver randomly chooses her private key x_R and generates her public key as

$$Y_R = x_R G.$$

Then, they share their public keys to each other and keep their private keys secret. Both sender and receiver agreed on key generation paramerters that are given in the below Table 3.2.

TABLE 3.2: Global Setting

x_S	a secret key of sender
Y_S	a public key of sender
x_R	a secret key of receiver
Y_R	a public key of receiver
M	plain text
C	a ciphertext

After key generation, the sender have input (M, x_S, Y_S). Now sender uses his public key Y_S and secret key x_S to signcrypt message M and produce an output $\alpha = (C, E, \mathcal{S})$ where C is the ciphertext, E is the ecryption result and $\mathcal{S}$ is signatures value produced by the sender.

Details of Signcryption algorithm are presented below.

Algorithm 3.1.1. (Signcryption)

Input: (M, x_S, Y_S).

Output: $\alpha = (C, E, \mathcal{S})$.

1. Choose random number $k \in \{1, 2, \ldots q-1\}$.
2. Compute $kY_R = K \mod q$.
3. Compute $B = H_1(K) \mod q$.
4. Compute $C = B \oplus M \mod q$.

5. Compute $E = H_2(M, K, Y_S, Y_R)$.
6. Calculate $\mathcal{S} = k^{-1}(E + x_S) \mod q$.
7. If $\mathcal{S} = 0$, go to step 1.
8. Obtain the signcryption $\alpha = (C, E, \mathcal{S})$ and send α to the receiver.

Next presents the Unsigncryption algorithm of the Scheme.

Algorithm 3.1.2. (UnSigncryption)

when receiver obtains the output (signcryption) $\alpha = (C, E, \mathcal{S})$ then uses her public key Y_S and secret key x_R to unsigncrypt the signcrypted result α.

1. Evaluate $W = \mathcal{S}^{-1} \mod q$.
2. Evaluate $\beta = EWY_R + WY_S x_R \mod q$.
3. Evaluate $B^{'} = H_1(\beta)$.
4. Evaluate $M = B^{'} \oplus C \mod q$.
5. Evaluate $E^{'} = H_2(M, \beta, Y_S, Y_R)$.
6. When we get $E^{'} = E$ then return M, else return $\perp$.

3.1.2 Verification

For the verification of above signcryption scheme 3.1.1, below equations must hold and value of β must be equal to K. When $\beta = K$, its mean results of Sincryption algorithm are correct.
$\mathcal{S} = k^{-1}(E + x_S)$. Here $\mathcal{S}^{-1} = k(E + x_S)^{-1}$.

$$\begin{aligned}\beta =& EWY_R + WY_S x_R \mod q \\ =& E\mathcal{S}^{-1}Y_R + S^{-1}Y_S x_R \mod q \\ =& E\mathcal{S}^{-1}x_R G + \mathcal{S}^{-1}x_S x_R G \mod q \\ =& (E + x_S)k(E + x_S)^{-1}x_R G = kx_R G = kY_R = K \mod q \\ \beta =& K\end{aligned}$$

So by above equation , when $B^{'} = B$, and $E^{'} = E$ certify that the recipient can re-establish the message M of sender, also decryption process will be correct. Recepient can confirm the verification of signature of the sender when $E^{'} = E$ and this certify that the verification process is correct. Therefore this shows signcryption algorithm is correct. In next section, a block diagram of whole scheme is presented which is a pictorial view of the whole scheme.

3.1.3 Block Diagram of Signcryption Scheme

Block diagram 3.1 is illustrates the proposed scheme briefly.

3.2 Security Analysis

The following are the security analysis to be considered.

3.2.1 Confidentiality

Information must be kept confidential so that it can only be accessed by authorised users and cannot be shared with unauthorised users. An essential feature of encryption is confidentiality. The signcryption system must also provide confidentiality because signcryption required to implement signature and encryption.

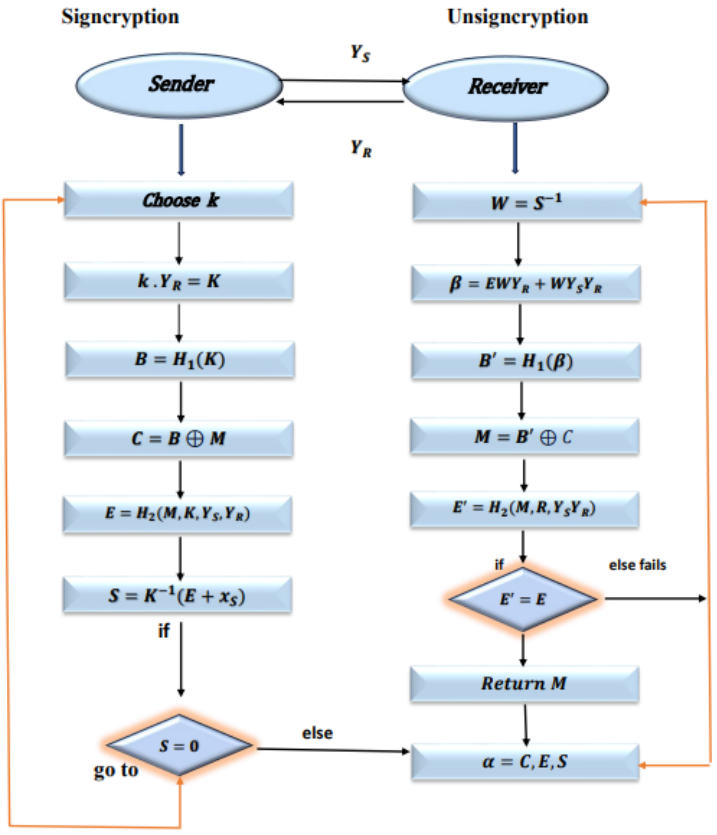


FIGURE 3.1: Block Diagram of Signcryption scheme

If an adversary wants to compute the plaintext he will be unable to compute the secret parameters B, K and x_S. Because if he wants to calculate the value of $C = B \oplus M$ in Step 4 of Algorithm 3.1.1. He has to solve $B = H_1(K)$ which is Step 2 of algorithm 3.1.1, where K involves the random secret number k and public key of receiver $Y_R = x_R G$. An attacker has to solve the ECDLP to obtain these secret parameter adversary . Which is computationally infeasible for an adversary to solve. So this signcryption scheme has confidentiality.

3.2.2 Unforgeability

A signature must have the capacity to be unforgeable. The signcryption technique must also be unforgeable because signcryption needs to implement both encryption and signatures. This secheme has unforgeability according to Algoritm 3.1.1. An adversary has no access to a valid signatures that are generated by authorized person. In Step 6 of reviewed scheme, if an adversary wants to generate a valid

signature $\mathcal{S} = k^{-1}(E + x_S)$ of Signcryption Algorithm 3.1.1, then secret random number k and hash bit string $E = H_2(M, K, Y_S, Y_R)$ in Step 5 of Algorithm 3.1.1 must be known to him, which involves the secret parameter $K = kY_R$, $Y_R = x_R G$ and $Y_S = x_S G$ and message M (which is confidential). It is computationaly infeasible to solve ECDLP to get these values.

3.2.3 Integrity

Integrity relate to the ability of data to remain unchanged in the time of transmission and storage, whether accidently or intentionally. In this scheme the information among the sender and receiver cannot easily be tampered with using signcryption method. Because of clash of a hash function and the actuality that this interference requires the hash value $B = H_1(K)$ in step 3 of Signcryption Algorithm 3.1.1, this hash value will be correspond to random point on the elliptic curve, the attacker will be unable to identify the point on the elliptic curve that corresponds to the hash value B. Additionally, each message block is dependent on every component of the ciphertext $C = B \oplus M$ in Step 4 of signcryption algorithm 3.1.1. Any modification to a specific block of data by a malicious attacker will result in a change to the whole ciphertext. This signcryption approach is hence trustworthy.

3.2.4 Nonrepudiation

Nonrepudiation applies to both signatures and signcryption. Nonrepudiation forbids a communicating party from retracting a prior commitment or action. Nonrepudiation refers to a signer's inability to later retract his signature from a legitimate communication in a signcryption method.

In this signcryption technique, a hash value of message M is evaluated by sender. To obtain this value sender has to use both public keys Y_R, Y_S. Now sender use his own private key x_S to sign this hash value. Therefore, the sender cannot dispute that message M bears its signature. Additionally, the receiver will determine the

hash value in unsigncryption using both its own public key Y_R and the sender's public key Y_S. If it matches the hash value of the received signature, the sender actually signed the signature. Consequently, this scheme includes nonrepudiation.

3.2.5 Availability

Information may be accessible by authorised entities and utilised immediately. The term availability means that all staff can be used by the authorized person at the right time.

To get the message M that is signed by the sender , receiver has to use his private key in Step 4 of Unsigncryption Algorithm 3.1.2. After getting message M receiver has perform other required operations. Therefore this signcryption scheme has availibilty.

3.2.6 Forward Secrecy

The confidentiality of previously encrypted messages is unaffected by the disclosure of the encryptor's private key, which is known as forward secrecy.

If Private key of sender is disclosed, then adversary in this signcryption scheme should have the knowledge of the value of $B = H_1(K)$ to acquire the contents of the previous session which are mention in Step 1 of Signcryption Algorithm 3.1.1, the adversary be required to know the value of k which is randomly choosen integer. Hence, even if adversary calculated the secret key of sender, he still can not recover the paintext information. Hence this scheme has forward secrecy.

3.2.7 Internal Security

Security analysis of signcryption can be divided into external and internal security. Internal security means that an attacker has knowledge of both public and secret keys of both sender and receiver and external security means that attacker

knows public information. If attacker wishes to regenerate the plaintext M from cipheretext C he must have to solve the hash value $B = H_1(K)$ which is difficult to solve (ECDLP), also attacker has knowledge of k which is random integer in step 2 of Signcryption Algorithm 3.1.1. So attacker can not get the point of an elliptic curve that correspond to that hash value. On the other hand if attacker has access to secret key of recepient x_R, it is impossible to generate a valid ciphertext $C^{'}$ because even if attacker uses receiver's secret key x_R and can calculate value of β, gets the hash value $B^{'}$ by Step 2 in Algorithm 3.1.2, and then uses $C = B \oplus M$ to obtain the ciphertext $C^{'}$ is invalid. Because the ciphertext C in the signcryption result 3.1.1 is the encryption of plaintext $M^{'}$ and in signcryption result 3.1.1 the signature $\mathcal{S}$ is true for plaintext M, which will make unsigncryption fails. Therefore this scheme has internal security.

In this chapter, we reviewed the Zhang et al [28] signcryption scheme which is based on elliptic curve cryptography. This scheme has four phases, step up, key-generation, signcryption and unsigncryption. This scheme has multiple security attributes which are mentioned in this chapter with details. A block diagram of the signcyption scheme is also presented.

Chapter 4

ECC Based Gerneralized Signcryption Scheme

In this chapter we proposed a new generalized signcryption scheme in Section 4.1. Signcrytion scheme of Zhang et al [28] works efficiently when both confidentiality and authenticity are required. Proposed generalized scheme has additional capabilities. It operates in signcryption mode if both confidentiality and authenticity are required, and in encryption-only mode or signature-only mode if only one of them is required.

4.1 Proposed Generalized Signcryption Scheme

The proposed scheme explained in the steps in Section 4.1. As in Chapter 3, there are four phases of the proposed generalized scheme.

1. Setup
2. Key Generation
3. Signcryption
4. Unsigncryption

Setup Phase

Consider elliptic curve $E_q(a, b)$ with operators a and b over field F_q. Let G be the base point of elliptic curve $E_q(a, b)$. H is a hash function which applies on elliptic curve points. M is a plaintext which is also point of elliptic curve $E_q(a, b)$. The parameters are presented to participents sender and recipient. Required parameters are shown in Table 4.1

TABLE 4.1: Setup

Variables	**Description**
q	a prime number, $q \in \{1, 2, 3, \ldots n-1\}$
G	the base point on elliptic curve
n	order of the base point G; $nG = \mathcal{O}$
$\mathbb{F}_q$	is a finite field of order q
$E_q(a, b)$	elliptic curve with parameters a and b over field $\mathbb{F}_q$
H	a one way hash function

Key Generation

The second phase of the proposed generalized signcryption scheme is keygeneration. Both Ayeza(sender) and Baber(receiver) are agreed on parameters which are decribed in Table 4.1 and then generates their private and public keys by using procedure which is described below.

- Sender chooses the private key $x_S \in \{1, 2, 3, \ldots n-1\}$.
- Computes the public key $Y_S = x_S G \mod q$.
- Receiver chooses the private key $x_R \in \{1, 2, 3, \ldots n-1\}$.
- Computes the public key $Y_R = x_R G \mod q$.
- Both sender and receiver exchange their public keys and generate a session key.
- Sender compute $K^* = x_S Y_R = (k_1, k_2) \mod q$.

- Receiver compute $K^* = x_R Y_S = (k_1, k_2) \mod q$. Both generates the same session key K^*.

The parameters of key generation are presented in Table 4.2.

TABLE 4.2: Key Generation

VARIABLES	DESCRIPTION
x_S	a secret key of sender
Y_S	a public key of sender
x_R	a secret key of receiver
Y_R	a public key of receiver
E_k	symmetric Encryption using key k
D_k	decryption algorithm using key k
M	plaintext
C_2	ciphertext

Algorithm 4.1.1. (Signcryption)

1. Choose two random integers u_1 and u_2 from $\{1, 2, 3, \ldots q-1\}$.
2. If $u_1 =$ Null, then take $u_1 G =$ Null, and $C = M$. Then go to Step 8 , else
3. Compute $u_1 G = (p_1, p_2) \mod q$.
4. Compute $C = \{u_1 G, M + u_1 Y_R\} \mod q = \{(p_1, p_2), (q_1, q_2)\}$.
5. Compute $C_1 = \{k_1(p_1, p_2), k_2(q_1, q_2)\} \mod q$.
   $C_1 = \{(p_3, p_4), (q_3, q_4)\} \mod q$.
6. Compute $k = (p_3 + p_4 + q_3 + q_4) \mod q$.
7. To encrypt a message M, compute $C_2 = E_k(M) \mod q$.
8. Compute $r = H(C, k_1) \mod q$.
9. If $u_2 =$ Null, then send $\alpha_e = (C, C_1, C_2, r)$ to receiver.
10. Compute $u_2 Y_R = T \mod q$.
11. Compute $\mathcal{S} = u_2^{-1}(x_S + r \mod q) \mod q$.

12. Send $\alpha_s = (C, \mathcal{S}, T)$ to receiver, if $u_1 =$ Null then send $\alpha_s = (C, \mathcal{S}, T)$ else send $\alpha = (C, C_1, C_2, \mathcal{S}, T, r)$ to receiver.

Algorithm 4.1.2. (Unsigncryption)

1. If receiver receives $\alpha_e = (C, C_1, C_2, r)$ from sender,then
2. Also receive $C = (u_1 G, M + u_1 Y_R) = \{(p_1, p_2), (q_1, q_2)\}$
3. Compute $C_1^{'} = \{k_1(p_1, p_2), k_2(q_1, q_2)\} \mod q$
   $C_1^{'} = \{(p_3, p_4), (q_3, q_4)\} \mod q.$
4. Compute $k = (p_3 + p_4 + q_3 + q_4) \mod q.$
5. To decrypt a message C_2. Compute $M = D_k(C_2) \mod q.$
6. Compute $r^{'} = H(C, k_1) \mod q.$
7. If $r = r^{'} \mod q$ return M else rejected.
8. If receiver receives $\alpha_s = (C, \mathcal{S}, T)$,then
9. Compute $w = \mathcal{S}^{-1} = (u_2^{-1}(x_S + r \mod q))^{-1} \mod q.$
10. Compute $T^{'} = wr^{'}Y_R + wx_R Y_S.$
11. If $T = T^{'}$ then return signatures else rejected.
12. If receiver receives $\alpha = (C, C_1, C_2, \mathcal{S}, T, r)$, then goto step 1.

In the above proposed scheme two random numbers u_1, u_2 play an important role. If sender takes $u_1 =$ Null, then proposed scheme switches into Signature only mode and if sender choose $u_2 =$ Null, then it switches into Encryption and Decryption only mode.

Verification of Signatures

The proposed generalized scheme enables the receiver to authenticate the signatured data $(C, \mathcal{S}, T)$. For the verification of digital signatures we have the following equations described below must be satisfied,

1. Compute $w = \mathcal{S}^{-1} = (u_2^{-1}(x_S + r))^{-1}$.

2. Compute $T^{'} = wr^{'}Y_R + wx_RY_S$.

$$\begin{aligned} T^{'} =& r^{'}\mathcal{S}^{-1}Y_R + \mathcal{S}^{-1}x_RY_S. \\ =& r^{'}\mathcal{S}^{-1}x_RG + \mathcal{S}^{-1}x_Rx_SG. \\ =& \mathcal{S}^{-1}x_RG(r + x_S). \\ =& u_2(x_S + r)^{-1}x_RG(r + x_S). \\ =& u_2Y_R = T \end{aligned}$$

3. If $T = T^{'}$ return signature else rejected.

Verification of Encryption

A receiver may verify his calculations by using below equations. If the receiver confirms the following equation than message decryption is valid.

1. Compute $Y_R = x_RG \mod q$.

$$\begin{aligned} x_SY_R &= Y_Sx_R \mod q \\ &= x_SGx_R \mod q \\ &= x_SY_R \mod q. \end{aligned}$$

2. Decryption process is valid if $x_SY_R = Y_Sx_R \mod q$

4.1.1 Block Diagram of Proposed Generalized Signcryption

Now in Figure 4.1 block diagram of the proposed scheme is presented.

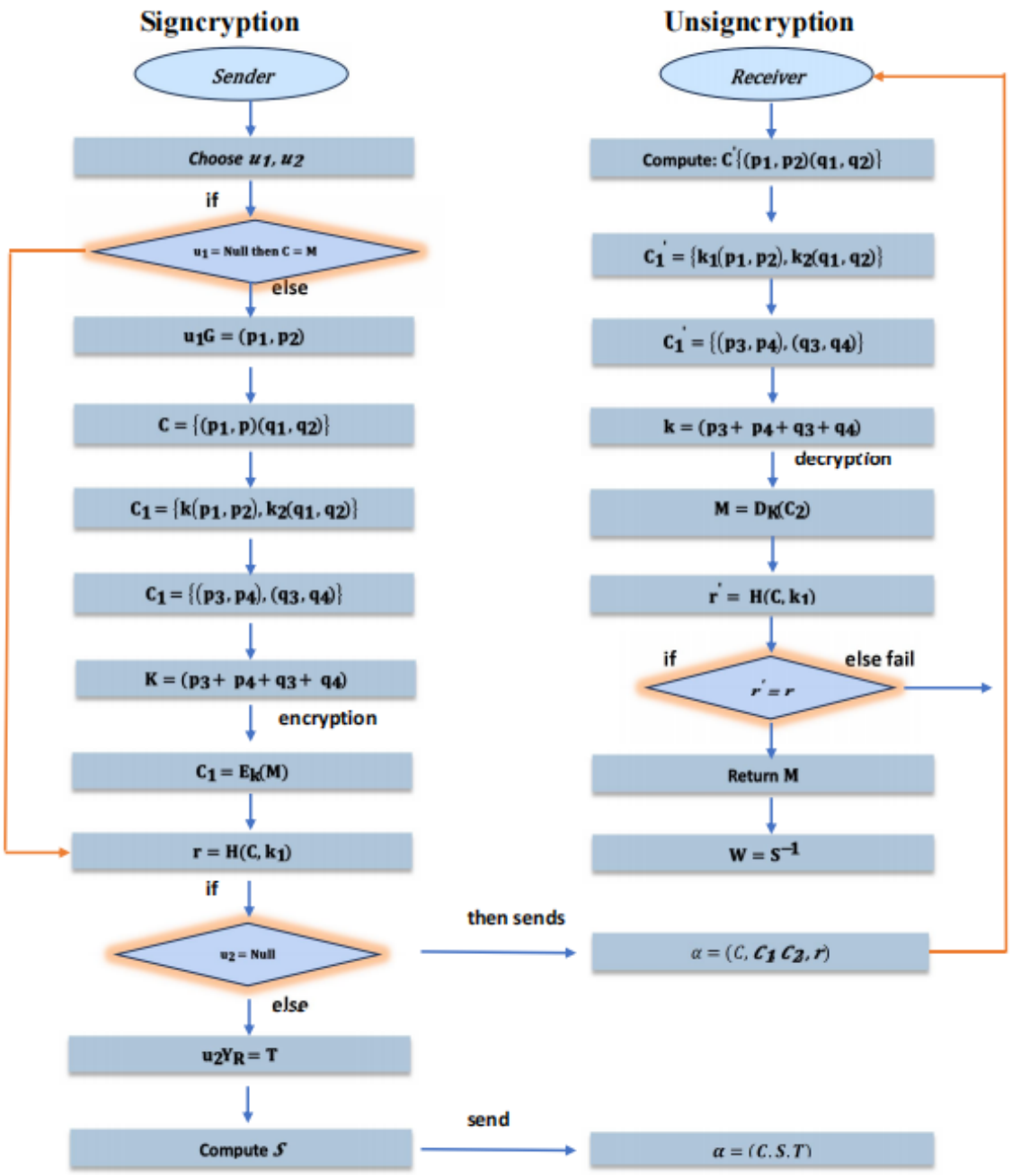


FIGURE 4.1: Block Diagram of Proposed scheme

4.2 Toy Example

In this section, a toy example illustrates the above proposed Generalized signcryption algorithm . For simplicity, the symmetric encryption is performed by using online calculators. Moreover, hash values are calculated by using online hash calculator https://codebeautify.org/crc-16-hash-generator. For modular inverse extended Euclidean algorithm is used. For elliptic curve point multiplication

and addition computer algebra system ApCoCoA is used.

Example 4.2.1. Suppose Ayeza wants to send message $M = (80, 61)$ to Babar in confidential and aunthenticated manner, where M is point on elliptic curve $E_{251}(0, -4)$,given as

$$y^2 = x^3 - 4 \mod 251. \tag{4.1}$$

The size of elliptic curve group is $\mid E_{251}(0, -4) \mid = 252$

Let $G = (47, 77)$ be the base point of elliptic curve then $n = 252$ is the order G. that is

$$252G = 252(47, 77) = \mathcal{O}$$

In order to perform signcryption following steps must be followed.

Key Generation

1. Ayeza chooses her secret key $x_S = 23$ and computes her public key as

$$Y_S = 23(47, 77) = (122, 19) \mod 251.$$

2. Babar chooses his secret key $x_R = 79$ and computes his public key as

$$Y_R = 79(37, 169) = (122, 19) \mod 251.$$

Both Ayeza and Babar exchange their public keys to generate session key

3. Ayeza computed her session key as follows

$$K^* = 23(37, 169) = (85, 41) \mod 251.$$

4. Babar computed his session key as

$$K^* = 79(122, 19) = (85, 41) \mod 251.$$

Both Ayeza and Babar have the same key pair. which is also known as symmetric key.

Generalized Signcryption

1. Select randomly two integers $u_1 = 121$ and $u_2 = 161$.
2. If $u_1 =$ Null then take $u_1G =$ Null $\mod 251$ and $C = M = (80, 61)$, else take $u_1 = 121$
3. Compute $u_1G = 121(47, 77) \mod 251 = (155, 170)$
4. Compute $C = (u_1G, M + u_1Y_R)$

$$= \{(155, 170), (80, 61) + (225, 201)\} \mod 251.$$
$$= \{(155, 170), (69, 166)\} \mod 251.$$

5. Compute $C_1 = \{k_1(p_1, p_2), k_2(q_1, q_2)\}$.

$$= \{85(155, 170), 41(69, 166)\} \mod 251.$$
$$= \{(210, 10), (165, 236)\} \mod 251.$$

6. Compute $k = (210 + 10 + 165 + 236) = 119 \mod 251$.

7. Applying symmetric key encryption S-DES.

$$\begin{aligned} C_2 =& E_k(M) = E_{119}(80, 61) \mod 251. \\ =& (212, 86) \mod 251. \end{aligned}$$

8. If $u_2 =$ Null, then take $u_2 x_R = T \mod q =$ Null, else

9. Compute $u_2 Y_R = T \mod q$.

$$\begin{aligned} &= 161(37, 169) \mod 251. \\ &= (141, 7) \mod 251. \end{aligned}$$

10. Compute $r = H\{(C, k_1\}$.

$$\begin{aligned} r =& h\{(80, 61), 85\} \mod 251. \\ r =& ae66 = 44646 \mod 251. \\ r =& 219 \mod 251. \end{aligned}$$

11. Compute $\mathcal{S} = u_2^{-1}(x_S + r \mod 251) \mod 251$.

$$\begin{aligned} \mathcal{S} =& (161)^{-1}(23 + 219) \mod 251. \\ =& 198(242) \mod 251. \\ =& 47916 \mod 251. \\ \mathcal{S} =& 226 \mod 251. \end{aligned}$$

Which is ciphertext. Now in next section we dicusses the process of unsigncryption of toy example.

Generalized Unsigncryption

1. Compute $C' = (u_1 G, M + u_1 Y_R) \mod 251$.

$$=\{(155,170),(80,61)+(225,201)\} \mod 251.$$
$$=\{(155,170),(69,166)\} \mod 251.$$

2. Compute $C_1' = \{k_1(p_1,p_2), k_2(q_1,q_2)\} \mod 251.$

$$=\{85(155,170),41(69,166)\} \mod 251.$$
$$=\{(210,10),(165,236)\} \mod 251.$$

3. Compute $k = (210+10+165+236) = 119 \mod 251.$

4. Applying symmetric key decryption S-DES.

$$M = D_k(C_2) = D_{119}(212,86) \mod 251.$$

$$=(80,61) \mod 251.$$

5. Compute $r^{'} = H(C,k_1)$

$$r^{'} = h\{(80,61),85\} \mod 251.$$
$$r = ae66 = 44646 \mod 251.$$
$$' = 219 \mod 251.$$

6. As $r = r^{'} = 219$. Accept the ciphertext.

7. $w = \mathcal{S}^{-1} = u_2(x_S + r \mod 251)^{-1} \mod 251.$

$$\begin{aligned} S^{-1} &= (226)^{-1} = 10 \mod 251. \\ w &= \mathcal{S}^{-1} = (161)(242)^{-1} \mod 251. \\ &= (161)(223) \mod 251. \\ &= 35903 \mod 251. \\ w &= 10 \mod 251. \end{aligned}$$

8. As $w = S^{-1}$. Accept signatures.

A new generalized signcyrption scheme based on elliptic curves is presented in this chapter. This scheme is efficient and secure as it has multiple security attributes which are mentioned in this cbapter. This scheme has a flexibility to perform three different modes, one is encryption only mode , second is signature only mode and third is signcyption mode. Prototype example of proposed scheme is also presented also in the end of chapter we presented the whole scheme through block diagram.

Chapter 5

Analysis of the Proposed Scheme

In this chapter, Section 5.1 presentes the security analysis of the proposed scheme. In this section we presented how our scheme has resistance agaits the diffenrent cryptographic attacks. A comparison of the proposed scheme with the existing schemes is displayed in Table 5.1 and computational cost is presented in Table 5.1.8. The security of the scheme againts various known attacks is discussed in Section 5.2.

5.1 Security Attributes

Our suggested scheme performs the following security properties.

5.1.1 Confidentiality

The proposed scheme security relies on hard problem of elliptic curve (ECDLP). Which is more secure in modren cryptography. Adversary will be unable to read or break the contents of ciphertext without the secret keys of sender x_S and receiver x_R and session key K^* in Signcryption Algorithm 4.1.1. An attacker will be unable to calculate $u_1G = (p_1, p_2)$ without secret random number u_1. To get these values an attacker has to solve ECDLP.

5.1.2 Authentication

In every scheme, authentication is important property of security. Proposed scheme has security property named authentication, as it involves both public keys of sender Y_S and receiver Y_R, where Y_S and Y_R are elliptic points on the associated elliptic curve also recepient uses public key of sender to verify the authenticity of received message.

5.1.3 Integrity

The integrity is also provided by the proposed scheme. After getting the signcryption result in Algorithm 4.1.1, the recepient will verify that the ciphertext is not modified during the transmission. If there is an attacker who changes the ciphertext from C_2 in Step 7 of Signcryption Algorithm 4.1.1 to C_2', then consequently $r = H(C, k_1)$ will be changed to $r^{'}$ in Step 8 of signcryption algorithm 4.1.1. Because of these changes, $w = S^{-1} = (u_2^{-1}(x_S + r))^{-1}$ in Step 9 of unsigncryption algorithm 4.1.2 will not be verified.

5.1.4 Unforgeability

The proposed scheme provides unforgeability, as the adversary cannot generate a valid signcrypted text $(C, C_1, C_2, \mathcal{S}, r, T)$ of his own choice without having the knowledge of secret key x_S of sender. Suppose that the adversary selects any message M of his own choice and generates a signcrypted text $(C^{'}, C_1', C_2', \mathcal{S}', r^{'}, T^{'})$ of his choice. But he will be unable to generate a valid signature without secret key of sender x_S and random number u_2 in Step 11 of Signcryption Algorithm 4.1.1 to compute $\mathcal{S} = u_2^{-1}(x_S + r \mod q)$.

5.1.5 Non-repudiation

When there is a disagreement between Ayeza (sender) and Babar (receiver), Babar may send $(C, C_1, C_2, \mathcal{S}, r, T)$ to confirm the validity of the message M, then use

the signature $\mathcal{S}^{-1}$ in Step 9 of the Algorithm 4.1.2, judge (third party) will be able to confirm the validity of the original message M. Only Ayeza is aware of the secret random number u_2, which is used to create the signature in Step 11 of the Signcryption Algorithm 4.1.1 to compute $\mathcal{S} = u_2^{-1}(x_S + r \mod q)$. As a result, Ayeza will be unable to deny sending the message.

5.1.6 Forward Secrecy

The proposed scheme additional security criterion is forward secrecy. Because the suggested technique uses this secret random numbers u_1 and u_2, an adversary would be unable to decrypt any messages even if the sender's private key x_S is disclosed. To obtain the secret random numbers u_1 and u_2, attacker has to solve the EDCLP, which is computationaly impossible. This guarantees the proposed scheme has capacity to maintain forward secrecy.

TABLE 5.1: Comparison of Security Attributes with Existing Schemes

Schemes	C	I	U.F	N.R	A	F.S
Zheng [9]	yes	yes	yes	yes	no	no
Elkamchochi [49]	yes	yes	yes	yes	no	no
Bao and deng [13]	yes	yes	yes	yes	no	no
Zheng an Imai [11]	yes	yes	yes	yes	no	no
Han et al [50].	yes	yes	yes	yes	yes	no
Zhou [51]	yes	yes	yes	yes	yes	no
Gamage et al [14]	yes	yes	yes	yes	yes	no
Mohamed [20]	yes	yes	yes	yes	yes	no
Zhang et al [28]	yes	yes	yes	yes	yes	yes
Proposed Scheme	yes	yes	yes	yes	yes	yes

C: Confidentiality, I: Integrity, U.F: Unforgebility, N.R: Non-repudiation, A: Authenticity, F.S: Forward secrecy.

5.1.7 Efficiency

In this section the efficiency of the proposed scheme is presented. In Table 5.2 the comparison of proposed scheme with different existing schemes is presented. To check the number of times all or some of these operations appeared in different schemes are shown in Table 5.2.

TABLE 5.2: Comparison of Efficiency with Existing Schemes

Schemes	HS	EM	EA	ME	MD	MM	MA
Zheng [9]	4	–	–	3	1	2	1
Han et al [50]	4	5	1	–	2	4	3
Elkamchochi [49]	6	–	–	3	1	4	1
Bao and Deng [13]	6	–	–	5	1	1	1
Zheng and imai [11]	4	3	1	–	1	3	1
Zhou [51]	6	6	7	–	1	4	2
Mohamed [20]	6	6	1	–	1	–	1
Gamage et al [14]	4	–	–	5	1	1	1
Lal and Kushwa	8	5	1	–	3	3	2
Zhang et al [28]	4	3	3	–	2	3	1
Proposed scheme	2	5	1	–	2	1	2

The various operations involved in different schemes are the use of one way hash function (HS), elliptic curve point addition (EA), elliptic curve point multiplication (EM), Modular division (MD), Modular exponentiation (ME), Modular addition (MA), Modular multiplication (MM) .

5.1.8 Computational Cost

Ellpitic curve for both encryption and signatures is used in the proposed scheme. The main advantage of elliptic curve cryptography is that it provides a smaller key size with the same level of security as compared to RSA [8] and Elgamal [7]. In the proposed scheme, calculations of signature generation involves simple arithmetic

operations and only one computation of hash function is involved, whereas the reviewed Zhang's scheme uses two hash functions. In [52] using the "Controller Infineons SLE66CUX640P", a single elliptic curve point multiplication operation takes 83 miliseconds, whereas a single modular exponentiation takes 220 miliseconds. In the below Table 5.3 the comparison of the number of main operations included in the proposed scheme with exsisting schemes is presented.

TABLE 5.3: Comparison of Computational Cost with Existing Scheme

Schemes	Computational time(ms)	Features
Zheng [9]	$3 \times 220 = 660$	SC
Han et al [50]	$5 \times 83 = 415$	SC
Elkamchochi [49]	$3 \times 220 = 660$	SC
Bao and Deng [13]	$5 \times 220 = 1100$	SC
Zheng and imai [11]	$3 \times 83 = 249$	SC
Zhou [51]	$6 \times 83 = 498$	SC
Yu and He [53]	$11 \times 220 = 2420$	SC
Waheed et al [54]	$5 \times 83 = 415$	GSC
Zhang et al [28]	$3 \times 83 = 249$	SC
Proposed scheme	$5 \times 83 = 415$	GSC

5.1.9 Performance Evaluation

In this section, we compare the computational cost and performance of proposed scheme with encryption only mode and signature only mode with the Zhou's [51], Mohamed [20] and Zhang et al [28] schemes .

Encryption only mode

In encryption only mode, the number of operations perform for encryption and its comparison with exsisting schemes is presented in below Table 5.4

TABLE 5.4: Comparison of Performance with Encryption only mode

Schemes	HS	EM	EA	ME	MD	MM	MA
Zhou [51]	3	4	5	–	–	4	1
Mohamed [20]	3	5	1	–	1	–	1
Zhang et al [28]	2	1	1	–	1	1	–
Proposed scheme	1	4	1	–	1	–	2

Signature Only Mode

The performance of proposed scheme while working with signature only mode is presented in below Table5.5

TABLE 5.5: Comparison of Performance with Signature only mode

Schemes	HS	EM	EA	ME	MD	MM	MA
Zhou [51]	3	2	2	–	1	–	1
Mohamed [20]	3	1	–	–	1	–	1
Zhang et al [28]	2	2	2	–	1	–	1
Proposed scheme	1	1	–	–	1	1	–

5.2 Attack Analysis

This section analyses the suggested scheme and demonstrates its resistance to a number of well-known cryptanalysis attacks.

5.2.1 Choosen Plaintext Attack

The objective of attacker is to chooses any message and finds its corresponding ciphertext, the attacker attempt to correspond the plaintext and corresponding ciphertext to find the secret key. Because the attacker can enter any message and try to decrypt the ciphertext to find the secret key, this form of attack is successful. In the described method, a hacker receives plaintext and ciphertext

messages (C_2, M), and make an effort to figure out the secret key x_S where $C_2 = E_k(M)$ in step 7 of Signcryption Algorithm 4.1.1. When given M and C_2, to obtain the secret key x_S of sender and attacker has to solve ECDLP, which is computationally infeasible and secure in modren cyrptography.

5.2.2 Ciphertext Only Attack

According to this attack paradigm, the attacker attempts to construct the original plaintext M or the secret key of sender x_S after obtaining ciphertext from publicly accessible sources. If the secret key x_S is revealed later, attacker wil be able to decipher all the ciphertext and obtains the plaintext messages M. In proposed scheme, an attacker attempts to obtains the secret key x_S or the plaintext message M. If he receives the ciphertext message $C_2 = E_k(M)$. Again, in order to retrieve x_S, he must solve ECDLP which is computationaly infeasible even if attacker has ciphertext message C_2 and the publicly communicated parameter $C = (u_1G, M + u_1Y_R)$. Without knowing the secret key x_S, he will be unable to get the original plaintext message M.

5.2.3 Choosen Ciphertext Attack

An attacker who uses a "selected ciphertext assault" can select any number of ciphertext messages and obtains the required plaintext. The attacker's primary goal is to obtain the secret key or to include the secret parameters in the transmission. In the suggested approach, an attacker chooses a desired ciphertext (C_2') and obtains the associated plaintext message (M'). The secret key x_S cannot be discovered by given ciphertext $C_2 = E_k(M)$ and plaintext M because it requires another secret parameter k. If a hacker wishes to discover the encryption key $k = (p_3 + p_4 + q_3 + q_4)$ in step 6 of Sincryption Algorithm 4.1.1, he has to know the secret random number u_1. However, computing $u_1G = (p_1, p_2,)$ in step 3 of Algorithm 4.1.1 requires again solving ECDLP, which is computationally impossible with the provided parameters C and C_1 in Step 4 and 5 of the Signcryption lAlgorithm 4.1.1 respectively.

5.2.4 Forgery Attack

In this attack paradigm, an attacker sets hold of the network communication between the sender and the recipient. The objective of the attacker is to change or modify the original message with the desired message in such a manner that the unsigncryption method can appropriately verify it. Assume the proposed scheme's sender and recipient network traffic is intercepted by an attacker. The unsigncryption algorithm is unable to validate the incoming message, therefore the intruder modifies and creates the signcrypted text of his choice, (C', C_2', S', r', T'), and transmits it to the recipient. Generalised Signcryption Algorithm 4.1.1 requires a secret random number u_2 and a secret sender key x_S that are not known to an adversary for the production of the signatures $\mathcal{S}$. Consequently, the fake signcrypted text can not be checked by unsincryption algorithm without using these secret parameters. Hence, the forgery attack on the proposed scheme can not be mounted.

5.2.5 Man in the Middle Attack

An adversary participates in the communication between the Ayeza (sender) and the Babar (recipient). The objective of the adversary is to either produce a mutually shared secret key or change the supplied data. For defence against this form of attack in communication, a strong authentication protocol is used. Consider the scenario when a rival tries to influence the mutual secret key generation process in the suggested method. For this reason, attacker selects his secret key x_M and calculates his public key as an elliptic curve point, $Y_M = x_M G$. After getting access to the Ayeza and Babar network messages, he must establish a unique and reliable connection with each of them. The attacker makes a first attempt to create a shared private key using his public key Y_M. However for either of sender or recepient, he will not be able to produce a legitimate mutual secret key K^* since Step 2 and Step 10 of the signcryption algorithm contains the secret number u_2, to which only the true sender has access. In this chapter, first presented the security analysis of the generalized signcryption scheme. A comparison of performance and

computational cost of the proposed scheme with the existing schemes is presented through Table 5.2 and Table 5.3. We also presented comparison of performance with single mode of the proposed scheme in Table 5.4 and Table 5.5. A proposed generalized scheme has resistance againts known cryptographic attacks.

Chapter 6

Conclusion

6.1 Conclusion

In this thesis first we reviewed and presented Zhang et al [28] ECC based signcryption scheme. This scheme is highly efficient and satisfies multiple security properties like confidentiality, integrity, non-repudiation, availibility, unforgeability, forward secrecy, internal and external security. In this thesis, we extended this ECC based signcryption scheme (Section 3.1) to an ECC based generalized signcryption in Section 5.1.8. Depending on the requirements of the user, the extended scheme has flexibility of signcryption mode, encryption only mode and signature only mode as needed. The main benifit and feature of the proposed generalized signcryption scheme is, if user wants only authenticity then signature only mode will be used. If user wants confidentiality only then encryption mode will be used and if user wants both confidentiality and authenticity then generalized signcryption mode will be used. The security of the proposed scheme depends upon the hardness of ECDLP and the properties of hash function. Our proposed ECC based generalized signcryption scheme is highly efficient and provides the multiple security properties like confidentiality, integrity, nonrepudiation, availibility, unforgeability, forward secrecy.

The proposed scheme performs double function so its computaional cost is slightly more than reviewed scheme of Zhang et al [28] but while working with the single

mode the computational cost is significantly lower than the actual signcryption scheme of Zhang et al [28]. The proposed scheme has resistance againts the known cryptographic attacks which are highlighted and proved in Chapter 5.

In future the proposed scheme can be extented to Blind Signcryption scheme. In Blind signcryption scheme, sender signs the plaintext without having the knowledege of message contents.

Bibliography

[1] W. Stallings, *Cryptography and network security, 4/E*. Pearson Education India, 2006.

[2] S. Goyal, "A survey on the applications of cryptography," *International Journal of Science and Technology*, vol. 1, no. 3, 2012.

[3] D. Coppersmith, "The data encryption standard (des) and its strength against attacks," *IBM journal of research and development*, vol. 38, no. 3, pp. 243–250, 1994.

[4] D. Coppersmith, D. B. Johnson, and S. M. Matyas, "A proposed mode for triple-des encryption," *IBM Journal of Research and Development*, vol. 40, no. 2, pp. 253–262, 1996.

[5] J. Daemen and V. Rijmen, "Aes submission document on rijndael, version 2," *Internet: http://csrc. nist. gov/CryptoToolkit/aes/rijndael/Rijndael. pdf [Jan, 12, 2010]*, 1999.

[6] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[8] J. Groth, "Cryptography in subgroups," in *Theory of Cryptography Conference*, pp. 50–65, Springer, 2005.

[9] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+ cost (encryption)," in *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17*, pp. 165–179, Springer, 1997.

[10] D. Hankerson and A. Menezes, "Elliptic curve cryptography," in *Encyclopedia of Cryptography, Security and Privacy*, pp. 1–2, Springer, 2021.

[11] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Information processing letters*, vol. 68, no. 5, pp. 227–233, 1998.

[12] S. D. Galbraith and P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem," *Designs, Codes and Cryptography*, vol. 78, pp. 51–72, 2016.

[13] F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," in *International workshop on public key cryptography*, pp. 55–59, Springer, 1998.

[14] C. Gamage, J. Leiwo, and Y. Zheng, "An efficient scheme for secure message transmission using proxy-signcryption," in *Proceedings of the Twenty Second Australasian Computer Science Conference*, pp. 18–21, 1999.

[15] B. Nayak, *Signcryption schemes based on elliptic curve cryptography*. PhD thesis, 2014.

[16] R.-J. Hwang, C.-H. Lai, and F.-F. Su, "An efficient signcryption scheme with forward secrecy based on elliptic curve," *Applied Mathematics and computation*, vol. 167, no. 2, pp. 870–881, 2005.

[17] L. M. Adleman, "On breaking the iterated merkle-hellman public-key cryptosystem," in *Advances in Cryptology: Proceedings of Crypto 82*, pp. 303–308, Springer, 1983.

[18] J.-B. Shin, K. Lee, and K. Shim, "New dsa-verifiable signcryption schemes," in *Information Security and Cryptology ICISC 2002: 5th International Conference Seoul, Korea, November 28–29, 2002 Revised Papers 5*, pp. 35–47, Springer, 2003.

[19] S. Bala, G. Sharma, and A. K. Verma, "An improved forward secure elliptic curve signcryption key management scheme for wireless sensor networks," in *IT Convergence and Security 2012*, pp. 141–149, Springer, 2013.

[20] E. Mohamed and H. Elkamchouchi, "Elliptic curve signcryption with encrypted message authentication and forward secrecy," *International Journal of Computer Science and Network Security*, vol. 9, no. 1, pp. 395–398, 2009.

[21] R. Ahirwal, A. Jain, and Y. Jain, "Signcryption scheme that utilizes elliptic curve for both encryption and signature generation," *International Journal of Computer Applications*, vol. 62, no. 9, 2013.

[22] X. A. Wang, X. Yang, and Y. Han, "Provable secure generalized signcryption," *Cryptology Print Archive*, 2007.

[23] W. Xuan, Y. Xiaoyuan, and Z. Jindan, "Provable secure generalized signcryption," *Journal of Computers*, vol. 5, no. 5, pp. 807–814, 2010.

[24] G. Yu, X. Ma, Y. Shen, and W. Han, "Provable secure identity based generalized signcryption scheme," *Theoretical Computer Science*, vol. 411, no. 40-42, pp. 3614–3624, 2010.

[25] G. Wei, J. Shao, Y. Xiang, P. Zhu, and R. Lu, "Obtain confidentiality or/and authenticity in big data by id-based generalized signcryption," *Information Sciences*, vol. 318, pp. 111–122, 2015.

[26] C. Zhou, Z. Zhao, W. Zhou, Y. Mei, *et al.*, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Networks*, vol. 2017, 2017.

[27] P. Farshim, *Extensions of Public-Key, Identity-Based and Certificateless Encryption Schemes*. PhD thesis, Citeseer, 2008.

[28] P. Zhang, Y. Li, and H. Chi, "An elliptic curve signcryption scheme and its application," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[29] J. J. Rotman, *Journey into mathematics: An introduction to proofs*. Courier Corporation, 2013.

[30] C. J. Benvenuto, "Galois field in cryptography," *University of Washington*, vol. 1, no. 1, pp. 1–11, 2012.

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

[32] K. S. McCurley, "The discrete logarithm problem," in *Proc. of Symp. in Applied Math*, vol. 42, pp. 49–74, USA, 1990.

[33] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pp. 365–390, 2022.

[34] H. Wu, "The hash function jh," *Submission to NIST (round 3)*, vol. 6, 2011.

[35] S. Debnath, A. Chattopadhyay, and S. Dutta, "Brief review on journey of secured hash algorithms," in *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, pp. 1–5, IEEE, 2017.

[36] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The first collision for full sha-1," in *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I 37*, pp. 570–596, Springer, 2017.

[37] L. Dadda, M. Macchetti, and J. Owen, "The design of a high speed asic unit for the hash function sha-256 (384, 512)," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 3, pp. 70–75, IEEE, 2004.

[38] B. Preneel, "The first 30 years of cryptographic hash functions and the nist sha-3 competition," in *Cryptographers' track at the RSA conference*, pp. 1–14, Springer, 2010.

[39] Y. Sasaki and K. Aoki, "Finding preimages in full md5 faster than exhaustive search," in *Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings 28*, pp. 134–152, Springer, 2009.

[40] R. C. Merkle, "A certified digital signature," in *Advances in cryptology—CRYPTO'89 proceedings*, pp. 218–238, Springer, 2001.

[41] J. Malone-Lee, "Identity-based signcryption," *Cryptology ePrint Archive*, 2002.

[42] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology: Proceedings of Crypto 82*, pp. 199–203, Springer, 1983.

[43] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of gsm encrypted communication," in *Annual international cryptology conference*, pp. 600–616, Springer, 2003.

[44] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication*, vol. 23, no. 3, pp. 212–223, 2008.

[45] D. Shree, S. Ahlawat, *et al.*, "A review on cryptography, attacks and cyber security.," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[46] E. Kiltz, A. O'Neill, and A. Smith, "Instantiability of rsa-oaep under chosen-plaintext attack," *Journal of Cryptology*, vol. 30, no. 3, pp. 889–919, 2017.

[47] K. Damasceno, A. de Oliveira, L. de Castro, *et al.*, "Alternative n-bit key data encryption for block ciphers," in *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pp. 409–414, SBC, 2019.

[48] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Nist special publication 800-57," *NIST Special publication*, vol. 800, no. 57, pp. 1–142, 2007.

[49] H. Elkamchouchi, M. Nasr, and R. Ismail, "A new efficient publicly verifiable signcryption scheme and its multiple recipients variant for firewalls implementation," in *2009 National Radio Science Conference*, pp. 1–9, IEEE, 2009.

[50] Y. Han, X. Yang, P. Wei, Y. Wang, and Y. Hu, "Ecgsc: elliptic curve based generalized signcryption," in *International conference on ubiquitous intelligence and computing*, pp. 956–965, Springer, 2006.

[51] X. Zhou, "Improved signcryption scheme with public verifiability," in *2009 Pacific-Asia Conference on Knowledge Engineering and Software Engineering*, pp. 178–181, IEEE, 2009.

[52] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62–73, 1993.

[53] X. Yu and D. He, "A new efficient blind signcryption," *Wuhan University Journal of Natural Sciences*, vol. 13, no. 6, pp. 662–664, 2008.

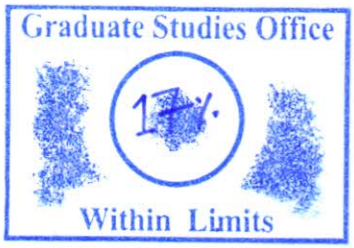
[54] N. Din, A. Waheed, M. Zareei, and F. Alanazi, "An improved identity-based generalized signcryption scheme for secure multi-access edge computing empowered flying ad hoc networks," *IEEE Access*, vol. 9, pp. 120704–120714, 2021.

Turnitin Originality Report

A New Generalized Signcryption Scheme Based on Elliptic Curves by Sukena Syed

From Ms Theses (CUST Library)

- Processed on 07-Dec-2023 16:46 PKT
- ID: 2248560160
- Word Count: 14813



Similarity Index
17%
Similarity by Source

Internet Sources:
9%
Publications:
14%
Student Papers:
5%

sources:

1 2% match (Malik Zia Ullah Bashir, Rashid Ali. "A Multi Recipient Aggregate Signcryption Scheme Based on Elliptic Curve", Wireless Personal Communications, 2020)

Malik Zia Ullah Bashir, Rashid Ali. "A Multi Recipient Aggregate Signcryption Scheme Based on Elliptic Curve", Wireless Personal Communications, 2020

2 2% match (Internet from 07-Nov-2022)

https://link.springer.com/article/10.1007/s11277-020-07637-z?code=1d8d071a-33a6-4061-9bce-cd752394463a&error=cookies_not_supported

3 1% match (Internet from 30-Nov-2020)

https://tutorsonspot.com/questions/project-1-block-encryption-in-cbc-using-3des-oc3j4u/

4 1% match (Ping Zhang, Yamin Li, Huanhuan Chi. "An Elliptic Curve Signcryption Scheme and Its Application", Wireless Communications and Mobile Computing, 2022)

Ping Zhang, Yamin Li, Huanhuan Chi. "An Elliptic Curve Signcryption Scheme and Its Application", Wireless Communications and Mobile Computing, 2022

5 1% match ("Encyclopedia of Cryptography and Security", Springer Science and Business Media LLC, 2011)

"Encyclopedia of Cryptography and Security", Springer Science and Business Media LLC, 2011

6 < 1% match (student papers from 06-Aug-2023)

Submitted to La Trobe University on 2023-08-06

7 < 1% match (student papers from 25-Mar-2019)

Submitted to Universidad de La Laguna on 2019-03-25

8 < 1% match (José Luis Gómez Pardo. "Introduction to Cryptography with Maple", Springer Science and Business Media LLC, 2013)

José Luis Gómez Pardo. "Introduction to Cryptography with Maple", Springer Science and Business Media LLC, 2013

9 < 1% match (Hwang, R.J.. "An efficient signcryption scheme with forward secrecy based on elliptic curve", Applied Mathematics and Computation, 20050815)

Hwang, R.J.. "An efficient signcryption scheme with forward secrecy based on elliptic curve", Applied Mathematics and Computation, 20050815

10 < 1% match ()

, Dhanashree Toradmalle, Varsha Sonigara, Kiran Singh, Omkar Kakade, Krishnachandra Panigrahy, "Implementation of ECC and ECDSA for Image Security", 'Auricle Technologies, Pvt., Ltd.', 2017

11 < 1% match (Caixue Zhou, Zhiqiang Zhao, Wan Zhou, Yuan Mei. "Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings", Security and Communication Networks, 2017)

Caixue Zhou, Zhiqiang Zhao, Wan Zhou, Yuan Mei. "Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings", Security and Communication Networks, 2017

12 < 1% match (student papers from 18-Dec-2014)

Submitted to Indian Institute of Technology, Kharagpure on 2014-12-18

13 < 1% match (Chien-Hua Tsai, Pin-Chang Su. "An ECC-Based Blind Signcryption Scheme for Multiple Digital Documents", Security and Communication Networks, 2017)