Design of Blind Signature Protocol Based upon DLP

by

Chanchal Chandra (109CS0107)

Thesis submitted on

13th May, 2013

to the

Department of Computer Science and Engineering

of

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA

in partial fulfilment of the requirement for the

Degree of Bachelor of Technology

under the guidance of

Prof. Sujata Mohanty

Department of Computer Science and Engineering

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA

Declaration of Authorship

I, Chanchal Chandra, declare that this thesis titled, 'Design of Blind Signature Protocol Based upon DLP' and the work presented in it are my own. I confirm that:

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

Signed: _____

Date: _____

Abstract

Blind signature scheme is based on public key cryptosystem. Public-key cryptosystem is widely used these days for various security purposes. The use of public key cryptosystems received huge amount of attention. They are beneficial in encipherment, authentication, non-repudiation as well as digital signature, which plays an essential role in electronic banking and financial transactions. This project has proposed a new blind signature scheme based on ElGamal signature scheme. Blind signature schemes, first introduced by David Chaum, allows a person to get a message signed by another party without revealing any information about the message to the other party. It is an extension of digital signature which can be implements using a number of common public key signing schemes, for instance RSA and ElGamal signature scheme. Blind signature is typically employed in privacy related protocols, where the signer and the requester are different person. In our project work we have taken an existing scheme based on ElGamal signature scheme as the reference scheme for comparison and proposed a new scheme. Aims of the proposed scheme is high security features and reduce the communication overhead, computation overhead, signature length. The proposed scheme aims to have lesser computation overhead and high security features than existing scheme [1, 2, 3, 5, 15, 16].

Keywords : Blind signature, digital signature, public key-cryptosystem, communication overhead, computation overhead.

Acknowledgements

I would like to express my earnest gratitude to my project guide, Prof. Sujata Mohanty for believing in my ability. Her profound insights has enriched my research work. The flexibility of work she has offered me has deeply encouraged me producing the research. I am indebted to all the professors, batch mates and friends at National Institute of Technology Rourkela for their cooperation. My full dedication to the work would have not been possible without their blessings and moral support.

Chanchal Chandra

Certificate

This is to certify that the work in the thesis entitled **Design of Blind Signature Protocol Based upon DLP** by Chanchal Chandra, bearing Roll No. 109CS0107, is a record of an original research work carried out by her under my supervision and guidance in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Date: **Prof. Sujata Mohanty**

Rourkela (National Institute of Technology, Rourkela)

Contents

Declaration of Authorship i

Abstract ii

Acknowledgements iii

List of Figures vi

List of Tables vii

Abbreviations viii

1 Introduction 1
- 1.1 Digital Signature . . . 1
  - 1.1.1 Authentication . . . 2
  - 1.1.2 Non-repudiation . . . 2
  - 1.1.3 Attacks on Digital Signature . . . 2
  - 1.1.4 Forgery . . . 3
- 1.2 Blind Signature . . . 3
- 1.3 Public-key Cryptosystem . . . 4
- 1.4 Security Goals . . . 4
  - 1.4.1 Confidentiality . . . 5
  - 1.4.2 Integrity . . . 5
  - 1.4.3 Availability . . . 5
- 1.5 Security Mechanism . . . 6
- 1.6 Problem Statement . . . 6

2 Literature Review 7
- 2.1 Mathematical Foundation . . . 7
- 2.2 RSA Scheme . . . 8
- 2.3 ElGamal Scheme . . . 9
- 2.4 Review of Mohammed, Emarah and Shennawy's **scheme** . . . 10

3 Scope of the Work 12
- 3.1 E-voting . . . 12

3.2 E-Cash . . . 12
3.3 E-Commerce . . . 14

4 Proposed scheme **16**
4.1 Setup Phase . . . 16
4.2 Blinding Phase . . . 16
4.3 Signing Phase . . . 17
4.4 Un-blinding Phase . . . 17
4.5 Verifying Phase . . . 17
4.6 Correctness . . . 18

5 Result **19**
5.1 Implementation result . . . 19
5.1.1 Comparison by Computational overhead . . . 19
5.1.2 Comparison by Signature Length . . . 20
5.2 Security Analysis . . . 21

6 Conclusion **22**

References **23**

List of Figures

1.1 Creating a digital signature 2
1.2 Blind Signature Protocol 4
1.3 Public-key Cryptosystem 5

3.1 E-Voting System 13

5.1 Existing Scheme 20
5.2 Proposed Scheme 21

List of Tables

5.1 Comparison of Computational Overhead 20
5.2 Comparison of Signature Length 20

Abbreviations

DLP	**D**iscrete **L**ogarithm **P**roblem
IFP	**I**nteger **F**actorization **P**roblem
EVS	**E**lectronic **V**oting **S**ystem
BS	**B**lind **S**ignature

Chapter 1

Introduction

These days public key cryptosystem are widely used for secure network communication. It has received well known attention. Along with authenticity it provides confidentiality, integrity, non-repudiation. Public key cryptosystem is very reliable for communication industry, financial transaction, electronic mail , e-commerce and internet. They are beneficial in encryption as well as digital signing which plays an essential role in electronic money transactions and identity verification [1, 15 ,16, 17]. In this project we have proposed a Blind Signature scheme based on ElGamal scheme and implemented the proposed scheme. We have compared the outcomes of proposed scheme with an existing scheme describe in Chapter 2.4.

1.1 Digital Signature

A digital signature verifies the authenticity of an electronic document or digital message. Digital signatures are commonly used to identify electronic entities for online transactions. A valid digital signature gives a user reason to believe that the message was created by a known legitimate sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption. Digital signatures are commonly used for software distribution, Authenticate online entities, Verify the origin of digital data. Ensure the integrity of digital data against tampering, financial transactions, and in other cases where it is important to detect forgery attack. A digital signature procedure is shown in Figure 1.1 [5, 13, 14].

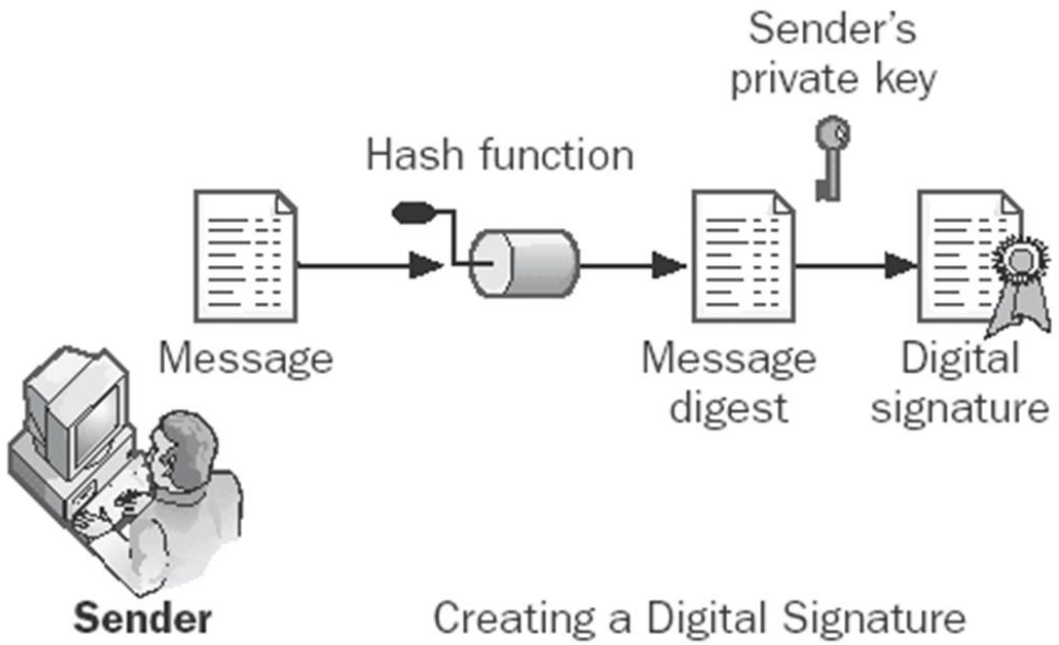

FIGURE 1.1: Creating a digital signature

1.1.1 Authentication

A message source is authenticate by digital signature. A valid signature shows that the message was sent by that user, where user is the requester. Authenticity in digital signature means that the message or the user is valid [5, 13, 14].

1.1.2 Non-repudiation

Non-repudiation is an important feature of digital signature. By this property, an entity that has signed some information cannot at a later time deny having signed it [5, 13, 14].

1.1.3 Attacks on Digital Signature

This section describes attack on digital signature. Key-Only attack, Known message attack and Chosen-Message attack are some attacks on DS. If the attack is successful, the result is a forgery. We can have two types of forgery [20, 21, 22].

1.1.4 Forgery

In a cryptographic digital signature system, digital signature forgery is the ability to create a pair consisting of a message and a signature that is valid for message, and message has not been signed by the legitimate signer [9]. Existential and Selective are the two types of forgery.

- **Existential Forgery**
  In an existential forgery the attacker is able to create a valid signature-message pair, but the attacker cannot use this pair really. This type of forgery is probable, but the attacker cannot benefit from it [20, 21, 22].

- **Selective Forgery**
  In the selective forgery, the attacker is able to forge signers signature on a message. The attacker gets benefit from this forge unlike existential forgery. The probability of such forge is low [20, 21, 22].

1.2 Blind Signature

Blind signature is an extension of digital signature in which a message is signed by a signer without knowing the content of the message. Blind signature was first introduced by David Chaum in 1983. It allows a person to get a message signed by another party without revealing any information about the message to the other party [2, 3, 4].
Sometimes we have a document that need to get signed without revealing the contents of the document to the signer. For example, a scientist, say Bob, might have discovered a very important theory that need to be signed by a public, say Alice, without allowing Alice to know the content of the document. Blind Signature protocol for this purpose works as follows [20]:

- Bob creates a message and blinds it. Bob sends the blinded message to Alice
- Alice signs the blinded message and send the signature on the blinded message
- Bob unblinds the signature to obtain a signature on the original message.

Basic security features of a standard blind signature are un-linkability, blindness and non-repudiation [20, 21].Lets see a block diagram of blind signature protocol see Figure 1.2. It consist of two participants a requester and a signer where, requester wants signer to sign a message m.Requester blind the message m with some blinding factor b. Signer sign the blind message, where d is signers private key. Requester un-blind the message and get the sign(m , d) which is signers signature on m [2, 3].

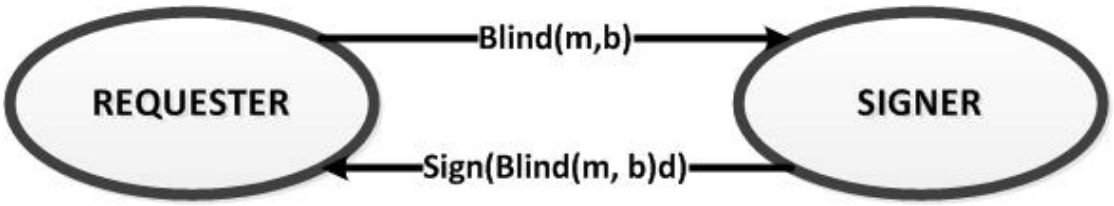

FIGURE 1.2: Blind Signature Protocol

1.3 Public-key Cryptosystem

Public key cryptosystem requires two separate key, one of which is secret and another is public. It is also called as asymmetric key cryptosystem. One key is used for encryption and another is used for decryption. Neither key can perform both operations by itself. The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages [15, 16, 17]. In the public key cryptosystem, the receivers public key is used for encrypting the senders message. This public key is known to everyone. The encrypted message is sent to the receiver, who will decrypt (unlock) the message by his private key. Only the receiver can unlock the encrypted message because no one else has the private key. Algorithm for encryption and decryption is same see Figure 1.3 [15, 16, 17].

1.4 Security Goals

Confidentiality, Integrity and Availability are the prime security goals of the Blind Signature scheme. These security goals have different specification in respect of security. Describe in the below section [20].

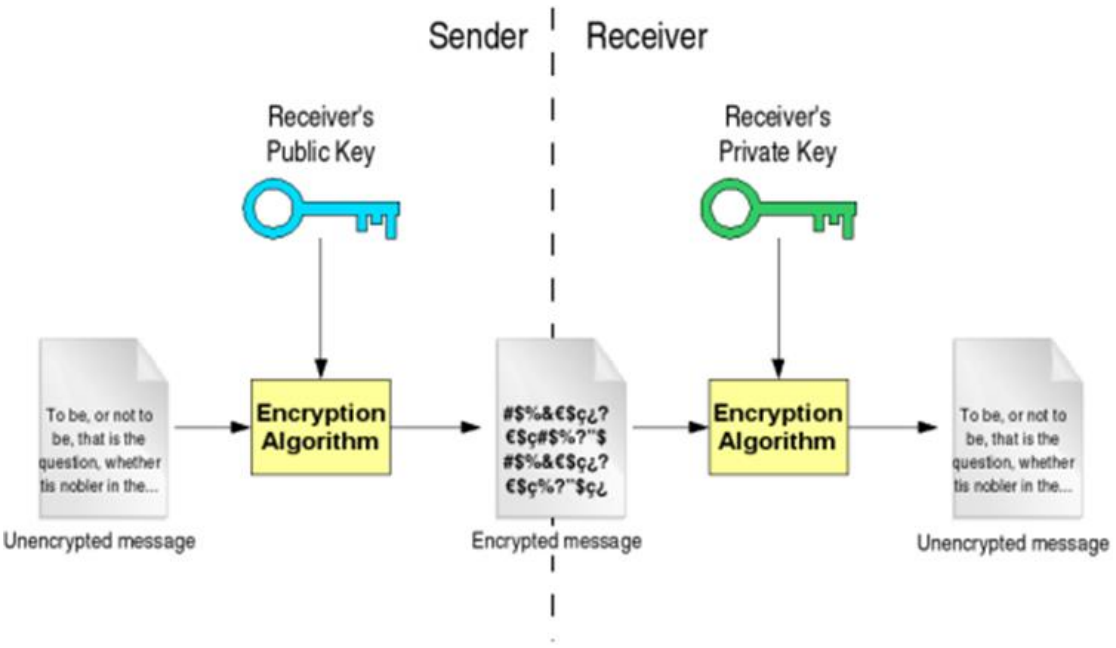

FIGURE 1.3: Public-key Cryptosystem

1.4.1 Confidentiality

Confidentiality means we need to protect our information. It is the most common property of data security. It is not only applies to the storage information, it also apply to the transmission of data. When we send a information or when we receive a information, we need to conceal it during transmission.

1.4.2 Integrity

Integrity means that the changes need to be done by legitimate authorized entity and through authorized mechanism. Integrity ensures that message should not be change during processing. Information needs to be changed constantly. Integrity violation is not necessarily the result of a malicious act. Document and Fingerprint, Message and Message Digest, Checking Integrity, Cryptographic Hash Function are some ways to maintain integrity [5, 13, 14, 20].

1.4.3 Availability

The last prime component of data security is Availability. The information need to be available for legitimate authority. The unavailability of information is result in same harmful as lack of confidentiality or integrity [20].

1.5 Security Mechanism

Encipherment, Data integrity, Access control, Digital signature, Authentication exchange are some mechanism to provide security [20].

1.6 Problem Statement

In literature all blind scheme have high communicational and computational overhead. There is a need to develop Blind signature scheme with high security feature and low communicational, computational overhead. Also the signature length must be low. Our objective is to design a BS scheme such that it should have high security features, lesser computational overhead, lessr communicational overhead and shorter signature length.

Chapter 2

Literature Review

2.1 Mathematical Foundation

In 1976, Diffie and Hellman first introduced the concept of public key cryptosystem. Their key distribution protocol is based on supposing that A and B want to share a secret K_{AB} where A has a secret x_A and B has a secret x_B . Let p be a large prime and a be a primitive element mod p, which are both known to A and B [5, 1].

A computes,

$$\mathrm{y}_A = a^{x_A} \pmod{p}$$

And sends y_A

$$\mathrm{y}_B = a^{x_B} \pmod{p}$$

And sends y_B

Then the secret K_{AB} is computed as,

$$\begin{aligned} \mathrm{K}_{AB} &= a^{x_A x_B} \pmod{p} \\ \mathrm{K}_{AB} &= y_B^{x_A} \pmod{p} \\ \mathrm{K}_{AB} &= y_A^{x_B} \pmod{p} \end{aligned}$$

Therefore both A and B are able to compute K_{AB} . But, for an intruder, computing appears to be difficult. The intruder will need to compute discrete logarithms modulo a prime, which is known to be a difficult problem. In all cryptographic systems based on discrete logarithms, p must be chosen so that p -1 has at least one large prime factor. If p -1 has only small prime factors, then computing discrete logarithms is easy [1, 5].

2.2 RSA Scheme

RSA cryptosystem is widely used to provide privacy. In RSA digital signature scheme, first the private and public keys of the sender is used, second the sender used her own private key to sign the document. The receiver uses the senders public key to verify it. The signing and verifying sites use the same function, but the parameters are different. The verifiers compares the message and the output of the function for congruence. If the result is true, the message is accepted [20]. Assume a standard RSA setting in which the public key is denoted as a pair (e, n) and the private key is denoted as a number d. Here the modulus n is a product of two large (secret) primes p, q and the private key d is the multiplicative inverse of e modulo (p-1)(q-1). For the security of the RSA system it is assumed that both p and q are sufficiently large (e.g., 200 digit numbers) such that it is infeasible to either find the factorization of n or to find the private key d, given only the public key (e, n)[1]. Let a message m be given for which an RSA signature is to be produced. m corresponds to an integer between 0 and n. The signature is produced in one step by the signer.

Signing Phase

The signer use the private key d to compute the signature :-

$$\mathrm{S} = \mathrm{m}^{d} \pmod{n}$$

Anyone can verify that s is signature on the message m with respect to public key (e,n) by performing the following step:

Verification Phase

Given a pair (m, s) the signature s is correct for message m if and only if the equation:

$$\mathrm{m}' = S^{e} \pmod{n}$$

If $\mathrm{m}' = m$ then verified successfully

2.3 ElGamal Scheme

EIGamal signature scheme was first introduced in 1985 and is described in this section. In this signature scheme the public key is used for encryption and signature verification [1]. In the signing process, two functions create two signatures, in the verifying process the output of the functions are compared. In the ElGamal scheme same function is used for signing and verification, but it uses different inputs [20]. For each user, there is a key pair, which consists of a secret key x, and a public key, y where:

$$\mathrm{y} = \mathrm{a}^{x} \pmod{p}$$

The public key y is published in a public file and known to everybody while the secret key x is kept secret. Let m be a document to be signed, where $0 \leq m \leq p-1$ and p is a large prime. The public file consists of the public key $\mathrm{y} = \mathrm{a}^{x} \pmod{p}$ for each user. To sign a document, a user A uses the secret key x_A to compute a signature for message m so that any user can verify that this message has been signed by A, using the public key y_A together with a and p. no one can forge a signature without knowing the secret key x_A. The signature for message m is a pair (r, s), where $0 \leq r, s \leq p-1$, chosen such that :

$$\mathrm{a}^{m} - y^{r} r^{s} \pmod{p} \qquad \text{.....(1)}$$

Signing Phase

The following three steps are done to compute the signature,
1. Choose a random number k, uniformly distributed between 0 and p - 1, such that, gcd (k, p-1)=1

2. Compute,

$$\mathrm{r} = \mathrm{a}^{k} \pmod{p}$$

3. Now (1) can be written as,

$$\mathrm{a}^{m} = a^{xr} a^{ks} \pmod{p}$$

which can be solved for s by using,

$$\mathrm{m} = (\mathrm{xr} + \mathrm{ks}) \mod (p-1)$$

Verification Phase

Given m, r and s, it is easy to verify the authenticity of the signature by computing both side of (1) and checking that they are equal.

2.4 Review of Mohammed, Emarah and Shennawy$'s$ scheme

A new blinding scheme is described in this section by E. Mohammed, A. E. Emarah, Kh. El-Shennawy, it is based on ElGamal signature scheme. ElGamal digital signature scheme shows randomness of k. Thus randomness assures that if the same message is signed twice the two signatures generated will be different. This is not possible in RSA. The mathematics of the new scheme will be explained through the Following example. Suppose that Requester wants the Signer to sign a message for her. The blinding procedure goes as follows [1]:-

Blinding Phase

Requester should Choose a random number k, uniformly between 1 and p - 1, such that, Compute,

$$\mathrm{r} = \mathrm{a}^{k} \mod (p-1)$$

Take a blinding factor h such that

$$\gcd(\mathrm{k},\ \mathrm{p\text{-}1}) = 1$$

Then compute,

$$\mathrm{m}' = hm \mod (p-1)$$

Requester then send m' to Signer [1].

Signing Phase

The Signer receives m' from Requester and treats it as m any ordinary message since the Signer does not recognize the blinding. The Signer computes s' from the relation,

$$\mathrm{m}^{'} = (kx + ks^{'}) \mod (p-1)$$
$$\mathrm{s}^{'} = (m^{'} - xr)k^{-1} \mod (p-1)$$

where $\mathrm{s}^{'}$ is the blinded signature on m. The Signer send $\mathrm{s}^{'}$ to Requester [1]

Un-blinding Phase

Requester should do the following to find the un-blinded signature s for m, ie for h=1

$$\mathrm{s} = \mathrm{xrk}^{-1}(h^{-1} - 1) + h^{-1}s^{'} \mod (p-1)$$

Which is already computed by requester. Now the complete signature pair of message m is (r,s) which are both known to requester but not known to signer [1].

Verifying Phase

Given m,r and s it is easy to verify the authenticity of the signature if,

$$\mathrm{a}^{m} = y^{r}r^{s} \mod (p-1)$$

So, accept [1]

Chapter 3

Scope of the Work

Our scheme can be applicable in real life scenario, where digital document need to be signed without disclosing its content. It is very useful for the application, where security is the prime necessity such as e-cash, e-voting, e-commerce. The proposed scheme has a wide range of scope in confidential transactions [2, 3].

3.1 E-voting

Blind signature is the most popular cryptographic technique in EVS by providing confidentiality of the voters vote. The signature is used to authenticate the voter without disclosing the content of a vote. The authority is not able to know whom a voter votes for [18]. In E-Voting, a vote is blinded in order to achieve its confidentiality. To ensure the secrecy of the voters vote, a voter casts a ballot, blinds a vote using a random number and sends it to the validator. The validator then signs the blinded vote after verifying the voter. After receiving the validated ballot, the voter un-blinds the ballot, to get the true signature, of the validator for the vote see Figure 3.1 [18].

3.2 E-Cash

Setup Phase: The legitimate authority generates a public/private key pair for a signature scheme. This key pair is used for verification of the details of the scheme and the bank's other public keys. The public key is widely published [19]. The bank generates a public/private key pair for a public-key encryption scheme.

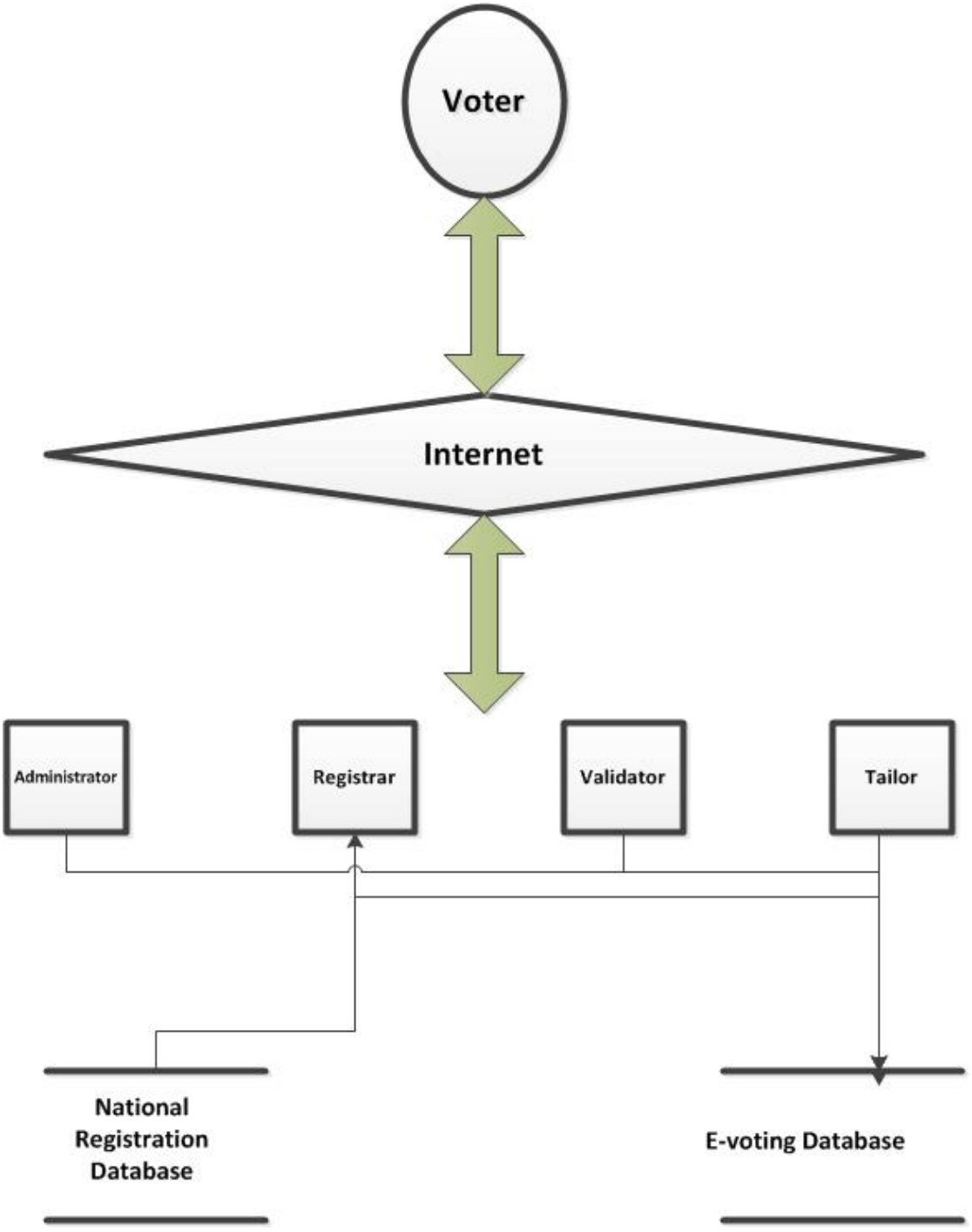

FIGURE 3.1: E-Voting System

The public key is widely published in a certificate signed using the legitimate authority's private key. The legitimate authority generates a series of public/private key pairs for the blind signature scheme for each denomination of coin. These are widely published in certificates signed using the legitimate authority's private key [19].

Withdrawal Phase: The user prepares a coin, which is blank. This contains information, in a predefined agreed format, for the identity of the bank, the denomination of the coin and a randomly chosen serial number. The user undertakes the blind signature protocol on the blank. The user also supply details of what denomination the coin should have and make payment for the coin. The private key is used to generate blind signature for denomination indicated by the user. The coin have a blank and the signature on the blank [19].

Deposit-spend Phase: The user encrypts the coin (blank and the signature) using the bank's public encryption key. The merchant received the ciphertext. The bank received the encrypted coin from the merchant. The bank decrypts it and recovers the coin. The bank now ensures that the signature verifies using the public key specified by the denomination of the coin by the blank. If not, the bank rejects the coin and informs the merchant about this. Otherwise the bank checks to see if the serial number of the coin exists. If so, the bank rejects the coin and the merchant is informed about this. If the serial number isn't valid, then the serial number is added to the database and coin got accepted. The merchant receive payment for coin [19].

3.3 E-Commerce

Often referred to as simply ecommerce, is used to describe business that is conducted over the Internet using any of the applications that depends on the Internet. Electronic commerce, an industry, where buying and selling of product or service is conducted over electronic systems, such as the Internet and other computer networks. Electronic commerce is normally considered as e-business. It also consists of the exchange of data to facilitate the financing and payment aspects of business transactions. Modern electronic commerce typically uses the World Wide Web [27]. It may encompass a wider range of technologies such as electronic-mail, social media, mobile devices, and telephones as well. Mobile, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), automated data collection systems are the technologies used by electronic commerce [27].

Some common applications related to electronic commerce are the following:

- Online Banking
- Electronic Ticket
- Document Automation
- Group Buying
- Online Shopping
- Teleconferencing
- Shopping Cart Software

Chapter 4

Proposed scheme

Proposed scheme emphasis on security. The overall computation overhead for the proposed scheme is lesser than the existing scheme and it can be made more lesser if we compromised with the security. This scheme consists of two participants namely signer (A) and requester (B). The scheme consists of five phases, setup, blinding, signing, un-blinding and verifying.

4.1 Setup Phase

Setup is a phase between a signer and requester in which signer and requester generates their private, public key and system parameters. After generations of keys they publish their public key. Setup phase starts from a P, which is a large prime number, q is a prime factor of (p-1), g is a generator Zq*. The signer chooses his private key $x_a \epsilon Zq*$ and publishes $y_a = g^{x_a} \pmod{P}$. The requester chooses his private key $x_b \epsilon Zq*$ and publishes his public key $y_b = g^{x_b} \pmod{P}$.

4.2 Blinding Phase

In blinding phase, the signer computes by choosing K, β randomly in Zq* and sends v to requester. The requester chooses l, K random and computes,

$$r = g^K \pmod{P}$$

$$S = (K + rx_A) \pmod{P}$$

$$\mathrm{v} = \mathrm{g}^{-S\beta} \pmod{P}$$

The requester sends the blinding message $\mathrm{t}^{'}$ to signer,

$$\mu = g^{l} \pmod{P}$$

$$\mathrm{t}^{'} = h(m, (\mu^{l^{-1}x_\beta})(y_\beta^{S^{-1}x_\beta})v\mu g^{-\alpha}) \pmod{P}$$

4.3 Signing Phase

After receiving $\mathrm{t}^{'}$, the signer generates signature as follows,

$$\mathrm{t} = \mathrm{t}^{'} + \beta$$

$$\mathrm{v}^{'} = tS$$

The Signer sends ($\mathrm{v}^{'}$, t) to the requester.

4.4 Un-blinding Phase

The requester computes,

$$\mathrm{S}^{'} = l - v^{'}$$

$$\mathrm{S}^{''} = (S^{'} - \alpha) \pmod{q}$$

($\mathrm{S}^{''}$, $\mathrm{t}^{'}$, S) is the blinding signature on message m.

4.5 Verifying Phase

Any verifier having message m with signature pair ($\mathrm{S}^{''}$, $\mathrm{t}^{'}$, S) can verify as follows, Compute

$$\mathrm{t}^{''} = h(m, y_\beta, g^{S(1+t')}, g^{S''}) \mod p$$

Check if $\mathrm{t}^{''} = t^{'}$ If so accepts.

4.6 Correctness

This is the prove of the verification of the proposed scheme.

$$\mathrm{t}^{'} = h(m, (\mu^{l^{-1}x_\beta})(y_\beta^{S^{-1}x_\beta})v\mu g^{-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, (g^{l.l^{-1}x_\beta})(g^{x_\beta})^{Sx_\beta^{-1}}.g^{-S\beta}.g^{l}.g^{-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, g^{x_\beta}.g^{S}.g^{-S\beta}.g^{l}.g^{-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{S}.g^{-S\beta}.g^{S'+tS}.g^{-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{S}.g^{-S\beta+S'+tS}.g^{-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{S}.g^{-S\beta+S'+(t'+\beta)S}.g^{-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{S}.g^{-S\beta+S'+t'S+\beta S}.g^{-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{S+S'+t'S-\alpha}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{(S-\alpha)+S(1+t')}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{S''+S(1+t')}) \mod P$$

$$\mathrm{t}^{'} = h(m, y_\beta.g^{S''}.g^{S(1+t')}) \mod P$$

$$\mathrm{t}^{'} = t''$$

Chapter 5

Result

5.1 Implementation result

Comparison of two scheme on the basis of computational time and the signature length. The proposed scheme can be made more efficient than the existing scheme if we compromise with the security feature, but in our scheme the main focus is on security of the Blind Signature. The comparison of the schemes is given in the table below Tables .

5.1.1 Comparison by Computational overhead

Comparison of the two schemes (existing [2.4] and proposed [4]) on the basis of computational time. The proposed scheme [Chapter 4] can be made more efficient than the existing scheme [Chapter 2.4] if we compromise with the security feature, but in our scheme the main focus is on security of the BS. The comparison of the computational time is given below in Table 5.1. The output is shown by Figure 5.1, 5.2.

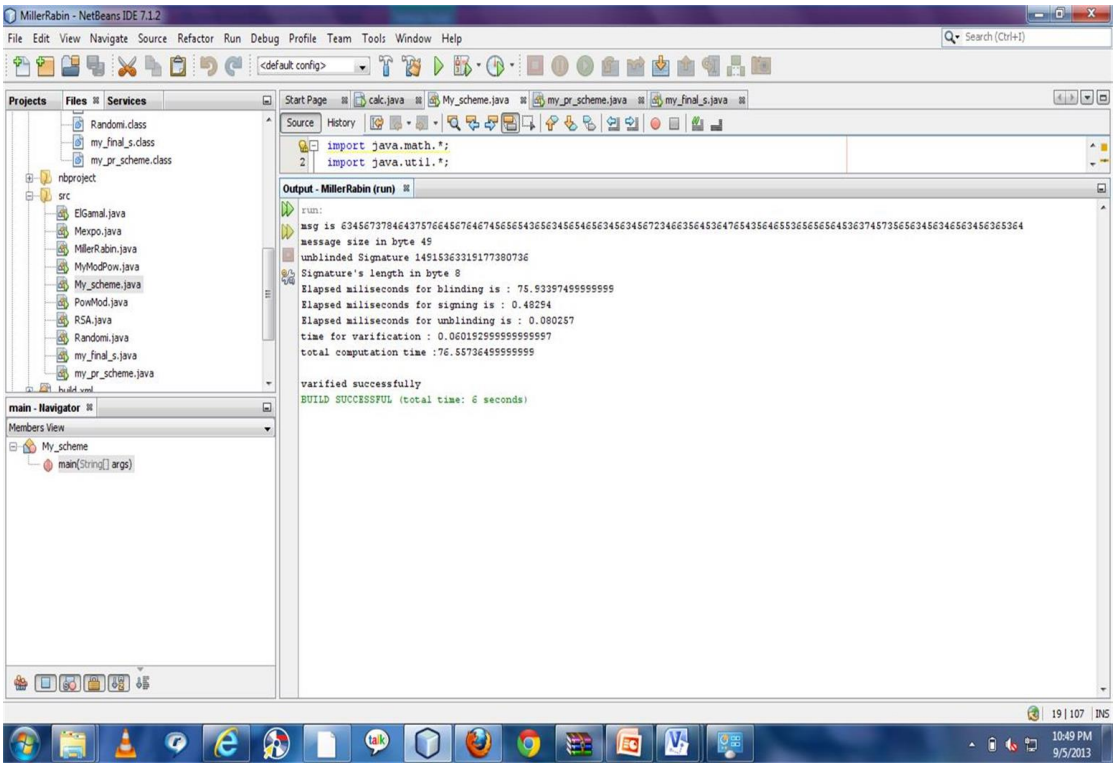

FIGURE 5.1: Existing Scheme

Phases	Existing scheme	Proposed Scheme
Blinding	75.933 ms	1.802 ms
Signing	0.482 ms	0.007 ms
Un-blinding	0.080 ms	0.731 ms
Verification	0.061 ms	0.065 ms
Total computational time	76.557 ms	2.606 ms

TABLE 5.1: Comparison of Computational Overhead

Phase	Signature Length
Existing	8 bytes
Proposed	6 bytes

TABLE 5.2: Comparison of Signature Length

5.1.2 Comparison by Signature Length

Comparison of the two schemes (existing [2.4] and proposed [4]) on the basis of signature length is shoen by Figure 5.1, 5.2. Comparison of signature length is given below in Table 5.2.

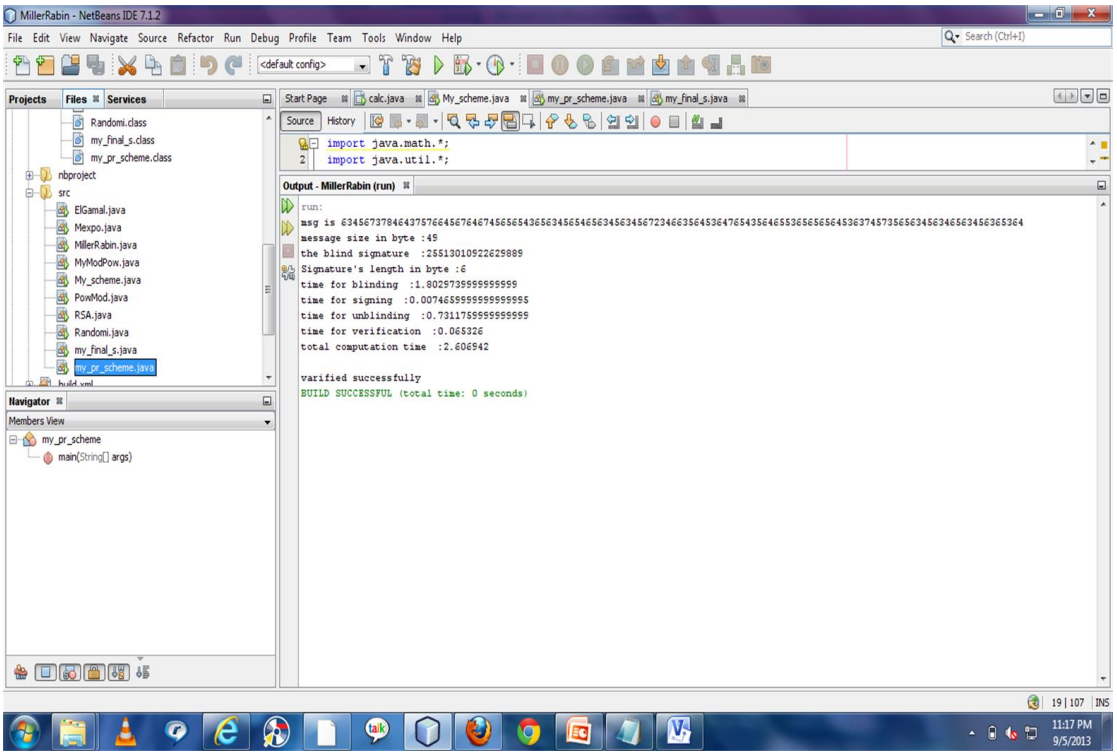

FIGURE 5.2: Proposed Scheme

5.2 Security Analysis

The proposed Blind signature scheme is based upon the security of solving hard computation assumption such as DLP and IFP. It is not possible to attack at this scheme to obtain private keys. The proposed scheme use complex function in order to obtain high security. Analysis of security features is done and found that it is resistant against forgery attack such as existential and selective forgery. Proposed blind signature scheme claims to be more secure than existing scheme. It is reliable for confidential transaction, e-commerce, e-cash, e-voting, communication etc.

Chapter 6

Conclusion

The proposed BS scheme is based upon the hard computation assumption such as DLP and IFP [Chapter 4]. The proposed scheme is implemented in Java. It is also analysed and verified successfully [Chapter 5]. Proposed scheme is compared with the existing scheme [see Table 5.1,5.2] and found that the computation overhead and signature length is lesser for proposed scheme than the existing scheme.The proposed scheme can have wide range of application in areas such as e-cash, e-voting, e-commerce [Chapter 3]. It ensures to be more secure than existing scheme. The proposed scheme ensure, verifiability, non-repudiation, identifiability [2, 3, 4].

References

[1]. E. Mohammed, A. E. Emarah, Kh. El-Shennawy, IEEE Arab Academy for Science and Technology, Air Defense Research Center,2000.

[2]. D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, Springer-Verlag (1983), 199-203.

[3]. D. Chaum, Security without identification: transaction systems to make big brother obsolete, Communications of the ACM 28 (10) (1985), 1030-1044.

[4]. B. Schneier, Applied Cryptography Second Edition, J. Wiley and Sons, 1996.

[5].W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, vol. IT-30,1976.

[6]. F. Zhang and K. Kim, Efficient ID-based blind signature and proxy signature from bilinear pairings, ACISP 03, LNCS 2727, pp. 312-323, Springer-Verlag, 2003.

[7]. Y. Baozheng, X. Congwei, International Conference on Computational Intelligence and Security Workshops Hefei, Anhui, 2007

[8]. S. Doug, Cryptography Theory and Practice, Second Edition, CRC Press, Inc, 2002.

[9]. T. EIGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans.Inform. Theory, vol. IT-31, 1985.

[10]. X. Yang, Zh. Liang, P. Wei and J. Shen, Fifth International Conference on Information Assurance and Security, China, 2009.

[11] W. Stalliigs, Cryptography and Network Security. Principle. and Practice. Second Edition. New Jersey, prentice hall, 1999.

[12] V. Serge, A Classical Introduction to Cryptography: Applications for Communications Security, Springer. p. 254. ISBN 978-0-387-25464-7.,2005.

[13] R. Rivest; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems".

[14]. US ESIGN Act of 2000, State of WI, National Archives of Australia, The Information Technology Act, 2000.

[15]. Borja Sotomayor, "public key cryptosystem", University of Chicago, 2005.

[16]. Frederick J. Hirsch. "SSL/TLS Strong Encryption: An Introduction".

[17]. N. Ferguson; B. Schneier (2003). Practical Cryptography. Wiley. ISBN 0-471-22357-3.

[18]. S. Ibrahim, M. Kamat, M. Salleh and S. R. A. Aziz, Secure E-Voting with Blind Signature, 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003.

[19] A. W. Dent, K. G. Paterson, P. R. Wil, Preliminary Report on Chaum's Online E-Cash Architecture, Royal Holloway, University of London, 2008

[20] B. A. Forouzan, D. Mukhopadhyay, Cryptography and Network Security, 2nd edition.

[21] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science (1994), 124-134.

[22] G.J. Simmons, The Prisoner's Problem and the Subliminal Channel,Advances in Cryptology - Crypto '83, Plenum Press (1984), 51-70.

[23] G.J. Simmons, Subliminal Communication is Easy Using DSA,Advances in Cryptology - Eurocrypt '93, Springer-Verlag (1993), 218-232.

[24] Tkacz, Ewaryst; Kapczynski, Adrian (2009). Internet Technical Development and Applications. Springer. p. 255. ISBN 978-3-642-05018-3. Retrieved 2011-03-28. "The first pilot system was installing in Tesco in the UK (first demonstrated in 1979 by Michael Aldrich)."

[25] D. Russell and G.T. Gangemi Sr, Computer Security Basics, O'Reilly & Associates, Inc., 1991

[26] B.S. Kaliski Jr, RFC 1319: The MD2 Message-Digest Algorithm, RSA Laboratories, April 1992.

[27] M.J. Wiener, Performance Comparison of Public-Key Cryptosytstems, CryptoBytes (1) 4 (Summer 1998)

[28] D. Chaum, Designated confirmer signatures, Advances in Cryptology - Eurocrypt '94, Springer-Verlag (1994), 86-91.

[29] G.J. Simmons, The Subliminal Signatures in the U.S. Digital Signature Algorithm (DSA), 3rd Symposium on State and Progress of Research in Cryptography (February 15-16, 1993), Rome, Italy.

[30] "Tim Berners-Lee: WorldWideWeb, the first Web client". W3.org. Retrieved 2012-12-21

[31] S. I. Ahmed (27 Oct 2009), "GSI Commerce to buy Retail Convergence for $180mln$".$Reuters.Retrieved2013 - 04 - 06$.