Certificateless Blind Signature

based on DLP

Samir Kumar

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India
May 2015

Certificateless Blind Signature based on DLP

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Samir Kumar

(Roll Number - 213CS2162)

Under the supervision of

Prof. Sujata Mohanty

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

May 2015

Dedicated to My Parents and Siblings

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India.

Certificate

This is to certify that the work in the dissertation entitled ***" Certificateless Blind Signature Based on Discrete Logarithmic Problem "*** presented by ***Samir Kumar*** is a record of an unique research work carried out by him under our supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science and Engineering with specialization in **Information Security**, National Institute of Technology, Rourkela. Neither this dissertation nor any part of it has been submitted for any degree or academic award elsewhere.

Dr. Sujata Mohanty
Assistant Professor
Department of CSE
National Institute of Technology, Rourkela

Place: NIT,Rourkela

Author's Declaration

I hereby declare that all work contained in this report is my own work unless otherwise acknowledged. Also, all of my work has not been submitted for any academic degree. All sources of quoted information has been acknowledged by means of appropriate reference.

Samir Kumar
Roll No.: 213CS2162
Department of Computer Science
NIT Rourkela

Acknowledgment

As a matter of first importance, I might want to express my profound feeling of appreciation towards my supervisor Prof Sujata Mohanty, who has been the directing compel behind this work. I need to express gratitude toward her for acquainting me with the field of Digital Signature and issuing me the chance to work under her. Her unified confidence in this point and capacity to draw out the best of explanatory and viable abilities in individuals has been significant in extreme periods. Without her significant counsel and help it would not have been workable for me to finish this proposition. I am enormously obligated to her for her consistent support and priceless exhortation in every part of my scholastic life. I think of it as my favorable luck to have got a chance to work with such a sublime individual.

I wish to show my gratitude to all faculty members and secretarial staff of the CSE Department for their generous cooperation.

During my studies at N.I.T. Rourkela, I made many friends. I would like to thank them all, for all the great moments I had with them.

When I look back at my accomplishments in life, I can see a clear trace of my family's concerns and devotion everywhere. My dearest mother, whom I owe everything I have achieved and whatever I have become; my beloved father, for always believing in me and inspiring me to dream big even at the toughest moments of my life; and my brother and sister; who were always my silent support during all the hardships of this endeavor and beyond.

Samir Kumar

Abstract

The most widely used digital signature in the real word application such as e cash e-voting etc. is blind signature. Previously the proposed blind signature follow the foot steps of public key cryptography(PKC) but conventional public key cryptography uses an affirmation of a relationship between public key and identity for the holder of the corresponding private key to the user, so certificate management is very difficult. To overcome this problem Identity based cryptography is introduced. But Identity based cryptography is inherited with key escrow problem. Blind signature with certificateless PKC(CLBS) used widely because it eliminate the problem related to certificate management of cryptography and the key escrow problem of ID based PKC. Because of large requirement of CLBS scheme in different applications many CLBS scheme is proposed, but they were based on bilinear pairing. However, the CLBS scheme based on bilinear pairing is not very satisfiable because bilinear pairing operations are very complicated.

In our proposed scheme, we designed a certificateless blind signature scheme based on the discrete logarithmic problem. The proposed scheme fulfills all the security requirements of blind signature as well as certificateless signature. We analyzed security properties such as blindness, unforgeability and unlinkability. The proposed scheme has less computational cost. The hardness of discrete logarithmic problem (DLP) is used to prove the security of the proposed scheme.

Contents

List of Figures

List of Tables

List of Abbreviations

BS . . . . . Blind Signature

IND CCA1 . . . Indistinguishability Chosen Ciphertext Attack

IND CCA2 . . . Indistinguishability Adaptive Chosen Ciphertext Attack

DLP . . . . . Discrete Logarithmic Problem

IFP . . . . . Integer Factorization Problem

CDH . . . . . Computational Diffie-Hellman Problem

DDH . . . . . Desicion Diffie-Hellman Problem

IDB-PKC . . . . Identity Based Public key cryptography

CLS-PKC . . . Certificateless Public key cryptography

CLBS . . . . . Certificateless Blind signature

Chapter 1

Introduction

A significant trouble in creating secure frameworks taking into account public key cryptography is management of frameworks to backing the cryptographic keys authenticity. An affirmation is needed for the relationship between public key and their corresponding private key.

In conventional public key cryptography(PKC) there an assertion is needed about the binding between public key of user and private key of user, because public key is open for all so attacker use that key to send the message to receiver. in a conventional PKC, there is a certificate authority(CA), who keep relationship between public and private keys[1]. The main problems of conventional PKC are management of certificate and revocation also in key storage, key distribution and the certificate verification computational cost is also very high. These are especially intense in processor or transmission capacity restricted situations.

For resolving the problems of conventional PKC a new mechanism is proposed by, Shamir (in 1984) called the Identity Based Public key Cryptography (IDB-PKC) [21].In IDB-PKC user identification like user ID or user system IP address is declared as public key of user.

In ID based-PKC a trusted third party called TTP is used that receive the public key of user(user IP address or email id) and on the basis of this public key user private key is generated, hence no certification authority is required. From one point of view the immediate determination of public keys in IDB-PKC kills the prerequisite for certificates and a rate of the issues connected with them. Then again the reliance on a TTP, who utilizes a framework to create private keys, inexorably acquaints key escrow with ID based-PKC

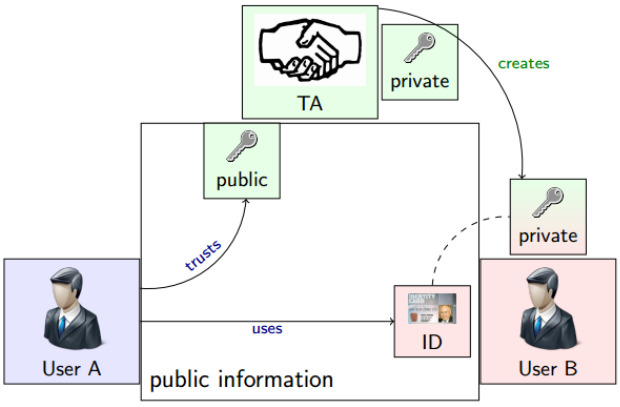

Figure 1.1: ID-Based Public Key Cryptography[20]

frameworks. ID-PKC inherently has the key escrow problem(KEP). key escrow problem is the problem where TTP has ability to decrypt any cipher-text in an ID based-PKC scheme. Therefore, ID based-PKC can't offer genuine non- denial in the same way as that of in standard conventional-PKC. The key escrow problem can be settled to a some percentage, by the use of different PKGs and the utilization of limit methods , yet it fundamentally includes additional correspondence and framework. Consequently, this cryptosystem may very well be suitable for minimal private frameworks with restricted security prerequisites.

To handle the problem related to management of certificate in the TR-PKC and the problem related to IDB-PKC like key escrow problem, Al-Riyami and Paterson (2003) proposed the idea of the certificateless public key cryptography(CLSPKC)[3]. In CLS-PKC there is a PKG(Private key generator) in place of trusted third party. Like TTP in ID-PKC here private key generator(PKG). In PKG using master key and user ID PKG generate partial private key(PPK), and using PPK and secret key of user's private key is generated. Hence PKG doesn't have information about user's private key. In CLS-PKC there is no direct relationship between public key of user and private key of user. The capacity and correspondence data transmission of CLS-PKC is less because of the identifier only contains applicable data certificate-related information are not required.

1.1 Introduction of Certificateless Cryptography:

In CL-PKC in the place of TTP there is PKC private key generator having own secret key called master key. PKC doesn't has the information about user key. He know only user

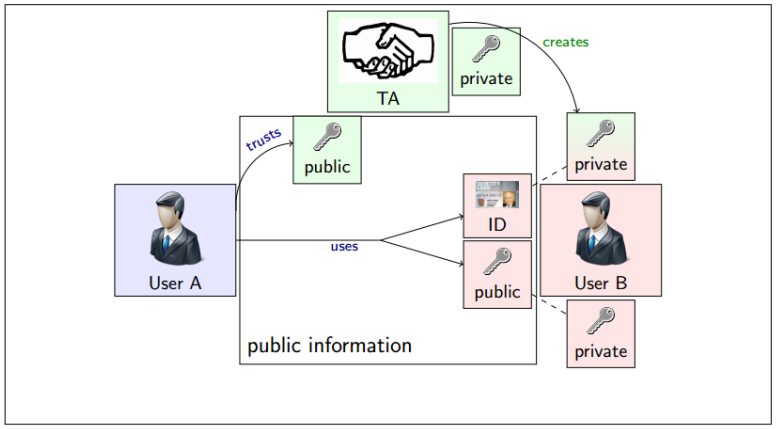

Figure 1.2: Certificateless Public Key Cryptography[20]

identity and on the basis of that identity and system parameter with master key PPK is generated. user select a secret key, using this and secret key and partial private key the user private key is generated.

A CLBS is defined in the following 7 phases.

1. **Set up phase:** PKG runs the key setup algorithm. For this algorithm security parameters are available. The algorithm takes security parameters as input and output a master key and a parameter list param. param is declared public and keep master private key private.

2. **Partial private key generation phase:**PKG taken public parameters using user ID and master private key calculates partial private key.

3. **User Secret key generation phase:**User Key generation: Secret key generation phase: User secret key use for generating full private key of user. User chooses his private key chosen from the set that are available in param.

4. **User private key generation phase:** User Generates full private key us using PPK and user secret key.

5. **User public key generation phase:** User public key is generating at this step using secret key of user and master public key. So here no direct relationship between public key of user and private key of user. User can generate any key first either public or private.

6. **Encrypt:** In this phase, the message m is encrypted available parameters for this phase are a message msg, system parameters params, the public key of user and

identity of user. It gives cipher-text of mesage m as output. It may output null symbol if the encryption failure.

7. **Decrypt:** In this phase using private key and input parameters with cipher-text, it returns a message msg if the decryption occur sucessfully otherwise return a null value if the decryption failure.

1.2 Digital Signature

Digital signature is an electronic signature used in the authenticity, validity, and integrity of a message[14]. Digital signature is not included with the document like conventional signature, it is send as a separate document. A digital signature is asymmetric key system in which the document signs by signer with his/her private key and verifier verifies it using public key of signer. A secure digital signature scheme provide message authentication, message integrity and non repudiation.

1.3 Blind Signature

Blind signature is a type of digital signature. In BS a signer signs the message without knowing the content of the message. Initially this scheme is proposed by David Chaum (1983)[7]. The blind signature scheme generally utilized into electronic voting and electronic money because of the properties of its for example, anonymity, blindness, and unforgeability[8].

In Blind signature scheme bob will get a valid signature from the signer Alice without disclosing the contents of the message as well as the signature to her. Alice will be able to verify the signature after getting message m and signature but cannot link the message and signature pair to the to the definite occurrence of the signing phase.

It permits to acknowledge secure electronic payment frameworks ensuring client's protection and other cryptographic conventions securing the members' obscurity (e.g. secure voting conventions). At first this idea appears a bit peculiar why would you need to sign something without seeing it. Things being what they are, when connected appropriately, this thought has some extremely decent applications in circumstances where obscurity is a major issue.

Two such applications are digital cash and internet voting. When you present an online vote, you may like for that vote to be mysterious so nobody can tell whom you voted in favor of. So also with electronic money, you may not need another person to know who you are the point at which you spend it. This is like typical paper money - when you make a purchase,the seller pretty much has no clue who you are, however he can most likely tell whether the cash you issued him is legitimate.Specically, in this electronic money situation, a record relates to an electronic coin or note, and the underwriter speaks to a bank.The high-roller holds obscurity in any exchange that includes electronic coins in the event that they are Blindly signed.
Two proposals for blind signature schemes have been published: the first, presented in, is based on the RSA scheme and other based on Elgamaland Schnorr signature schemes[23]. Both the signatures can be used in digital cash but as they are the firs blind signatures they lack in security features. Blind DSA signatures are quite a bit more complicated, but can also be accomplished.

The blind signature has 4 phases they are:

1. **Blinding Phase:** In this phase the requester hides the message or blind the message for the signer such that the signer can not be able to see the actual content of the message and he did that by either multiplying the message with random number or by encrypting it with some key or it can be hashed also.

2. **Signing Phase:** In this phase the signer signs the message by its own signature but without revealing the actual content of the message. The signer signs blindly on the message sent to him by the requester.

3. **Unblinding Phase:** In this step received message is unblinded by the requester.

4. **Veryfying Phase:**In this phase the verifier receives the signature and it verifies the legitimacy of the signature by checking the verifying equations.

The following properties must be fullfilled by the blind signature scheme. They are blindness, correctness, unlinkability, untraceability and unforgeability.

1. **Correctness :** Those who has the signer's Public key will be able to check the corectness of the blind signature scheme.

2. **Blindness :** Signer will not be able to see the contents of the message while signing on it.

3. **Unforgeability :** The signature should not be forged by some attacker and if forged should be caught in the verification phase.

4. **Untraceability:** No one including the signer will be able to link between the signature and the message signature pair.

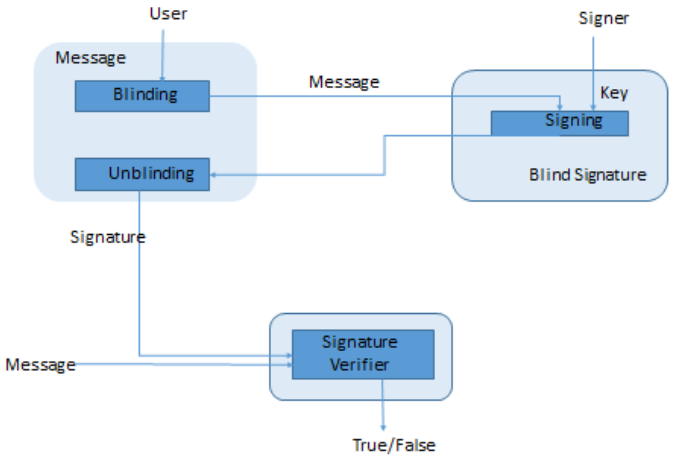

Figure 1.3: Blind Signature

1.4 Certificaleless Blind Signature

After the proposal of blind signature scheme by Chaum's, numerous blind signatures schemes were proposed for diverse applications, these were based on TR-PKC, but in TR-PKC fronts certificate management problem. In a TR-PKC, real trouble is the arrangement and administration cryptographic keys. Therefore IDB-PKC is introduced, that removed the certificate management problem but here the TTP used that creted the key escrow problem. To handle both the problem that are related with traditional PKC and ID based-PKC Certificateless-PKC is introduced. In Certificateless-PKC on the place of TTP there is PKC private key generator having own secret key called master key. PKC doesn't has the information about user key. He know only user identity and on the basis of that identity and system parameter with master key PPK is generated. user select a secret key s, using this PPK and s the user private key is generated. Certificateless Blind Signature has combined features of certificatelss cryptography and blind signature. [28, 26]The phase of certificateless blind signature are follows:-

1. **Set up phase:** PKG runs the key setup algorithm. For this algorithm security parameters are available. The algorithm takes security parameters as input and output a master key and a parameter list param. param is declared public and keep master private key private.

2. **Partial private key generation phase:**PKG taken public parameters using user ID and master private key calculates partial private key.

3. **User Secret key generation phase:**User Key generation: Secret key generation phase: User secret key use for generating full private key of user. User chooses his private key chosen from the set that are available in param.

4. **User private key generation phase:** User generates full private key us using partial private key and - secret key of user.

5. **User public key generation phase:** User public key is generating at this step using secret key of user and master public key. So here no direct relationship between public key of user and private key of user. User can generate any key first either public or private.

6. **Signing:** This phase complete in 3 steps: Blinding, Signing , Unblinding. In blinding user blind the message using his own random number and blinding factor. After blinding the message the user send the blinded message to signer.
   After receiving the blinded message from user signer sign the message using his own private key and random number, and then send this signed content to signer.
   User receive the signed content now user unblind the message using random number that user use in blinding phase.

7. **Verifying phase:** At this phase the verifier verify the signature validity whether the signature is valid or not.

1.5 Applications of Certificaleless Blind Signature

1.5.1 E-Voting System

Blind signature broadly utilized as a part of e-voting. Voter is allowed to vote in favor of anybody he/she make their vote, however the administrator doesn't have any learning

about their casting. In any case, administrator give the signature that everything happened their is valid. He didn't have power to think about who make the choice for whom. In government framework today's this kind of e-voting plan is utilized, this application may be made by any organization specialists, private affiliation, or any exceptional get-together of people. The security of customer who make the vote is keeping outwardly impeded. Each customer's tossed vote can be adequately affirmed with the help of executive's character. In advanced mark confidentiality issue is a to a degree comprehended by blind signature.

1.5.2 Digital cash:

e-money was presented by David Chaum as a anonymous money framework. It is fascinating to realize that e coins are blind signatures. e-money is a three gathering convention, in which a client or the requester demands for cash withdrawal to his/her bank or the underwriter for purchasing items from the trader. The underwriter checks the realness of the requester and after that sends marked tokens to the requester. The requester sends the tokens to the vendor and the trader give the token to the bank for confirmation of the tokens. So we can see one exchange can issue one legitimate token bundle or one valid signature. For various transaction the comparing signatures or the e-coins will be distinctive. Anyway, these days numerous requester gets to be pernicious and spends the e-coins for various times. This is known as the twofold spending issue. Despite the fact that blind signature gives untraceability or unlinkability yet at times it is important to uncover the personality of the requester. To do so,one requester ought not daze all the interior structure of the message. It ought to blind the external piece of the message so that by utilizing the general public parameters the signer can ready to follow the identity of the malicious requester. This is somewhat malicious is known as restrictive blind signature.

1.5.3 E-Business

The improvement of e-business accelerates on-line product dissemination, so protected and proficient behavior of electronic installment has turn into a most serious issue which needs to be unraveled critically. E-Business is a mix of "email" and "e-commerce".Both administration leads their functionality in the open system or over the free Internet, the offering and a remarkable piece of the early stress about the security issues related to them, can be solved with CLBS system.

1.6 Motivation and Objective

Digital Signature plays an significant role in almost every field of information technology for the purpose of authentication. In the technology advancement the concept of digital signature is extended to Blind Signature. Several schemes was proposed that follows the concept of Bilinear pairing, but either one of the proposed scheme has to compromise with very high computational complexity, which is nearly impossible to implement in today's cyber world. The only purpose of our research work is to propose a scheme which provides improved security features with the least computation overheads. So, we proposed an algorithm which is based on DLP that uses the Certificate less concept.

1.7 Organization of Thesis

The rest of Thesis is organized as follow:

Chapter 2 : Chapter 3 : In this Chapter we discuss the mathematics of cryptography. It describes the methods required to generate the prime numbers, the methods to test the primality of a number,the cryptographic hash functions to generate the message digest and the basic building blocks of discrete logarithm problem. At the very last of this chapter we discuss about the security models for certificateless blind signature scheme.

Chapter 4:This chapter describes the proposed certificateless blind signature scheme based on discrete logarithmic problem.

Chapter 5:In this chapter we perform the security analysis of our proposed scheme. We showed that the proposed scheme fulfills all the properties like blindness and unlinkability.

Chapter 6:Here we show that how the scheme is implemented in java language and what are the results after implementation.

Chapter 2

Literature Survey

We have gone through the paper Certificateless Public Key Cryptography the author Al-Riyami and Paterson published in 2003[3]. In his work, he discussed about the details of the Public Key cryptography and the problems related as well as in authentication such as certification and complexity. They discussed the basic information about ID based cryptography to overcome the certificate related problem in public key cryptography. They have also discussed about the problems that are inherited with the Identity based public key cryptography, and then they introduced the new type of cryptography called certificateless public key cryptography to overcome the problem that arised due to PKC and Identity based PKC. They have divided this scheme into seven steps, these steps are key setup, partial private key generation, user secret key generation user private key generation , user public key generation, encryption and decryption. This scheme's security is based on the Generalized Bilinear Diffie-Hellman Problem (GBDHP), considering that the GBDHP is hard.

We reviewed the paper On the Security of Certificateless Signature Scheme from Asiacrypt by Xinyi Huang, Futai Zhang etc in the year 2003[18]. In this paper they discussed about two types of attacks, they explained these attacks using game in which a challenger and an attacker participate. Challenger provide some options for attacker, such as attacker has the ability to change the public key or he can have the information about master secret key. In TYPE 1 attack, the challenger first share all the public parameter with attacker and the authority to change the public parameters. Attacker now can replace the public parameter and challenger has to accept it as a real public key, and in TYPE 2 attack the challenger share the information of the master private key with attacker. In this

paper they showed that the scheme proposed by Al-Riyami and Paterson(2003) [3] is not secure against TYPE 1 attack, but secure against TYPE 2 attack. In the same paper they proposed the new type of certificateless Signature scheme that are secure against both type of attack[18].

We have studied the paper Certificateless Signature Revisited presented by Xinyi Huang, Duncan S. Wong, and Wei Wu[17], in which they again visited the security models of certifcateless signature and introduced 2 new certificateless signature schemes. Their proposed scheme is based on bilinear pairing. They partition the security attacks on the basis of their attack capacity(normal, Strong and super type attacks). They proposed two new ceriticateless signature schemes, the first one is secure against normal and strong type attacks but not secured against super type attacks and the second signature scheme is secure against all three types of attacks.

We have studied the paper Certificateless Signature and Blind Signature proposed by Zhang Lei Zhang Futai[28]. They first present the certificateless signature scheme showing some advantage on previous certificateless scheme, after that they proposed the certificateless blind signature scheme. They are the first one, who introduced the blind signature into certificateless public key cryptography. Both the scheme of this paper is based on bilinear pairing, and the both schemes securities are based on Computational Diffie-Hellman(CDH) problem. They discussed about the security attacks such as unforgability and blindness and found secure.

Chapter 3

Preliminaries

Here, we gave the details about the mathematical term, theorem and algorithms that are used in our proposed scheme. We first give a short introduction about the integer factorization and prime factorization, then we discuss the basics related to the primarily test also the diffenrent algorithms that are used to check the primarily test. After that we gave detail about discrete logarithmic problem and hash functions. In the end of this section, we gave details of different security models related to certificateless signature and blind signature[6].

3.1 Mathematical Background

3.1.1 Integer factorization and Prime Factorization

[14]A composite number is a positive whole number that has no less than one positive divisor other than one or the number itself. As such, a composite number is any number more noteworthy than one that is not a prime number. Prime number is the number that have no any other factor other than one and that number itself. Decomposition of a composite number into smaller integer is called integer factorization. Prime factorization of a number is the the factorization of any composite number into the products of prime numbers. Prime factors of the any number can be calculated using following steps:

1. First we start from the first prime number 2, divide the number with that prime number, goes to step 2.

2. Continue till the number is divisible by that prime

3. If the last factor is prime then return else divide the factor with next prime number and continue step 2.

3.1.2 Primality Tests

Prime number is very useful in cryptography, because every number other than 0 and 1 can be expressed as the product of prime number. In many algorithm the prime factorization technique is used because the prime factorization of a large number is taking much time. The primality test is the type of test used to check the given number is prime or not. [14]. Many algorithms are available for this test. A naive algorithm or Square root test:

1. Take a positive integer number P that are grater than 2, and divide this P by the odd numbers that are greater than or equal to 3 to the square root of P.

2. Giving a condition that if P is divisible by any of the number from 3 to square root of P then the number P is composite. The most pessimistic scenario is that we need to experience all odd number testing cases up to square root P. The compexity of this algorithm is O(square root of N)

Fermat Test: There are two version of this algorithms are available [14]. In first version for cheking a number is prime or not. Let us consider a number n, to check whether n is prime check the equation $a^{n-1} = 1 \mod n$ Here a is any integer. And the second version of this theorem is to check n is prime then $a^n = a \mod n$ Here a is any integer.

Miller-Rabin Test: This test having combined features of Fermat test and square root test[14]. It is described using following step:-

Step 1: Take a number n. Finding the value of a and b such that $n - 1 = a * 2^b$.

step 2: Find the value of R such that $g^a \mod n$

step 3: Now if the value of R is equal to 1 or -1 then return thta the number n is prime. Else the process enter into next step.

step 4: Now checking from 1 to $b-1$, calculating the value of R as $R = R^2 \mod n$. Checking the value of R every time if value of R is equal to 1 then result that the number n is composite number and if value of R is equal to -1 then result that the number n is prime number.

3.2 Discrete Logarithmic Problem

Let us consider a given a group G having p number of element, g is the generator of this group. Let us choose a number n from the group G, there exists a number x such that it satisfy the following condition[15].

$$g^x \mod p = n \tag{3.1}$$

. It is not always true that dlp is always hard. Its depends on the hardness of groups. DLP is believed to be much harder than Integer factorization problem. This is why several Encryption algorithms use DLP as their base like Elgammal and DSS. DLP holds the similar relation to these systems as factorization does to the RSA: the security of these frameworks depends on the presumption that discrete logarithms are hard to figure. DLP when used for cryptographic purposes we usually chose Zn^* as a group.

3.3 Cryptographic Hash Function:

A cryptographic hash function is a deterministic function which maps a string of arbitrary length to a string of fixed length called hashed value. This hashed message is called message digest. Rov Rivest developed many hash algorithms[14] they are MD2, MD4 and MD5. MD-2 takes 18 rounds to generated 128 bits message digest, but it is vulnerable to a preimage attacks, so it is not considered to be secured. mD-4 takes 48 rounds to generates 128 bit message digest, but it found vulnerable against the collision attack published in 2007. mD-5 takes 64 rounds to generates 128 bit message digest, but it found vulnerable against the collision attack published in 2013[22]. It is found that message digest size 128 bit is small to resist the collision. So National Institute of Standard and Technology developed a new type of hash algorithms secure hash algorithm(SHA). In Which message digest size is upto 512 bits. In our proposed SHA-2 algorithms is used. SHA-2 algorithms having message digest size 256 bits.

Chapter 4

Certificateless Blind Signature Based on DLP

4.1 Description of the proposed scheme:

The proposed scheme has Seven phases for creating the signature and verifying it. These are: setup ,partial private key generation, Secret key generation, User private key generation, User public key generation, signing phase, verifying phase. Here three parties are involved in this signature generation scheme- PKG, user and signer.

PKG Key generation:

Set up phase: PKG chooses a very large prime number p. PKG calculate q a large factor of p. After calculating q PKG find g the generator of group z_q^*. PKG chooses a random number m_s ($m_s \in z_q^*$) and declares m_s as a private key of PKG called master private key. PKG also calculate master public key m_p It is calculating using this equation $m_p = g_s^m \mod q$

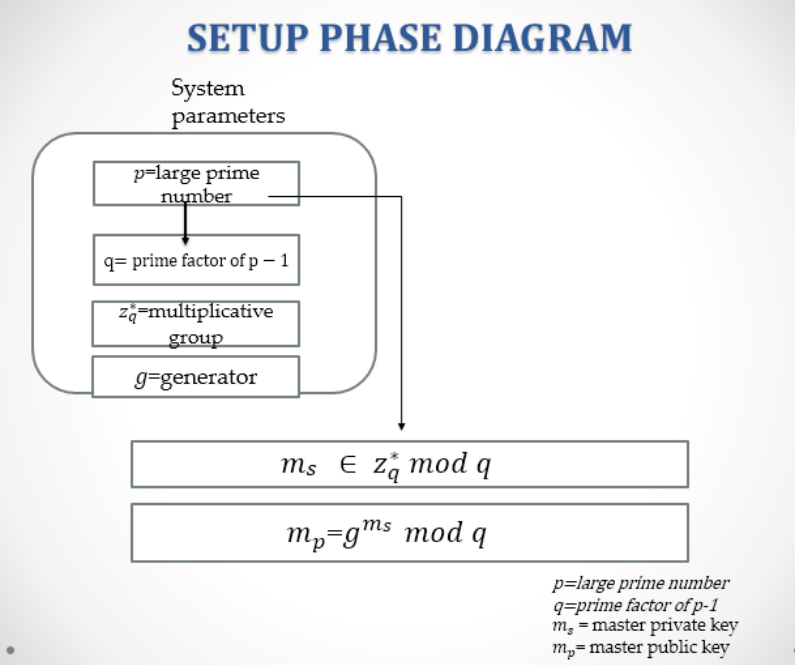

Figure 4.1: Set up phase

Partial private key generation phase: PKG taken public parameters using user ID and master private key calculates partial private key.$ppk = (id + m_s) \mod q$

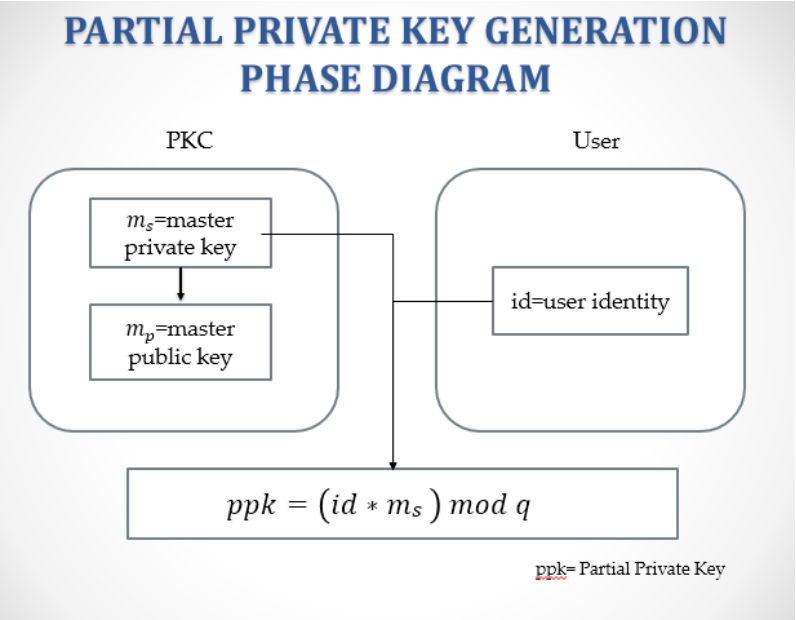

Figure 4.2: Partial private key generation phase

User Key generation: Secret key generation phase: User secret key x_A use for generating full private key of user. User chooses his private key chosen from the set. $x_A in z_q^*$

User private key generation phase User Generates full private key u_s using PPK

and user secret key. It is calculating using equation $s = (ppk * x_A)$

User public key generation phase User Generates his public key u_p using master public key and user secret key. It is calculating using equation $u_p = m_p^{x_A}$

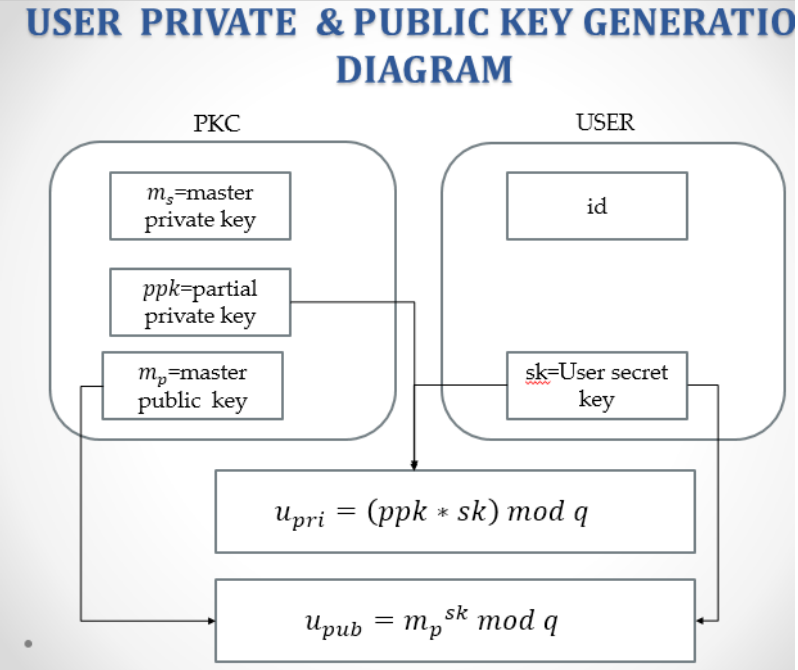

Figure 4.3: User public private key generation

Signing phase Signer chooses d as private key from the set of z_q^*.($d \in z_q^*$). Signer computes his public key e for the use of verification phase, using the equation $e = g^d \mod q$.

User send request to signer for sign the message. A random number k is chosen by signer from set z_q^* and v ($e = g^k \mod q$)is calculated and sent to user. User selects 2 random number a and b from set z_q^* and calculates blinding factor f, as $f = (a * b * v)^{-1}$ User blinded the message using blinding factor f. The blinded message is indicated using m'. user Chooses a random number l from the set z_q^* and compute $u = g^u$.

$$m' = f * H(m, u^{s*l^{-1}}) \mod q \tag{4.1}$$

Where, Function $H(m, u^{s*l^{-1}})$ calculated applying hashing algorithm (SHA-256) on both the parameters $H(m, u^{s*l^{-1}}) = SHA-2(m) * SHA-2(u^{s*l^{-1}})$ Now, User sent m' to signer.

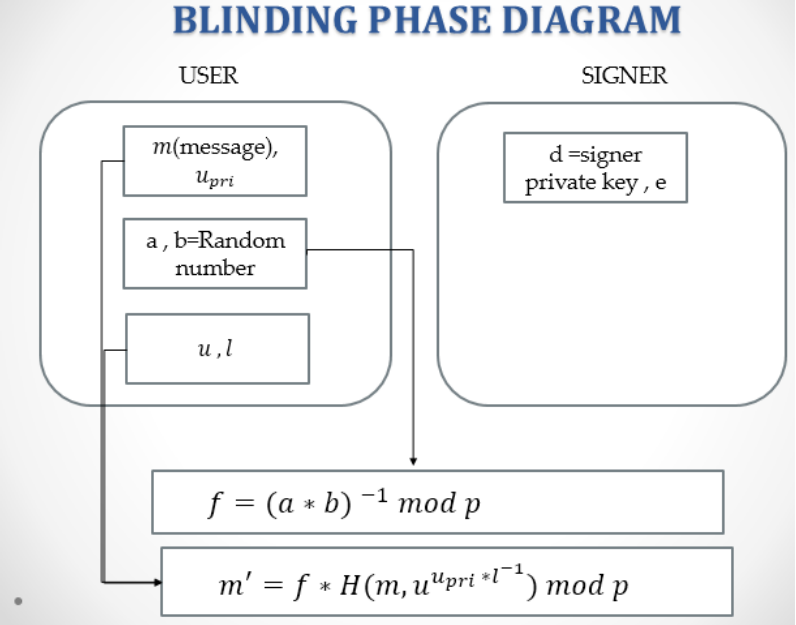

Figure 4.4: Blinding

Signer sign the message using his private key.

$$t' = d * m' \mod q \tag{4.2}$$

Signer sent the signed message to user. User unblinded the message using his random number. $t = a * t' * b \mod q$

Finally user declared (t, e) as signature of signer. [ht]

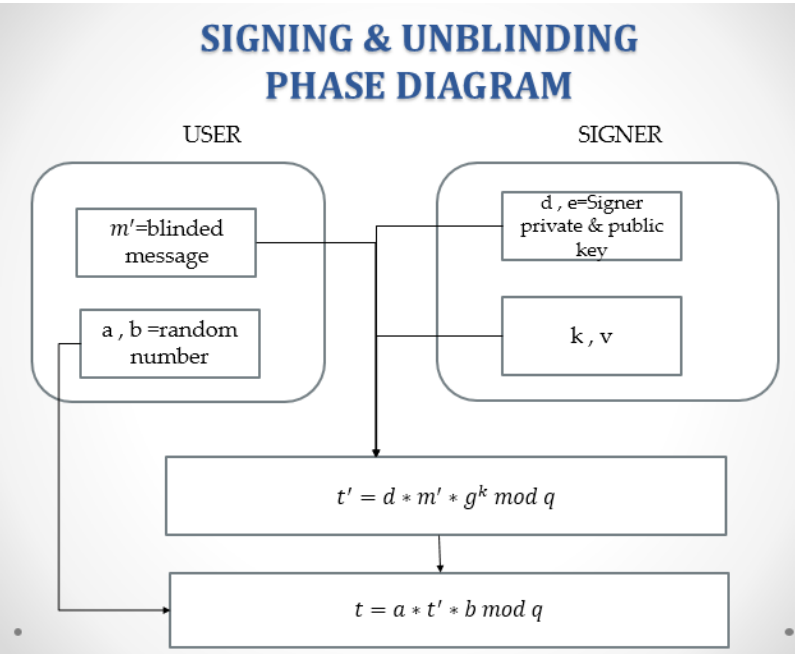

Figure 4.5: Signing and Unblinding

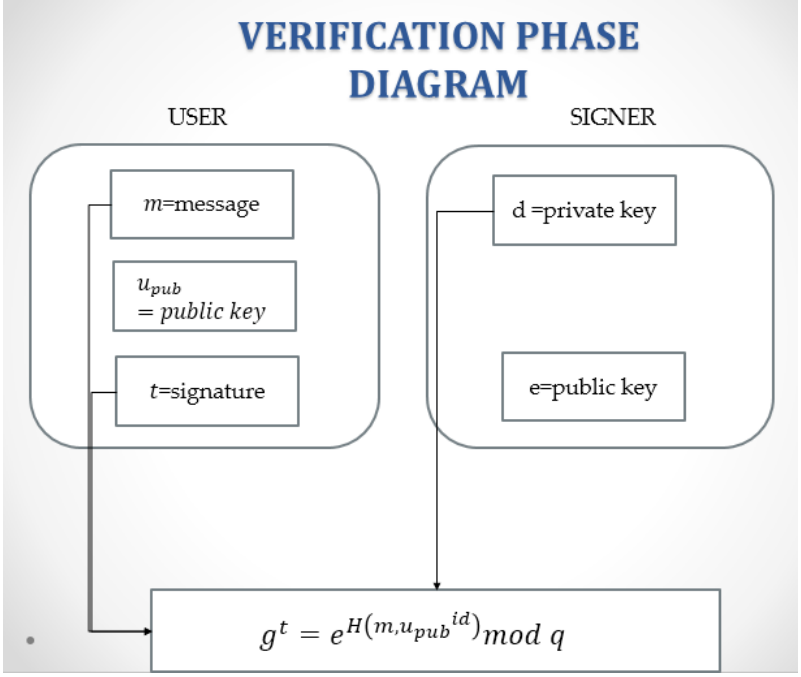

Figure 4.6: Verification phase

Verification phase: Anyone with the public parameters, user public key and signature pair can verify the equation. If the following equation is true the signature verified else note verified.

$$g^t = e^{H(m,u_p^{id})} \mod q \tag{4.3}$$

Where, Function $H(m, u^{s*l^{-1}})$ calculated applying hashing algorithm (SHA-256) on both the parameters. $H(m, u_p^{id}) = SHA - 2(m) * H(u_p^{id})$

Chapter 5

Security Analysis of Proposed Algorithm

Correctness:

$$g^t = e^{H(m,u_p^{id})} \mod q \tag{5.1}$$

proof: Taking from left side

$$\begin{aligned}
g^t &= g^{a*t1*b} \mod q \\
&= g^{a*d*m1*b} \mod q \\
&= g^{d*a*m1*b} \mod q \\
&= e^{a*f*h1*b} \mod q \\
&= e^{h}1 \mod q \\
&= e^{H(m,u^{upri*l^{-1}})} \mod q \\
&= e^{H(m,g^{l^{s*l^{-1}}})} \mod q \\
&= e^{H(m,g^{s})} \mod q \\
&= e^{H(m,g^{ppk*x_A})} \mod q \\
&= e^{H(m,g^{id*m_s*x_A})} \mod q \\
&= e^{H(m,g^{m_s*x_A*id})} \mod q \\
&= e^{H(m,u_p^{id})} \mod q
\end{aligned} \tag{5.2}$$

Theorem 1: The proposed CLBS scheme follows blindness properties.

Proof: The message blindness needs to be utilized along with some parameter v sent by signer. After connected, the user who uses the random number a_1 and b_1 to generate a blinding factor and combine it with an input message that are going through the hash function and the whole operation is represented by the given equation.

$$m1' = f * H(m1, u^{u_s * l^{-1}}) \mod q \tag{5.3}$$

Where, $f1 = (a1 * b1 * v)^{-1}$. The hash function we are utilizing as a part of our proposed scheme is SHA-2, which is the safe message digest. So that, the attacker will not be able to uncover anything about a genuinity of message, that is the reason we will be able to prove that our scheme has fulfilled blindness property.

Theorem 2: The proposed CLBS scheme is follow unlinkabiliy properties.

Proof: Let us assume, two different messages M and N. The both message signed by signer S individually. The proposed signature schemes are relied on upon DLP where we have (M,t1,e1) and (N,t2,e2) message signature pair.

$$\begin{aligned} g^{t1} &= g^{a1*t1'*b1} \mod q \\ &= g^{a1*d1*m1*v1*b1} \mod q \\ &= g^{a1*d1*v1*b1*f1*H(M,u^{s1*l1^{-1}})} \mod q \end{aligned} \tag{5.4}$$

$$\begin{aligned} g^{t2} &= g^{a2*t2'*b2} \mod q \\ &= g^{a2*d2*m2*v2*b2} \mod q \\ &= g^{a2*d2*v2*b2*f2*H(N,u^{s2*l2^{-1}})} \mod q \end{aligned} \tag{5.5}$$

For the message M in blinding process random number a1 and b1 is used for blinding the message. For the message N in blinding process random number a2 and b2 is used for blinding the message, also hashed value of two different messages M and N is different. For every new request to signer a different random value is generated so adversary cannot

link the message signature pair.

Chapter 6

Implementation and result

In our proposed scheme we have used Java platform for the implementation. There is no need to use any database because we are not using any key storing in our proposed algorithm. We have used NetBeans as integrated development environment for the purpose of implementation. We are using BigInteger value for taking a large number operation power, modpower, and random number generator. java security package is used for cryptographic hash function and prime number generator. Signer signed the blinded message and user unblinded the message. Now if the verification equation is true then the signature is verified. We are using java util package for choosing a large prime number.In our proposed scheme there are three parties private key generator, user and signer. In have taking message input from file its size is 5KB. Blinding of message in our scheme is done using cryptographic hash function. we are using SHA-2 our implementation. Our proposed scheme consists of following seven phases in implementation:

1. Set up phase
2. Partial private key generation phase
3. Secret key generation phase
4. User private key generation phase
5. User public key generation phase
6. Signing phase
7. Verification phase

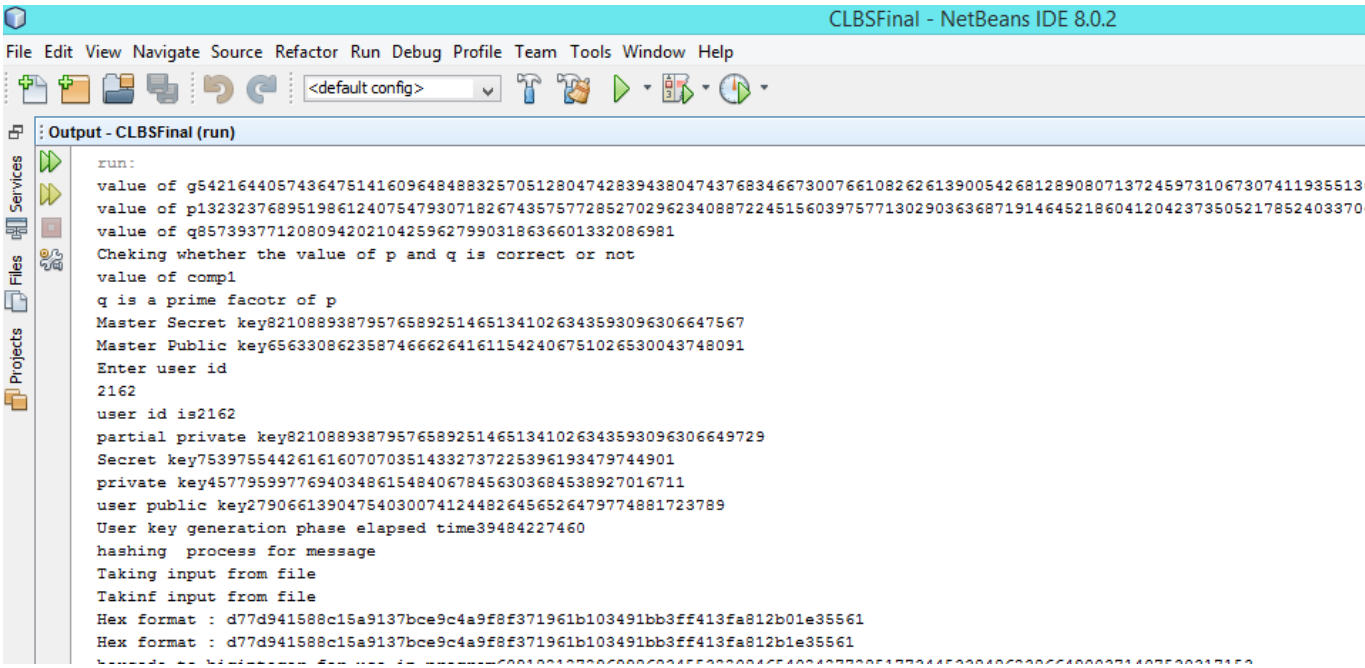

Figure 6.1

The values for setup phases are given is bellow:

Generator g= 5421644057436475141609648488325705128047428394380474376834667300766108262613

Prime number p = 1323237689519861240754793071826743575772852702962340887224515603975771302

Prime Factor q= 85739377120809420210425962799031863660133208698l

Master Secret key= 821088938795765892514651341026343593096306647567

Master Public key= 656330862358746662641611542406751026530043748091

Enter user id, user id is=2162

partial private key= 8210889387957658925146513410263435930963066497 29

Secret key= 753975544261616070703514332737225396193479744901

private key= 457795997769403486154840678456303684538927016711

user public key= 279066139047540300741244826456526479774881723789

hashing process for message

Taking input from file

Hex format : 5a5032123d2b68966d42412ce620c341f38247a9d49e83705a70c28a8989a576

Hex format : d77d941588c15a9137bce9c4a9f8f371961b103491bb3ff413fa812b01e35561

hexcode to biginteger for use in program=

609182127296998683455322084654024277285177344533848623866490037140753031715 3

elapsed time in hashcode generation of the message= 4.7ms Signing phase

signer public key= 54732997858202440286088558550866805973913743946

Unblinded content=725228640443498187188340260843964851477287066100

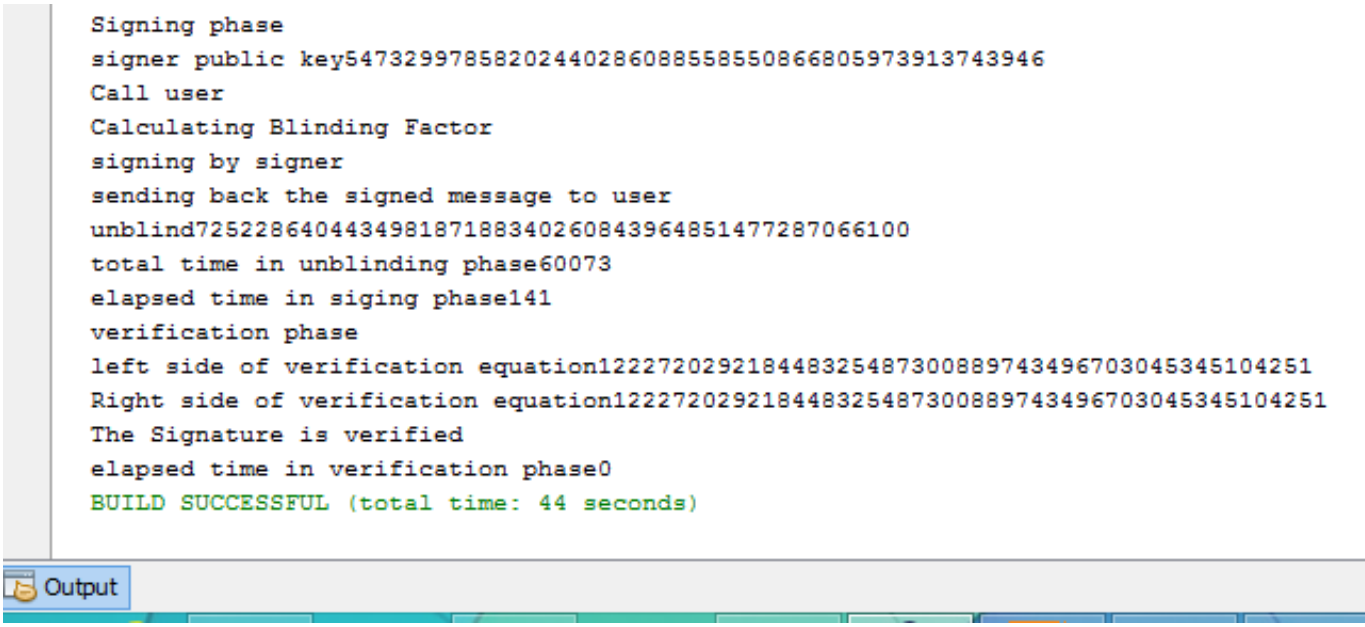

Figure 6.2

Table 6.1: Analysis of Execution time in (ms)

Key Generation	Hashing	Signing	Verification
599ms	4.7ms	79ms	0.18 ms

signature=725228640443498187188340260843964851477287066100

Signature length= 19 byte

verification phase

left side of verification

equation= 1222720292184483254873008897434967030453451042 51

Right side of verification equation= 1222720292184483254873008897434967030453451042 51

The Signature is verified.

Chapter 7

Conclusions and Future Work

In this paper, we have presented an efficient certificateless blind signature scheme. Their security is based on the hardness of Discrete Logarithmic problem. Having all security features with low computational overhead as well as feasible. In future our scheme can be used to get a fair system policy in e-commerce. With the help of our scheme a more secure E-cashing, E-voting, E-business can be build up in a great way. This proposed algorithm can also be used for crime avoidance.

Bibliography

[1] Carlisle Adams and Steve Lloyd. *Understanding public-key infrastructure: concepts, standards, and deployment considerations*. Sams Publishing, 1999.

[2] Sattam Al-Riyami. *Cryptographic schemes based on elliptic curve pairings*. PhD thesis, University of London, 2004.

[3] Sattam S Al-Riyami and Kenneth G Paterson. Certificateless public key cryptography. In *Advances in Cryptology-ASIACRYPT 2003*, pages 452–473. Springer, 2003.

[4] Xu an Wang, Xinyi Huang, and Xiaoyuan Yang. Further observations on certificateless public key encryption. In *Information Security and Cryptology*, pages 217–239. Springer, 2009.

[5] Rouzbeh Behnia, Swee-Huay Heng, and Che-Sheng Gan. An efficient certificateless undeniable signature scheme. *International Journal of Computer Mathematics*, (ahead-of-print):1–16, 2014.

[6] Jan L Camenisch, Jean-Marc Piveteau, and Markus A Stadler. Blind signatures based on the discrete logarithm problem. In *Advances in Cryptology—EUROCRYPT'94*, pages 428–432. Springer, 1995.

[7] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[8] David Chaum. Blind signature system. In *Advances in cryptology*, pages 153–153. Springer, 1984.

[9] Hu Chen, Rushun Song, Futai Zhang, and Fagen Song. An efficient certificateless short designated verifier signature scheme. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*, pages 1–6. IEEE, 2008.

[10] Yu-Chi Chen, Chao-Liang Liu, Gwoboa Horng, and Kuo-Chang Chen. A provably secure certificateless proxy signature scheme. *International Journal of Innovative Computing, Information and Control*, 7(9):5557–5569, 2011.

[11] Kyu Young Choi, Jong Hwan Park, Jung Yeon Hwang, and Dong Hoon Lee. Efficient certificateless signature schemes. In *Applied Cryptography and Network Security*, pages 443–458. Springer, 2007.

[12] Sherman SM Chow, Colin Boyd, and Juan Manuel González Nieto. Security-mediated certificateless cryptography. In *Public Key Cryptography-PKC 2006*, pages 508–524. Springer, 2006.

[13] Sherman SM Chow and W-S Yap. Partial decryption attacks in security-mediated certificateless encryption. *IET Information Security*, 3(4):148–151, 2009.

[14] Behrouz A Forouzan. *Cryptography & Network Security*. McGraw-Hill, Inc., 2007.

[15] Dan Gordon. Discrete logarithm problem. In *Encyclopedia of Cryptography and Security*, pages 352–353. Springer, 2011.

[16] Debiao He, Baojun Huang, and Jianhua Chen. New certificateless short signature scheme. *IET Information Security*, 7(2):113–117, 2013.

[17] Xinyi Huang, Yi Mu, Willy Susilo, Duncan S Wong, and Wei Wu. Certificateless signature revisited. In *Information Security and Privacy*, pages 308–322. Springer, 2007.

[18] Xinyi Huang, Willy Susilo, Yi Mu, and Futai Zhang. On the security of certificateless signature schemes from asiacrypt 2003. In *Cryptology and Network Security*, pages 13–25. Springer, 2005.

[19] Xiang-xue Li, Ke-fei Chen, and L Sun. Certificateless signature and proxy signature schemes from bilinear pairings. *Lithuanian Mathematical Journal*, 45(1):76–83, 2005.

[20] Georg Lippold. Encryption schemes and key exchange protocols in the certificateless setting. 2010.

[21] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in cryptology*, pages 47–53. Springer, 1985.

[22] Marc Stevens. Fast collision attack on md5. *IACR Cryptology ePrint Archive*, 2006:104, 2006.

[23] Shifeng Sun and Qiaoyan Wen. Novel efficient certificateless blind signature schemes. In *Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on*, pages 1–5. IEEE, 2009.

[24] Raylin Tso, Xun Yi, and Xinyi Huang. Efficient and short certificateless signatures secure against realistic adversaries. *The Journal of Supercomputing*, 55(2):173–191, 2011.

[25] Changji Wang and Rongbo Lu. A certificateless restrictive partially blind signature scheme. In *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on*, pages 279–282. IEEE, 2008.

[26] RONG Wei-jian. Certificateless partially blind signature scheme [j]. *Journal of Zhangzhou Normal University (Natural Science)*, 4:011, 2008.

[27] Jianhong Zhang and Shengnan Gao. Efficient provable certificateless blind signature scheme. In *Networking, Sensing and Control (ICNSC), 2010 International Conference on*, pages 292–297. IEEE, 2010.

[28] Lei Zhang and Futai Zhang. Certificateless signature and blind signature. *Journal of Electronics (China)*, 25(5):629–635, 2008.