Signcryption Schemes Based on Elliptic Curve Cryptography

Biswojit Nayak

Roll. 212CS2111

under the guidance of

Prof. Banshidhar Majhi

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

Signcryption Schemes Based on Elliptic Curve Cryptography

Dissertation submitted in

June 2014

to the department of

Computer Science and Engineering

of

National Institute of Technology Rourkela

in partial fulfillment of the requirements

for the degree of

Master of Technology

by

Biswojit Nayak

(Roll. 212CS2111)

under the supervision of

Prof. Banshidhar Majhi

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

Dr. Banshidhar Majhi
Professor

Certificate

This is to certify that the work in the thesis entitled *Signcryption Schemes Based on Elliptic Curve Cryptography* by *Biswojit Nayak*, bearing roll number 212CS2111, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology* in *Computer Science and Engineering Department*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Banshidhar Majhi

Acknowledgment

First of all, I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Banshidhar Majhi, who has been the guiding force behind this work. I want to thank him for introducing me to the field of Signcryption and giving me the opportunity to work under him. His undivided faith in this topic and ability to bring out the best of analytical and practical skills in people has been invaluable in tough periods. Without his invaluable advice and assistance it would not have been possible for me to complete this thesis. I am greatly indebted to him for his constant encouragement and invaluable advice in every aspect of my academic life. I consider it my good fortune to have got an opportunity to work with such a wonderful person.

I thank our H.O.D. Prof. Santanu Kumar Rath and Prof.(Ms) Sujata Mohanty for their constant support in my thesis work. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I would also like to thank all faculty members, PhD scholars, my seniors and juniors and all colleagues to provide me their regular suggestions and encouragements during the whole work.

At last but not the least I am in debt to my family to support me regularly during my hard times.

I wish to thank all faculty members and secretarial staff of the CSE Department for their sympathetic cooperation.

Biswojit Nayak

Abstract

Signcryption is cryptographic primitive which simultaneously provide both the function of digital signature and public key encryption in a single logical step. Identity based cryptography is an alternative to the traditional certificate based cryptosystem. Its main idea is that each user uses his identity information as his public key. Many identity based signcryption scheme have been proposed so, far. However, all the schemes were proven using bilinear pairing.

Elliptic curve cryptosystem (ECC) have recently received significant attention by research due to their low computational and communicational overhead. Elliptic curve cryptography (ECC) is the hardest computational problems, the elliptic curve discrete logarithm problem and elliptic curve Deffie-Hellman problem are the most reliable cryptographic technique in ECC. The advantages of ECC that it requires shorter key length compared to other public-key algorithms. So, that its use in low-end systems such as smart cards because of its efficiency and limited computational and communicational overhead.

We introduce new signcryption schemes based on elliptic curve cryptography. The security of proposed schemes is based on elliptic curve discrete logarithm problem (ECDLP) and elliptic curve Diffie-Hellman problem (ECDHP). The proposed schemes provide various desirable security requirements like confidentiality, authenticity, non-repudiation and forward security as well as chosen ciphertext attack and unforgeability.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Security Goals

Network Security is most important to provide security in a public network, because we place most critical information in this network. To provide security in public network we must consciously of the three primary goals of network security. These goals are:

- **Confidentiality**: Confidentiality ensures that data or information can't access by unauthorized users.
- **Integrity**: This primary goal of network security prevents unauthorized modification of data at the time of transmission.
- **Availability**: This goal ensures that network resources are always accessible to authorized parties when needed.

Message encryption and digital signature schemes are cryptographic tools for providing confidentiality, integrity, authentication, and non-repudiation. Confidential can be achieved by encryption. Integrity, authentication and non-repudiation can be achieved by digital signature.

1.2 Message Encryption

Encryption is the process of encoding messages that only authorized users can access it. In an encryption scheme, the message or information, known as plaintext, is encoding using an encryption algorithm, converted it into an unreadable ciphertext. This is generally done with the use of an key along with encryption algorithm. So, any adversary can't be able to settle anything about the original message. An authorized user, however, is capable of decode the ciphertext by using a decryption algorithm, that normally requires a secret decryption key, that adversaries do not have access to it. Cryptography has two way of an encryption process called symmetric key encryption and asymmetric key encryption or public key encryption is given below.

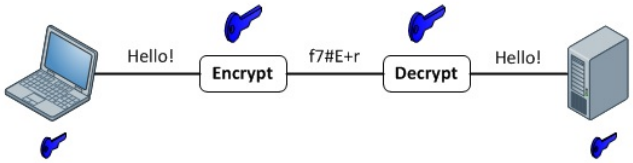

Figure 1.1: Symmetric Key Encryption Process

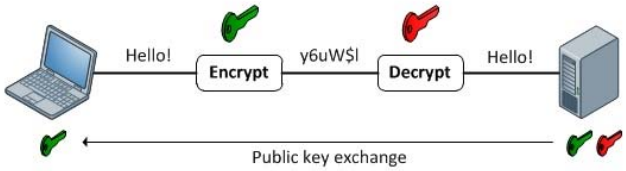

Figure 1.2: Asymmetric Key Encryption Process

1.3 Digital Signature

Digital signatures rely on certain types of encryption to ensure authentication of sender. The signature process intended to receiver that the message was sent by

sender and nothing modified at the time of transmission. Digital signatures are generally made in a two-step. The first step is to use a secure hashing algorithm on the data. Thus, when a signature is verified by the public key, it decrypts to a hash matching the message. That hash can only be deciphered by using the public key if it were encrypted with the private signing key.

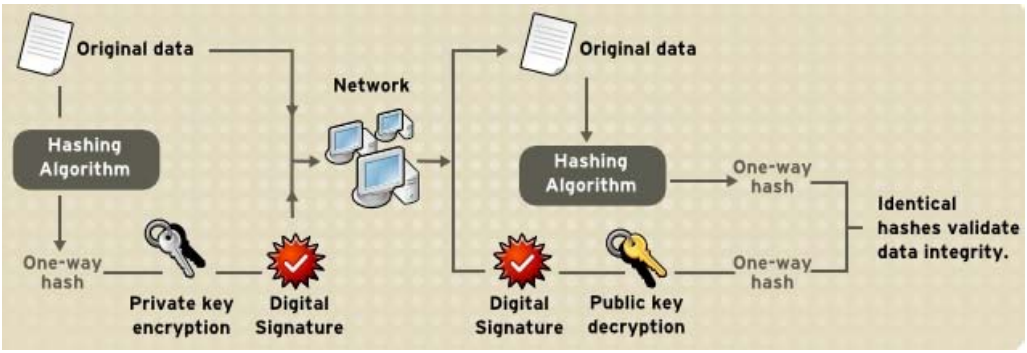

Figure 1.3: Digital Signature

1.4 Signature-Then-Encryption

This is a traditional method of providing confidentiality and authentication by using two serial algorithms [14].

- In first step sender sign message using his/her private key for authentication and then encrypt message using public of receiver.
- At the receiver end, recipient verifies the signature then decrypt the message.

This technique is known as signature-then-encryption. Steps of process are given in the figure [1.4].

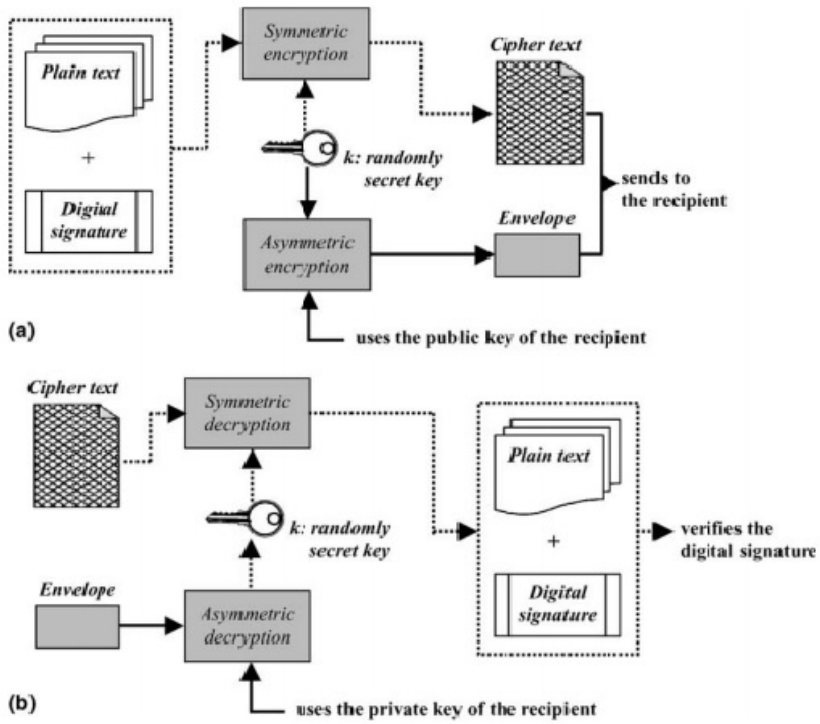

Figure 1.4: Signature-Then-Encryption

1.5 Disadvantages of Signature-Then-Encryption Approach

The disadvantages of traditional signature-then-encryption are in terms of

- Number of bits
- Computational operations
- Size of an entire data packet

In traditional signature-then-encryption, above indicator are increase as compare to signcryption.

1.6 Signcryption

In cryptography, Signcryption is a public key primitive which full fill both the functionality of a digital signature and public key encryption in a single logical step. In the signcryption scheme, the sender generates a one times secret key by using the recipient's public key for symmetric key encryption. Then the sender sends the ciphertext to recipient. After the recipient receives the ciphertext, he derives same secret key by using his/her private key [14].

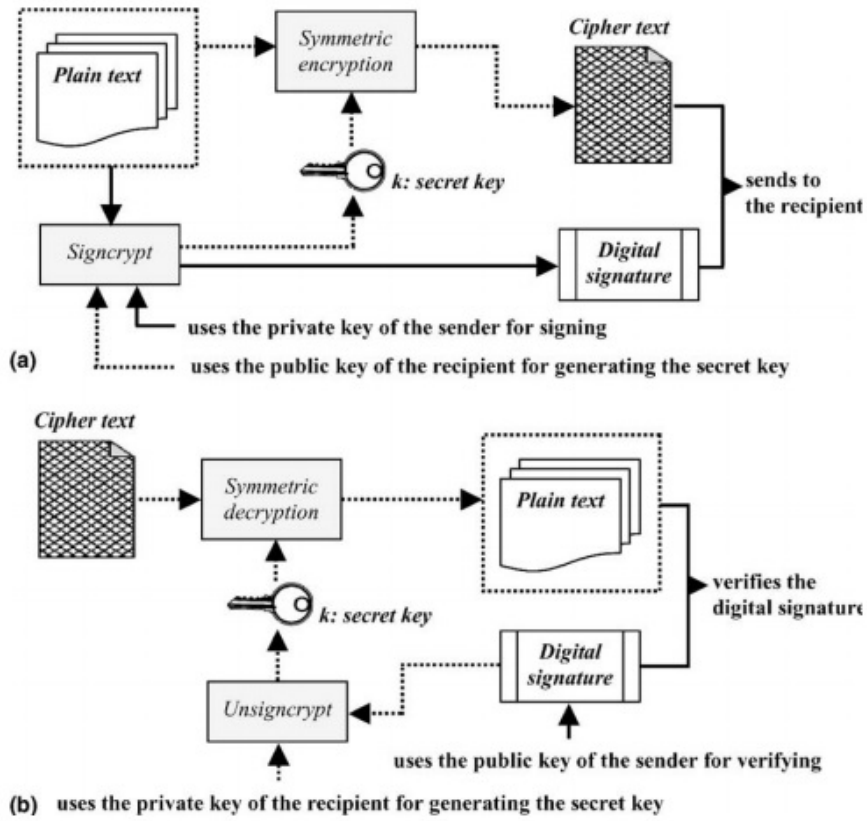

Figure 1.5: Signcryption

1.7 Motivation

Digital signature and message encryption is two cryptographic primitive that provide security goals like confidentiality, authenticity, non-repudiation, integrity. Traditional signature-then-encryption process contains two different steps to achieve all these security goals. Signcryption is a cryptography, which provides both the functionality of digital signature and message encryption in a single logical step. There are lots of research have been done in signcryption since 1997.

In identity-based signcryption, user identity likes name, email, telephone no. is used as a public key. A lot of research has been done in identity based signcryption. However, most of the ID-based signcryption has proven secure in random oracle model. It is a formal model used in cryptographic proofs, where the one way hash function is taken as a black box that maps every unique query with a random response from its output domain. Conversely, it has been proven that security proofs in the random oracle model doesn't imply the security in the real world.

Bilinear mapping is a hardest computational problem, which combining the elements of two vector space to yield an element of another vector space. ID-based signcryption uses bilinear mapping, which is easy to prove in random oracle model. However, bilinear mapping has been more computational as well as simulation overhead as compare to other hardest problems.

Elliptic curve cryptography (ECC) is hardest computational problem and is based on the algebraic structure of an elliptic curve over a finite field. ECC has received significant research due to their performance, and shorter key compare to another public-key algorithm.

1.8 Objective of Research

The main objectives we find from the motivation to work in signcryption are discussed as follows:

- To design a secure identity-based signcryption in the standard model. Standard model is a computational model in which the attacker have some limited of time and calculative power available.
- To develop a ID-based signcryption based on hardness of elliptic curve cryptography (ECC).
- To proof its security goals are under hardness of the elliptic curve discrete logarithm problem (ECDLP) as well as elliptic curve Diffie-Hellman problem (ECDHP).
- To design a strong designation verifiable signcryption scheme based on the elliptic curve discrete logarithm problem (ECDLP) and prevent this scheme from chosen ciphertext attack and unforgeability.

1.9 Organization of the Thesis

The rest of the thesis is organized as follows:

1. Chapter 1: In this chapter we have discussed about the introduction to signcryption, motivation and objective of our research.
2. Chapter 2: In this chapter we present the literature review where we have described some existing works on signcryption.
3. Chapter 3: In this chapter we discussed the mathematical background of thesis work.
4. Chapter 4: In this chapter we present our proposed ID-based signcryption scheme based on ECC their implementation.
5. Chapter 5: In this chapter we present our proposed strong designated verifiable signcryption scheme based on ECDLP and their implementation.
6. Chapter 6: At last we concluded in this chapter.

Chapter 2

Related Work

2.1 Related Work on Signcryption

Encryption and digital signature schemes are cryptographic tools for providing confidential, integrity, authentication, and non-repudiation. Confidential can be achieved by encryption. Integrity, authentication and non-repudiation can be achieved by digital signature. To achieve simultaneously all these goals, the traditional signature-then-encryption approach is first to sign a message and then to encrypt it. In 1997, Zheng [1] proposed a cryptography primitive that fulfill the function of both digital signature and message encryption simultaneously called signcryption , and also proved that cost of signcryption is significantly lower than that needed by traditional signature and encryption approach. There are several signcryption [2–5] have been proposed since 1997.

In the traditional signcryption scheme, the public key of a user is a random element chosen from a group. So, that signcryption doesn't provide the authentication of user by itself because group element cann't define the user identity. This problem can be solved through a certificate based signcryption, which provides arrangement that binds public keys with respective user identities by a certificate authority (CA). That form a hierarchical structure is called public key infrastructure

(PKI). A PKI has a difficulty for the creation, storage and distribution of digital certificates.

To reduce the key management procedure, Shamir [5] introduced the concept of identity-based cryptosystem. The main idea is that the identity information such as name, e-mail, telephone no. of each user uses as his public key. In other words, the identity is used to calculate a user's public key instead of than being extracted from a certificate issued by CA. In ID-Based cryptosystem; users communicate securely without distributing public key certificate, without storing public key directory, and without online participation of a PKG. Malone-lee first proposed the identity based signcryption scheme[6]. There are several ID-based signcryption have been proposed [5–10].

2.2 Related Work on Signcryption Based on ECC

In 1999, Y. Zheng and H. Imai [2] used the hardness of elliptic curve cryptography in signcryption and proposed a signcryption scheme based on the elliptic curve discrete logarithm problem (ECDLP). They also proved that signcryption have approximately, 58% computational cost and 40% of communication cost less than that of traditional Signature-then-Encryption scheme based on the elliptic curve, but the scheme was missed of forward secrecy and public verifiability.

Later F. Bao, R.H. Deng [11] point out that judge can't verify sender authentication without recipient's private key, so they extended Zheng's Signcryption scheme that the judge can verify signature of sender without the recipient's private key. C. Gamage et al. [12] was proposed a signcryption scheme based on Zheng's Signcryption that anyone can verify the sender authentication, but the application area was fixed to firewalls only. H.Y. Jung et al. [13] point out that when the sender's private key is lighted, Zheng's scheme can't provide forward secrecy. In 2005, Ren-Junn Hwang [14] proposed a Signcryption scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP) and Elliptic Curve

Diffie-Hellman Problem (ECDHP) with forward secrecy and public verifiability.

Jun-Bum Shin et al. [15] used a concept of standard DSA algorithm in the verification phase and proposed a DSA-verifiable Signcryption scheme, but the scheme doesn't provide forward secrecy. Raylin Tso [16] proposed a signcryption scheme which uses a standard algorithms for verification, based on hardness of Elliptic Curve Digital Signature Algorithm (ECDSA). The scheme was modified of Shin et al.'s scheme and also proved the property of forward secrecy.

In 2009, M. Toorani and A. A. Beheshti Shirazi [17] proposed a Signcryption scheme based on elliptic curved which provide both the properties of forward secrecy and public verifiability.

2.3 Related Work on ID-Based Signcryption Scheme in Random Oracle Model

In 2002, Malone-Lee [5] uses the concept of identity based cryptography and signcryption, and designed an identity based signcryption scheme based on bilinear pairing.

Libert and Quisquart [18] showed that Malone Lee's proposed scheme has a problem that the signature of the message is visible in cipher text so, it does not provide semantically secure. Libert and Quisquart also proposed three IBSC schemes, but these schemes satisfy either forward security or public verifiability.

In 2004 Chow et al. [19] proposed an ID-Based signcryption scheme that allows for both forward security and public verifiability.

Boyen [20] designed an ID-Based signcryption scheme that provides forward security and public verifiability as well as ciphertext anonymity and unlinkability. After that Malone Lee [21] modified Boyen's scheme and construct a more efficient scheme.

Barreto et al [18] constructed the most reliable and efficiency ID-Based signcryption scheme to date.

The above ID-Based signcryption schemes are proven secure in the random oracle model. It is a mathematical model, where hash function is taken as a random function and is used to analyze cryptography schemes. So, the security proof in the random oracle model does not imply security in the real world.

2.4 Related Work on ID-Based Signcryption Scheme in Standard Model

In cryptography, the standard model is a computational model in which the attacker is only limited of time and computation power available. The security scheme which are proven secure using the complexity assumption are said to be secure in the standard model.

In 2009, Yu et al. [8] proposed an ID-Based signcryption scheme is standard model based on Water's ID-Based message encryption scheme [14] and pateson's and Schuldt's ID-Based signature scheme.

In 2010, Jin et al [9] point out that Yu et al.'s scheme does not prevent against adaptive chosen ciphertext attack and proposed a modified ID-Based signcryption scheme. Jin et al proved that the modified scheme is semantically secure in the standard model.

In 2011, Li et al. [10] pointed that Jin et al. scheme do not have existential unforgeability against adaptive chosen message attacks and indistinguishability against adaptive chosen ciphertext attack . To construct a more flexible scheme which allow ID and message of arbitrary length, collision resistance hash function and used a secure one time symmetric key encryption scheme.

2.5 Related Work on Strong Designation Verifiable Signcryption scheme

In 1996 Jakobsson [22] introduced a strong designated verifier signature scheme in which the private key of designated verifier is used to verify the validity of signature and identity of signer. But that scheme has a problem that, the third party can't determine whether the signer or designated verifier issued the signature. To overcome this problem, Saeednia et al. [23] proposed a strong designated verifier scheme. However, in 2008 Lee-Chang [24] pointed out that Saeednia's scheme would reveal the identity of the signer if the secrete key of the signer is compromised means the signature can be verified not only with the designated verifier's secret key but also the singer's secret key. To overcome this problem Lee and chang [24] proposed a designated verified signature scheme in which a signature can be verified only with the designated verifier signature.

In 2012, S. Mohanty and B. Majhi [25] proposed a strong designated verifiable signcryption scheme based on the mechanism of Lee and Chang proposed signature scheme and incorporated in to signcryption scheme.

2.6 Summary

In this chapter, we have discussed some existing work related to signcryption. A lots of research have been done in signcryption, we briefly mention some of the work and it's flaws.

Chapter 3

Mathematical Background

3.1 Mathematics of Cryptography

3.1.1 Modular Arithmetic

Modular arithmetic is defined as a system of arithmetic for integers, where we are interest in only remainder not quotient [32].

Set of Residues: Z_n

A residues modulo n, or Z_n is always an integer between 0 and $n-1$ or we can say that a nonnegative integer less than n.

$$Z_n = \{0, 1, 2, ...(n-1)\}$$

Additive Inverse

Additive inverse in set of residues or Z_n means, if two numbers x and y are additive inverse of each other then

$$x + y = 0(modn)$$

Additive inverse of x in modulo n can be calculated as $y = n - x$. For example, the additive inverse of 8 in Z_{12} is $12 - 8 = 4$.

Multiplicative Inverse

In the set of residues or Z_n, if the multiplicative inverse x is y or vice versa, then $xy = 1(modn)$. For example in Z_{11}, the multiplicative inverse of 2 is 6. In other word, a integer element x has a multiplicative inverse in Z_n if and only if $gcd(n, x) = 1(modn)$.

In this case, x and n are said to be relatively prime. For example, there is no multiplicative inverse of 8 in Z_{10} because $gcd(8, 10) = 2 \neq 1$.
The Set Z_n and its 3 instances are shown below

1. Z_{n^*}: The set, Z_{n^*} is defined as a subset of Z_n and it contains elements of set Z_n that have multiplicative inverse. In the set Z_n, all the elements have additive inverse, but only some members have a multiplicative inverse.
   Example:
   $Z_7 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ $Z_{7^*} = \{1, 3, 7, 9\}$

2. Z_p: In the set Z_p, p is a prime number and same as Z_n i.e, contains all elements from 0 to $p - 1$. In Z_p, all the elements.
   Note: We need to use Z_n when additive inverses are needed; we need to use Z_{n^*} when multiplicative inverses.
   Example:
   $Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

3. Z_{p^*}: In the Set Z_{p^*}, p is a prime number and same as Z_{n^*} i.e, contains all the elements from 1 to $p - 1$. In Z_{p^*}, all the elements have additive and multiplicative inverse.
   Example:
   $Z_{13^*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

3.1.2 Algebraic Structures

In this chapter, we briefly discuss the subject of algebraic structure. Algebraic structure is defined as the set of element with an operation that is applied to the

element of the set. There are three common algebraic structure known as groups, rings, and fields [32].

- **Groups**: A group(G) is defined as a set of elements, which satisfies following four properties with a binary operation, denoted as $G =< \{...\}, \bullet >$.

  1. **Closure**: If $a, b \in G$, then $c = a \bullet b \in G$.
  2. **Associativity**: If $a, b, c \in G$, then $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.
  3. **Identity**: $\forall a \in G$, there exists an identity element e, such that $e \bullet a = a \bullet e = a$.
  4. **Inverse**: For all $a \in G$, $\exists\ a'$, called the inverse of a, such that $a \bullet a' = a' \bullet a = e$.

  If a group which satisfies above four properties along with commutative property is called commutative group or Abelian group. Commutative property means $\forall a, b \in G$, we have $a \bullet b = b \bullet a$.

  Finite Group: If a set contains a finite number of elements, then it is called finite group, otherwise it is an infinite group.
  Order of a Group: Total number of elements that contains in a group is called order of a group, i.e, $|G|$.
  Subgroups: A subgroup is a subset of group and subgroup itself is a group. If **G** and **H** are two groups of same operation and elements of **H** is a subset of element of **G**, then **H** is subgroup of **G**. The above definition implies that:

  - If $a, b \in$ **G** *and* **H**, then $c = a \bullet b \in$ **G** *and* **H**.
  - Both group and subgroup share the same identity element.
  - If $a \in$ **G** *and* **H**, then $a' \in$ **G** *and* **H**.
  - The group made of identity element of **G**, **H** $=< \{e\}, \bullet >$ is a subgroup of **G**.

– Each group is a subgroup of itself.

Cyclic Subgroups: A subgroup of a group is called cyclic subgroup, if all the elements of group generated using the power of an element. The term power means repeatedly applying the group operation to the element.

$$a^n \rightarrow a \bullet a \bullet ... \bullet a(n\ times)$$

Cyclic Groups: The element that generates all the elements of cyclic subgroup can also generate all the elements group is called a generator. A cyclic group is a group that itself own cyclic subgroup. If g is a generator, the element in the finite group can be written as
$\{e, g, g^2, ..., g^{n-1}\}$,where $g^n = e$

- **Rings**: A Ring(R) is a set with two binary operations. It is denoted as $R =< \{...\}, \bullet, \square >$. The first and second operation must satisfy all five and two properties respectively. In addition, the second operation must be distributed over first, means that for all a, b, and c elements of R we have $a\square(b \bullet c) = (a\square b) \bullet (a\square c)$ and $(a \bullet b)\square c = (a\square c) \bullet (b\square c)$. If the second operation satisfies commutative operation, then ring is called commutative ring.

- **Fields**: A Field(F) is a set of elements with binary operation, denoted as $F =< \{...\}, \bullet, \square >$. Both two operation satisfies all five properties except the identity of the first operation has no inverse.

3.2 Hash Function

A hash function takes a group of characters and maps it to a value of a certain length called a hash value or message digest. The hash value is representative of the original string of characters, but is normally smaller than the original. Hash function is mainly used to generate a fixed length of string. It is also used to check, where two objects are same or not. Hash function generates same result, if two

input string are same, so it is called deterministic. There are different type of design approach of hash function likes MD, MD2, MD4, MD5, SHA, SHA1, SHA2, SHA3. I have use SHA1 in our scheme.

In our proposed work, we used SHA1 hash function for experimental use. SHA1 takes maximum $2^{64} - 1$bit length of input string and generates 160bit length of output string. SHA1 is collision free hash function, so we used in our proposed work.

3.3 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz as an alternative mechanism for implementing public-key cryptography based on elliptic curve over finite field. ECC is based on discrete logarithm that is much more difficult to challenge at equivalent key lengths as compare to other public key cryptography. It uses smaller key as compare to other public key cryptography with same security level. So, it is used widely in lower resource system like mobile communication.

3.3.1 Elliptic Curve

An elliptic curve is define as a nonsingular cubic curve over finite field in two variables, $f(x, y) = 0$, with a rational point (which may be a point at infinity) which satisfy the equation: $y^2 = x^3 + ax + b$. The field K is generally taken to be the complex numbers, reals, rationales, or a finite field.

3.3.2 Why ECC?

The National Institute of Standards and Technology recommended the key sizes to protect keys used in conventional encryption algorithms like the (DES) and (AES) together with the key sizes for RSA, Diffie-Hellman and elliptic curves that are

needed to provide equivalent security are given in the Table [3.1].

Table 3.1: Key sizes for equivalent security levels (in bits)

Symmetric	ECC	DH/DSA/RSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360

From given table, we conclude that if the symmetric key size is increase the required key sizes for RSA and Diffie-Hellman increase at a much faster rate than the required key sizes for elliptic curve cryptosystems. Hence, elliptic curve systems offer more security per bit increase in key size than either RSA or Diffie-Hellman public key systems [35].

3.3.3 Elliptic Curves over GF(p)

An elliptic curve E over R (real numbers) is defined by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

The Weierstrass equations can be simplified by performing the following change of variables:

$$(x, y) \rightarrow (x - \frac{a_2}{3}, y - \frac{a_1x + a_3}{2})$$

and set $a_1 = 0, a_3 = 0$

$$a = \frac{1}{9a_2^2} + a_4, b = \frac{2}{27a_2^3} - \frac{1}{3a_2a_4a_6}$$

we get one of the simplified Weierstrass equations:$y^2 = x^3 + ax + b$ where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0$, together with a special point 0 called the point at infinity.

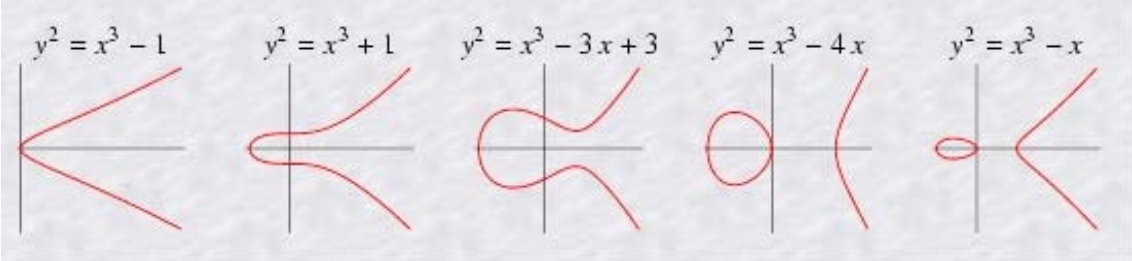

Figure 3.1: Elliptic Curve

Point addition

Addition of two point in elliptic curve is defined as a line between two point and the intersection of line in the elliptic curve. The negative of the intersection point is used as the result of the addition.

The operation is denoted by $P + Q = R$, or $(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$. This can algebraically be calculated by:

$$\lambda = \frac{y_q - y_p}{x_q - x_p}$$

$$x_r = \lambda^2 - x_p - x_q$$

$$y_r = \lambda(x_p - x_r) - y_p$$

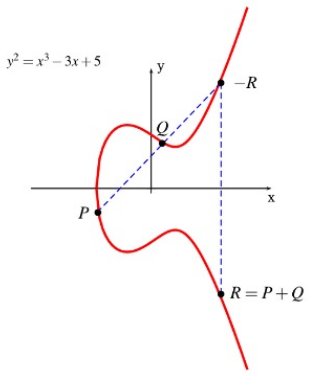

Figure 3.2: Point Addition Image

Point doubling

Point doubling in elliptic curve is defined as a tangent of the point and the intersection of line in the elliptic curve. The negative of the intersection point is used as the result of the addition.

$$\lambda = \frac{3x_p^2 + a}{2y_p}$$

$$x_r = \lambda^2 - 2x_p$$

$$y_r = \lambda(x_p - x_r) - y_p$$

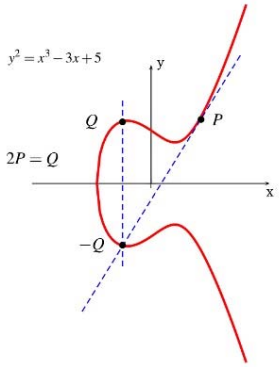

Figure 3.3: Point Doubling Image

Point multiplication

Point multiplication is nothing but scalar multiplication is defined as repeated addition of point. There is a method for point multiplication called double and square method, which is similar to multiply and square method in modular exponentiation. The algorithm is given as follows:

For computing dP, take the binary representation for $d : d = d_0 + 2d_1 + 2^2d_2 + \cdots + 2^m d_m$, where $[d_0..d_m] \in 0, 1$

3.4 Elliptic Curve Hardest Problem

This section describes definition of the hard computational problems in which the security of the proposed scheme relies [27].

3.4.1 Elliptic Curve Discrete Logarithm Problem

With the given two point of an elliptic curve A and B, where $A = k.B$, it is difficult to find out the value of k.

3.4.2 Elliptic Curve Diffie-Hellman Problem

With the given two points of elliptic curve A and B, where $A = c.G$ and $B = d.G$ without c and d, it is difficult to find out another point $K = c.d.G$.
The ECDLP and ECDHP is a computational infeasible problems [30].

3.5 Summary

In this chapter, we briefly discussed mathematical background of our thesis work. All the mathematics we define are being use in our proposed work.

Chapter 4

ID-based Signcryption Scheme Based on ECC

In this chapter, we proposed an identity based signcryption scheme based on elliptic curve cryptography. The scheme, based on the concept of Li et al. [10], which allow ID and message of arbitrary length, collision resistance hash function and used a secure one time symmetric key encryption scheme.

4.1 Formal model of identity-based signcryption

An identity-based signcryption scheme consists of the following four algorithms [8].

- **Setup**: Here, the private key generator (PKG) takes input as security parameter k and generates the system's public parameters *params* and a master secret s. PKG publishes params and keeps the master secret to itself.
- **Extract**: Given an identity ID_u, the PKG computes the corresponding private key x_u and transmits it to its owner in a secure way.
- **Signcrypt**: To send a message m from Alice to the receiver Bob whose identity is ID_b, Alice computes cipher text c using algorithm Signcrypt(m, x_a, y_b).

- **Unsigncrypt**: After receiving ciphertext c, Bob computes Unsigncrypt(c, y_a, x_b) and generates the plain text m if the ciphertext is valid between two identities otherwise the symbol $\perp$.

4.2 Proposed Scheme

This scheme consists of three parts, namely PKG, Signcryptor and Receiver. The PKG provides private and public key of all parties, when they join first time in the network. There are four phases in the proposed scheme: Setup, Extract, Signcrypt, Unsigncrypt. In the initial phase, the system chooses and publishes all the parameter of elliptic curves and PKG generates private key and the related public key of each user in the network.

- **Setup**: Here, PKG selects and publish system security parameters are given below.

  q is a large prime number.

  (a, b) two elliptic curve element which is smaller than q satisfying the equation $4a^3 + 27b^2 \neq 0$ and $q \neq 0$.

  F the elliptic curve over finite field which satisfying the equation $q : y^2 = x^3 + ax + b$ mod q.

  G a generator of elliptic curve.

  0 a point at infinity of elliptic curve and n the order of F, which satisfy $n.G = 0$.

  Hash functions $H : \{0, 1\}^* \rightarrow Z_q$ and PKG choose a number s as master secret and compute master public key $R = s.G$.

  Publish parameter (q, G, a, b, H, R).

- **Extract**: If U has the identity ID_u, the PKG computes the private key of signcryptor as follows.

$$X_u = (H(ID_u)).s \, mod \, q$$

and compute its public key as $Y_u = X_u.G$

The PKG generates private and public key of the sender and receiver as follows.

$$X_s = (H(ID_s)).s \; mod \; q \tag{4.1}$$

$$Y_s = X_s.G \tag{4.2}$$

$$X_r = (H(ID_r)).s \; mod \; q \tag{4.3}$$

$$Y_r = X_r.G \tag{4.4}$$

- **Signcrypt**: Sender chooses a random number $r \in [1....(q-1)]$ and computes,

$$Z = r.G \tag{4.5}$$

$$K = ID_r.r.Y_r = (K_1, K_2) \tag{4.6}$$

$$c = E_{K_1}(m) \tag{4.7}$$

$$h = Hash(m, ID_s, ID_r, K_2) \tag{4.8}$$

$$S = ID_r.r - ID_s.h.X_s.Z \tag{4.9}$$

The cipher text is (c, h, S, Z)

- **Unsigncrypt**:The receiver receives ciphertext (c, h, S, Z), and computes,

$$K = S.Y_r + ID_s.h.Z.Y_s.X_r = (K_1, K_2) \tag{4.10}$$

$$m' = D_{K_1}(c) \tag{4.11}$$

$$h' = Hash(m', ID_s, ID_r, K_2) \tag{4.12}$$

Verify, if $(h = h')$ then receiver accepts the signature.

4.3 Security analysis of the proposed scheme

In this section, the correctness of the proposed signcryption scheme is evaluated. Then, there is a brief discussion of the security aspects of the proposed scheme. We also proof that the proposed scheme provides all the security goals.

4.3.1 Correctness

The signcrypted text (c, h, S, Z) is a valid one; its correctness is given below.

$$\begin{aligned} K &= S.Y_r + ID_s.h.Z.Y_s.X_r \\ &= (ID_r.r - ID_s.h.X_s.Z).Y_r + ID_s.h.Z.Y_s.X_r \\ &= ID_r.r.Y_r - ID_s.h.X_s.Z.Y_r + ID_s.h.Z.Y_s.X_r \\ &= ID_r.r.Y_r - ID_s.h.Z.X_s.Y_r + ID_s.h.Z.X_s.G.X_r \\ &= ID_r.r.Y_r - ID_s.h.Z.X_s.Y_r + ID_s.h.Z.X_s.Y_r \\ &= ID_r.r.Y_r \end{aligned}$$

4.3.2 Security Proof

The proposed work provides message confidentiality, integrity, authentication, non-repudiation, unforgeability, and forward secrecy.

Confidentiality

The proposed scheme provides message confidentiality. If an attacker tries to obtain the original message from the ciphertext, he must know the secret parameter K. Now we discuss some ways that attacker can try to obtain the secret key K.

$$K = ID_r.r.Y_r \tag{4.13}$$

$$Z = r.G \tag{4.14}$$

Suppose the attacker tries to derive secret key K from Eq. (4.13), he must find out secret parameter r from Eq. (4.14). But the Eq. (4.14) has properties ECDLP. So, it is infeasible to solve to derive K from Eq. (4.13) and (4.14).

$$R = s.G \tag{4.15}$$

$$K = H(ID_r).ID_r.r.s.G \tag{4.16}$$

If the attacker tries to derive secret K, by using Eq. (4.16) from Eq. (4.14) and Eq. (4.15), then attacker has to solve the hardest ECDHP.

$$S = ID_r.r - ID_s.h.X_s.R \tag{4.17}$$

$$K = S.Y_r + ID_r.h.Z.Y_s.X_r \tag{4.18}$$

It is also possible to derive K from Eq. (4.18) by using Eq. (4.17), but the attacker has to gotten X_r, which is infeasible to derive. Therefore, proposed scheme provides message confidentiality.

Authentication

The recipient uses public key Y_s and certificate S in Eq. (4.18) for verifying sender authentication. The sender signed with its private key X_s in Eq. (4.17). So, in the proposed scheme recipient can authenticate identity of sender.

Integrity

In the proposed scheme, the receiver can verify that whether the ciphertext is tampered or not at the time of transmission.

$$h = Hash(m, ID_s, ID_r, K_2) \tag{4.19}$$

If the attacker change the cipher text c to c'. Then the original message in Eq. (4.19) also change from m to m'. At the time of verification it is infeasible in one way hash function that $h = h'$. Therefore, our scheme provides integrity.

Unforgeability

Unforgeability ensure that, the attacker can't create a valid ciphertext. In the proposed scheme, the attacker cannot create a valid (c, h, S, Z) without the private key of the sender. If an attacker forge a valid $(c,', h', S', Z')$ from previous (c, h, S, Z), then (c', h', S', Z') has to satisfy Eq. (4.18).
To generate a correct h' and S', the attacker must get random secret r. But the attacker can't get the correct random secret r and S. To obtain r from $Z = r.G$, then attacker should have to solve ECDLP firstly but it computationally infeasible. Therefore, proposed scheme prevents the properties of unforgeability.

Non-Repudiation

In proposing schemes the recipient can know from Eq. (4.18), whether the original message send by sender or not. As the sender sign with his private key in Eq. (4.17), the recipient can verify. So proposed scheme provides non-repudiation.

Forward Secrecy

The proposed scheme ensures that, if the sender private key is lighted, but attacker can't recover original message m from ciphertext (c, h, S, Z). In our scheme if an attacker tries to derive plain text m, he has to decrypt its cipher text by secret key K. Therefore our proposed scheme provides forward secrecy.

4.4 Comparison

We compare cost of our proposed work with some elliptic curve cryptography schemes and try to reduce the cost of computation. We have used some notation to define number of operation, in the Table [4.1] are given below.
MUL= modular multiplication operation.
DIV= modular division operation.

ADD= modular addition operation.

ECPM= elliptic curve point multiplication operation.

ECPA= elliptic curve point addition operation.

HASH= one way hash function.

Table 4.1: Comparison based on the Computational Cost

Schemes	MUL	DIV	ADD	ECPM	ECPA	HASH
Hwang	1	0	1	5	1	2
Zheng	3	1	1	3	1	4
Proposed Scheme	3	0	1	5	0	2

4.5 Implementation

All the security schemes are operated by large number to protect different type of attacks. Java has a special class for implementing security schemes, called BigInteger class. The proposed scheme is implemented using java BigInteger class.

4.5.1 Block Diagram of Classes

The proposed scheme is using three classes that are given in the Fig.[4.1]. Signcryption.java, class is the base class, where the algorithm of the scheme is implemented. ECC.java class contains the elliptic curve parameters and different point operation. There is another class, that defines the x and y coordinates of elliptic curve points as well as some methods.

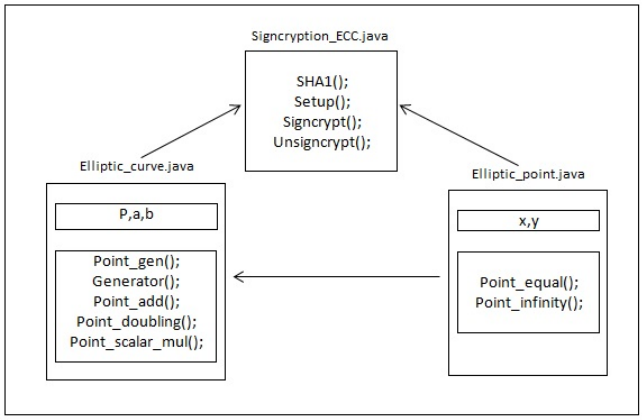

Figure 4.1: Block Diagram of Classes

4.5.2 Snapshot of Output

In our scheme we have used the SHA1, a one way hash function that take variable length of input and generates a 160bits of output. The elliptic parameters are chosen randomly and generate points in the curve. It takes an arbitrary length of message and calculates the cipher text and sends it to recipient. At the recipient end verify the signature and decrypt the message. The snapshot of the output is given below in Fig.[4.2].

4.6 Summary

In this chapter, we have described our proposed ID-based Signcryption Scheme Based on ECC. The proposed scheme consist of three algorithm and two different parties. We proof, the correctness of the scheme and also different type security goals that satisy the scheme.

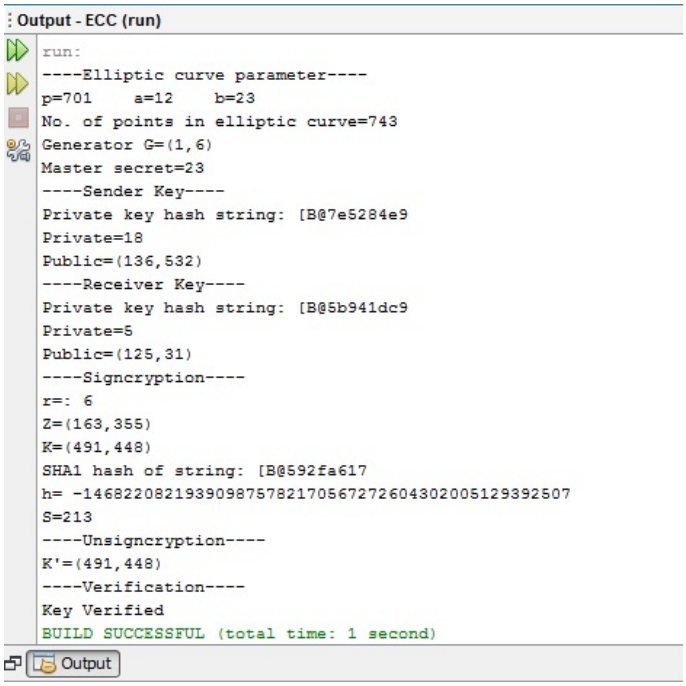

Figure 4.2: Snapshot of Output

Chapter 5

A Strong Designated Verifiable Signcryption Scheme Based on ECDLP

In this chapter, we proposed a Strong Designated Verifiable Signcryption Scheme Based on elliptic curve discrete logarithm problem. The scheme, based on the S. Mohanty and B. Majhi [25] proposed a strong designated verifiable signcryption scheme based on the discrete logarithm problem (DLP).

5.1 Existing Scheme

In this section, there is a brief discussion of S. Mohanty and B. Majhi [25] proposed scheme. The scheme consists of three algorithms, namely, setup, signcryption and unsigncryption with veificaion.

- **Setup**: The signcryptor(S) chooses $n = p.q$, where $p = 2fq'$ and $q = 2fq' + 1$. p, q, p', q' are distinct primes.

  The signcryptor chooses his private key $X_S \in Z_{q^*}$ and computes his public key

as follows.

$$Y_S = g^{X_S} \ mod \ p$$

The designated verifier also chooses his private key $X_R \in Z_{q^*}$ and computes his public key as follows.

$$Y_R = g^{X_R} \ mod \ p$$

- **Signcryption**: The signcryptor chooses $t \in Z_{q^*}$ and computes

$$K = {Y_R}^t \ mod \ p$$
$$C = E_K(m)$$
$$r = H(K)$$
$$s = t - r.X_S \ mod \ p$$

The signcryptor send the cipher text $\delta = (r, s, C)$ to designated verifier.

- **Unsigncryption**: After receiving $\delta = (r, s, C)$, the designated receiver computes K' as given below.

$$K' = (g^S {Y_S}^r)^{X_R} \ mod \ p$$

Then he verifies the authenticity of sender by checking the following condition.

$$r = H(K')$$

Then message m is recovered from the ciphertext as follows.

$$m = D_k(C)$$

5.2 Proposed Scheme

This scheme consists of two parties namely Signcryptor and Receiver. There are three phases in the scheme : Setup or key generation, Signcrypt and Unsigncrypt.

In the initial phase, signcryptor generates and publishes all the public parameter of elliptic curve as well as each user chooses his own private key and calculates his related public key.

- **Setup**: In this phase, signcryptor setup some elliptic curve parameter are given below.

  q is a prime number.

  (a, b) two integer element and $(a, b) < q$ satisfy $4a^3 + 27b^2 \neq 0 \bmod q$.

  F is the elliptic curve over finite field with order n, which satisfy equation $y^2 = x^3 + ax + b \bmod q$.

  G a base point of F.

  hash function $H : \{0, 1\}^* \rightarrow Z_q$.

  Publish parameter(q, G, a, b, H, n).

  Signcryptor chooses his private key $X_s \in [1, 2...(n-1)]$ and computes his public key as

$$Y_s = X_s.G = (Y_{s1}, Y_{s2}) \tag{5.1}$$

  Receiver also chooses his private key $X_r \in [1, 2...(n-1)]$ and computes his public key as

$$Y_r = X_r.G = (Y_{r1}, Y_{r2}) \tag{5.2}$$

- **Signcrypt**:Signcryptor chooses a random number $t \in [1....(n-1)]$ and computes

$$K = t.Y_r = (K_1, K_2) \tag{5.3}$$

$$c = E_{K_1}(m) \tag{5.4}$$

$$r = H(m, K_2) \tag{5.5}$$

$$s = (t - r.X_s) \ mod \ n \tag{5.6}$$

  The cipher text is $\delta = (c, r, s)$

- **Unsigncrypt**:The receiver receives ciphertext $\delta = (c, r, s)$ and computes

$$K' = s.Y_r + r.X_r.Y_s = (K'_1, K'_2) \tag{5.7}$$

The message is recovered from the cipher text $\delta = (c, r, s)$ as follows.

$$m' = D_{K'_1}(c) \tag{5.8}$$

Then he verifies the authenticity by checking the following condition.

$$r' = H(m', K'_2) \tag{5.9}$$

5.3 Security analysis of the proposed scheme

In this section, the correctness of the proposed signcryption scheme is evaluated. Then, there is a brief discussion of the security proof of the different type attack that the proposed scheme provides.

5.3.1 Correctness

The signcrypted text $\delta = (c, r, s)$ is a valid one; its correctness is given below.

$$\begin{aligned} K &= s.Y_r + r.X_r.Y_s \\ &= (t - r.X_s).Y_r + r.X_r.Y_s \\ &= t.Y_r - r.X_s.Y_r + r.X_r.X_s.G \\ &= t.Y_r - r.X_s.Y_r + r.X_s.Y_r \\ &= t.Y_r = (K_1, K_2) \end{aligned}$$

5.3.2 Security Proof

Definition 1: A signcryption scheme is said to have the indistinguishability against adaptive chosen ciphertext attack property, if no polynomially bounded adversary has a non-negligible advantages in the following game [8].

1. The challenger C runs the setup algorithm with security parameters and obtains common parameters params. He sent the parameter to adversary A.

2. The adversary A asks adaptively a polynomially bounded number of queries to signcryption and unsigncryption.

   - signcryption queries: In this phase, adversary chooses a message m along with an arbitrary recipient public key Y_r and sends them to the challenger. Then the challenger, runs the signcryption algorithm signcrypt(m, X_s, Y_r) with private key of signcryptor X_s and send ciphertext back to adversary.
   - unsigncryption queries: In this phase, adversary A submits a ciphertext C for decryption to the challenger. Then the challenger runs the signcrypt algorithm unsigncrypt(C, X_r, Y_s). If the plaintext is valid for the recovered signcryptor's public key, then the challenger returns the plaintext to A, otherwise the challenger returns the symbol $\perp$.

3. A chooses two plaintexts, m_0 and m_1, and an arbitrary private key X_s, on which he wishes to be challenged. Challenger chooses randomly a bit b, computes δ=Signcrypt(m_b, X_s, Y_r) and sends it to A.

4. A asks a polynomial number of queries adaptively again as in the first stage. It is not allowed to make query the unsigncryption corresponding to δ.

5. Finally, A produces a bit b' and wins the game if $b' = b$. The advantage of A is given as

$$Adv(A) = \Pr[b' = b] - 1/2$$

Proof: We proof the scheme based on above game that, the proposed scheme is secure against adaptive chosen ciphertext attack.

We assume that, the adversary chooses a signcryptor's private key and two message m_0 and m_1 of equal length and send them to challenge. The challenger then chooses a random b and compute the ciphertext δ with given receiver public key Y_r.

$$\delta = (c, r, s)$$

Adversary after receiving the challenge ciphertext δ, he first guess of b and generates a new ciphertext by choosing a random message m'. Then he chooses a random $X'_s \leftarrow z_q*$. Then A computes,

$$Y'_s = X'_s.G \tag{5.10}$$

$$K' = t'.Y_r = (K'_1, K'_2) \tag{5.11}$$

$$c' = E_{K'_1}(m') \tag{5.12}$$

$$r' = H(m', K'_2) \tag{5.13}$$

$$s' = (t' - r'.X'_s) \ mod \ n \tag{5.14}$$

The adversary then send the challenge ciphertext δ' to challenger for unsigncryption. After receiving ciphertext $\delta' = (c', r', s')$, the challenger computes $K = s'.Y_r + r'.X_r.Y_s = (K_1, K_2)$ and $m' = D_{K_1}(c)$

If $r = H(m', K'_2)$, then challenger returns the message m, otherwise rejects the message. The response is automatically rejected because $K' \neq K$ as X'_r can not be computed from Y_r, whose complexity elliptic curve discrete logarithm problem. So, we conclude that proposed scheme is prevent against adaptive chosen ciphertext attack.

Definition 2: The proposed signcryption scheme is unforgeable against chosen message attack.

proof: In proposed work, the attacker cannot create a valid ciphertext (c, r, s) without private key of sender. The computational complexity of sender private key is under hardness of elliptic curve discrete logarithm problem.

In case, the value K is leaked or compromised, the attacker can not generates s as it required two parameter, t and X_s. If attacker want to derive t from $K = t.Y_r$, he should have to solve ECDLP firstly, it computationally infeasible. Therefore, the proposed scheme satisfy the properties of unforgeability.
Definition 3: In proposed signcryption scheme the signcrypted message can not verify other than the designated receiver

Proof: In proposed scheme, one time symmetric key is generated using public key of designated receiver. To verified signcrypted message, one time symmetric key is generated from private key of designated receiver that is computationally hardness under ECDLP.

If the the private key of signcryptor(X_s) is compromised, the adversary A generates the signcrypted text δ before the designated receiver R receive it, the adversary can not verify the signature, because the signature is only verified by designated receiver that is protected under hardness of ECDLP.

5.4 Implementation

We implement this scheme in java using java BigInteger class. In this work, we used SHA1 a one way hash function, an elliptic curve class and a point class. The algorithm generates all elliptic curve points by choosing elliptic curve parameters. From all points one of the points chosen as generator, which can generate all the points of elliptic curve by scalar multiplication. Then the algorithm calculates privates and public key of sender and receiver using generator. In signcryption phase, sender calculates cipher text and sends it to receiver. In unsigncryption phase, receiver verifies sender identity and decrypts the message. The snapshot of output is given below in Fig.[5.1].

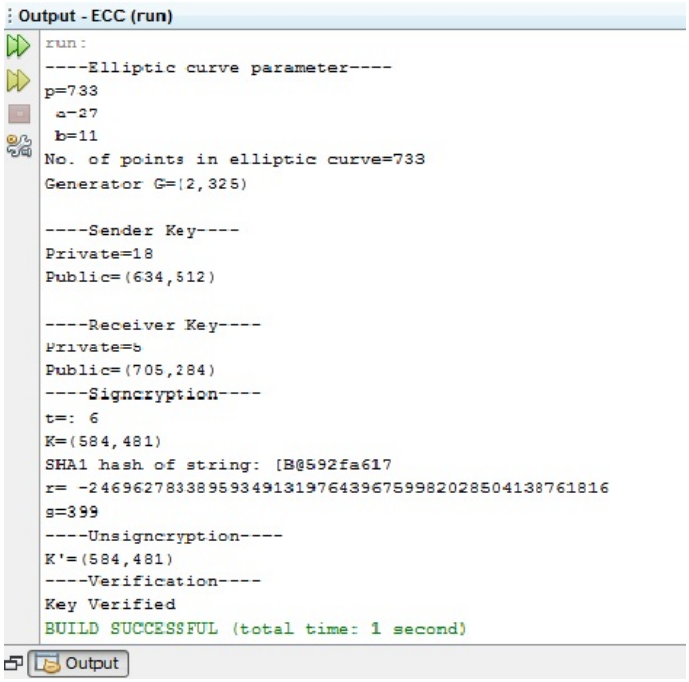

Figure 5.1: Snapshot of Output

5.5 Summary

In this chapter, we have introduced a strong designated verifiable signcryption scheme based on ECDLP. We also proved that, the proposed scheme is secure against chosen ciphertext attack and unforgeability. We have implemented this scheme in java and result is also given.

Chapter 6

Conclusion

Our proposed schemes based on ECDLP and ECDHP simultaneously provides message confidentiality, unforgeability, non-repudiation, integrity, authentication and forward security. The proposed schemes achieve the security properties with a saving in computational cost compared to the traditional signature the encryption scheme which makes the new scheme more appropriate for environment with limited power. Finally, the proposed schemes have low computational and communication cost so, can be applied to a smart phone environment more efficiently.

Scope for Further Research

In ID-based signcryption, a third is used to generate the private key of users called a private key generator (PKG). There is a problem of key escrow in ID-based signcryption that key is held in escrow, or stored, by a third party. So, to avoid this problem the proposed works can be design in certificateless signcryption.

Bibliography

[1] Zheng, Yuliang. "Digital signcryption or how to achieve cost (signature & encryption)? cost (signature)+ cost (encryption)." Advances in Cryptology-CRYPTO'97. Springer Berlin Heidelberg, 1997. 165-179.

[2] Zheng, Yuliang, and Hideki Imai. "How to construct efficient signcryption schemes on elliptic curves." Information Processing Letters 68.5 (1998): 227-233.

[3] Baek, Joonsang, Ron Steinfeld, and Yuliang Zheng. "Formal proofs for the security of signcryption." Journal of cryptology 20.2 (2007): 203-235.

[4] Steinfeld, Ron, and Yuliang Zheng. "A signcryption scheme based on integer factorization." Information Security. Springer Berlin Heidelberg, 2000. 308-322.

[5] A. Shamir. "Identity-based cryptosystems and signature schemes", in Proc. Advances in Cryptology-CRYPTO'84, LNCS 196, Springer-Verlag, pp. 47-53, 1984.

[6] J. Malone-Lee, "Identity-Based Signcryption," Cryptology ePrint Archive, Report 2002/098, 2002.

[7] D. Boneh, and M. Franklin. "Identity-based encryption from the weil pairing", in Proc. Advances in CryptologyCRYPTO 2001, LNCS 2139, Springer-Verlag, pp. 213-29, 2001.

[8] Yu, Yong, et al. "Identity based signcryption scheme without random oracles."Computer Standards & Interfaces 31.1 (2009): 56-62.

[9] Jin, Zhengping, Qiaoyan Wen, and Hongzhen Du. "An improved semantically-secure identity-based signcryption scheme in the standard model." Computers & Electrical Engineering 36.3 (2010): 545-552.

[10] Fagen, L. I., and Q. I. N. Zhiguang. "Analysis of an identity-based signcryption scheme in the standard model." IEICE transactions on fundamentals of electronics, communications and computer sciences 94.1 (2011): 268-269.

[11] Bao, Feng, and Robert H. Deng. "A signcryption scheme with signature directly verifiable by public key." Public Key Cryptography. Springer

[12] Berlin Heidelberg, 1998.Gamage, Chandana, Jussipekka Leiwo, and Yuliang Zheng. "An efficient scheme for secure message transmission using proxy-signcryption."Proceedings of the Twenty Second Australasian Computer Science Conference. 1999.

[13] Jung, Hee Yun, et al. "Signcryption schemes with forward secrecy."Proceedings of WISA2001, Springer-Verlag (2001).

[14] Hwang, Ren-Junn, Chih-Hua Lai, and Feng-Fu Su. "An efficient signcryption scheme with forward secrecy based on elliptic curve." Applied Mathematics and computation 167.2 (2005): 870-881.

[15] Shin, Jun-Bum, Kwangsu Lee, and Kyungah Shim. "New DSA-verifiable signcryption schemes." Information Security and Cryptology-ICISC 2002. Springer Berlin Heidelberg, 2003. 35-47.

[16] Tso, Raylin, Takeshi Okamoto, and Eiji Okamoto. "An improved signcryption scheme and its variation." Information Technology, 2007. ITNG'07. Fourth International Conference on. IEEE, 2007.

[17] Toorani, Mohsen, and Ali Asghar Beheshti Shirazi. "An Elliptic Curve-Based Signcryption Scheme with Forward Secrecy." Journal of Applied Sciences 9.6 (2009).

[18] Barreto, P.S.L.M., Libert, B., McCullagh, N. and Quisquater, J.-J., Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, ASIACRYPT 2005, pp. 515-532, 2005.

[19] Chow, Sherman SM, et al. "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity."Information Security and Cryptology-ICISC 2003. Springer Berlin Heidelberg, 2004. 352-369.

[20] Boyen, Xavier. "Multipurpose identity-based signcryption." Advances in Cryptology-CRYPTO 2003. Springer Berlin Heidelberg, 2003. 383-399.

[21] Chen, Liqun, and John Malone-Lee. "Improved identity-based signcryption." Public Key Cryptography-PKC 2005. Springer Berlin Heidelberg, 2005. 362-379.

[22] M. Jakobsson, K. Sako, and R. Impagliazzo, Designated verifier proofs and their applications, Advances in Cryptology-Eurocrypt 1996, LNCS1070, Springer-Verlag, 1996, pp.143-154.

[23] S. Saeednia, S. Kremer, O. Markowitch, An efficient strong designated verifier signature scheme, ICISC'03,Vol. 2971, Springer,Berlin, 2004, pp.40-54.

[24] J. Lee and J. H. Chang. Comment on Saeednia et al.'s strong designated verifier signature scheme. Computer Standards & Interfaces, Vol.31 (2009), pp.258-260.

[25] Mohanty, Sujata, and Banshidhar Majhi. "A Strong Designated Verifiable DL Based Signcryption Scheme." JIPS 8.4 (2012): 567-574.

[26] Zhang, Bo. "Cryptanalysis of an identity based signcryption scheme without random oracles." Journal of Computational Information Systems 6.6 (2010): 1923-1931.

[27] Hwang, Ren-Junn, Chih-Hua Lai, and Feng-Fu Su. "An efficient signcryption scheme with forward secrecy based on elliptic curve." Applied Mathematics and computation 167.2 (2005): 870-881.

[28] Zheng, Yuliang, and Hideki Imai. "How to construct efficient signcryption schemes on elliptic curves." Information Processing Letters 68.5 (1998): 227-233.

[29] Han, Yiliang, Xiaoyuan Yang, and Yupu Hu. "Signcryption based on elliptic curve and its multi-party schemes." Proceedings of the 3rd international conference on Information security. ACM, 2004.

[30] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), International Journal of Information Security 1 (1) (2001) 36-63.

[31] Elkamchouchi, Hassan M., Eman F. Abu Elkhair, and Yasmine Abouelseoud. "AN EFFICIENT PROXY SIGNCRYPTION SCHEME BASED ON THE DISCRETE LOGARITHM PROBLEM." International Journal of Information Technology (2013).

[32] Behrouz A. Forouzan. Cryptography and Network Security. Tata McGraw-Hill,2007.

[33] http://ijcta.com/documents/volumes/vol2issue4/ijcta2011020439.pdf

[34] Li, Fagen, and Muhammad Khurram Khan. "A Survey of Identity-based Signcryption." IETE Technical Review 28.3 (2011).

[35] http://www.nsa.gov/business/programs/elliptic-curve.shtml