View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by ethesis@nitr

A Novel Blind Signature Scheme And Its Variation Based on Discrete Logarithm Problem

A thesis submitted in partial fulfillment

of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Shubhanwita Sukhadarshini

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

May 2012

A Novel Blind Signature Scheme And Its Variation Based on Discrete Logarithm Problem

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Shubhanwita Sukhadarshini
(210CS2321)

under the guidance of

Prof. Sujata Mohanty

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India
May 2012

To my parents

Acknowledgment

Real knowledge is to know the extent of one's ignorance. - Confucius

The more I learn, the more is the need to learn and unlearn.

My humble and deep gratitude to those who have contributed in the completion of this thesis.

This thesis has been the result of the untiring patience and guidance of my advisor Prof.Sujata Mohanty, A true source of inspiration, she has been the key reason for my sustained interest in the topic "A Novel Blind Signature And Its Variation Based On Discrete Logarithm Problem".

My heartfelt thanks also goes to Prof.Sanjaya Kumar Jena and Saroj Panigrahy. Your kind words and unbiased views have always instilled in me the will to quest for more.

My lab mates and batch mates have given me the right kind of support and environment to grow intellectually and personally.

I thank all the members of the Department of Computer Science and Engineering, and the Institute, who helped me by providing the necessary resources, and in various other ways, in the completion of my work.

My family is the the backbone behind all my endeavours with their love and support. No word of thanks can be enough for them for their encouragement, support and belief in me.

My thanks and apologies to those whom I have inadvertently missed out.

Finally, I thank God for everything.

Shubhanwita Sukhadarshini

Abstract

Blind Signature is an addendum of Digital Signature.It is a two party protocol,in which a requester sends a message to a signer to get the signature without revealing the contents of the message to the signer. The signer puts the signature using his/her private keys and the generated signature can be verified by anyone using signer's public keys.Blind signature has a major property called as untraceability or unlinkability i.e after the generation of the signature the signer cannot link the message-signature pair. This is known as blindness property.

We have proposed blind signature scheme and its variation based on discrete logarithm problem(DLP),in which major emphasis is given on the untraceability property. We have cryptanalyzed Carmenisch *et al.*'s blind signature scheme and Lee *et al.*'s blind signature scheme and proposed an improvement over it. It is found that, the proposed scheme has less computational complexity and they can withstand active attacks.

Blind signature has wide applications in real life scenarios , such as, e-cash, e-voting and e-commerece applications.

Contents

Acknowledgement **i**

Abstract **ii**

List of Figures **v**

List of Tables **vi**

List of Abbreviations **vii**

1 Introduction **2**

1.1 Introduction 2

1.1.1 Digital Signature: 2

1.1.2 Blind Signature: 2

1.1.3 Characteristics of Blind Signature 3

1.1.4 Applications of Blind Signature 4

1.1.5 Variations of Blind Signature 5

1.2 Motivation 6

1.3 Related Work 7

1.4 Problem Statement 10

1.5 Thesis Organization 10

2 Mathematics of Cryptography **13**

2.1 Discrete Logarithm Problem 13

2.2 Miller-Rabin Primality Test 13

2.3 Generating Prime Numbers 14

2.4 Hash Function 14

3 A Novel Blind Signature Scheme Based On DLP 16

3.1 Introduction 16

3.2 Review of Carmenish *et al.*'s Blind Signature Scheme 16

3.3 Universal Forgery attack on Carmenish *et al.*'s Blind Signature Scheme 17

3.4 The Proposed Scheme 18

3.5 Security Analysis and Performance Evaluation 20

3.5.1 Security Analysis 20

3.5.2 Performance Evaluation: 22

3.6 Chapter Summery 23

4 An Improvement Over Lee *et al.*'s Scheme 25

4.1 Introduction 25

4.2 Review of Lee-Hwang-Yang Blind Signature Scheme 25

4.3 Review of the attack proposed by Lin *et al.*'s on Lee *et al.*'s Blind Signature Scheme 26

4.4 Proposed Methodology 27

4.5 Chapter Summery 30

5 Conclusion and Future Work 31

Bibliography 32

List of Figures

1.1 Operation of a Blind Signature Scheme 4

1.2 Operation of Chaum's Blind Signature Scheme 7

3.1 Operation of the Proposed Blind Signature Scheme 19

List of Tables

3.1 Computational complexity analysis 23

List of Abbreviations

DLP	Discrete Logarithm Problem
MD	Message Digest

Chapter 1

Introduction

Introduction

Motivation

Related Work

Problem Statement

Thesis Organization

Chapter 1

Introduction

1.1 Introduction

1.1.1 Digital Signature:

The digitization of paperwork has been a major leap in the field of creation and transfer of documents. Digital signature solves the major security concern for the document. It is being a digital analog of handwritten signatures and is crucial for identifying the the sender's identity and also whether the receiver has received it tamper free [1]. The services provided by digital signature are:

- Message integrity
- Non-repudiation
- Authentication

But the big cons of digital signature come when the user needs to identify himself during transactions like purchase (other than cash) or obtaining a service. This breaches the privacy of the person in concern. Organizations now have massive amounts of data, threatening these users' security. Taking it forward, where a digital signature reveals the identity of the person in any transaction whereas a Blind signature protects the sender's privacy and enables the user to get a signature without giving the actual message to the signer.

1.1.2 Blind Signature:

Blind signature gives an answer here enabling the user to conduct e-transactions securely and anonymously without jeopardizing his identity [1–3].It is a two party protocol consisting of a Signer and a group of Requesters.A requester requestes the signer for a valid signature.Without knowing the details of the document, the signer gives the signature using his/her private keys.The signature generated by the signer is a blind signature.When the requester gets the blind signature,first it unblinds the signature, verify it by his/her keys and then reveal the message-signature pair to the public.

1.1.3 Characteristics of Blind Signature

A blind signature protocol must satisfy the following basic properties [4, 5].

- Correctness: Any verifier can check the correcteness of a signature by using the signer's public keys.
- Authenticity: A valid signature indicates that the signer knowingly signed the message.
- Unforgeability: A valid Signer can generate a valid signature for the message.
- Non-reusability: The signature requester can not use the signature more than once.
- Non-repudiation: The signer can not disagree having signed a document that has valid signature.
- Integrity: It says that the contents of the document have not been changed.
- Blindness: It says that while generating a valid signature,the signer is unaware of the message signed by him [6, 7].
- Untraceability/Unlinkability: It says that when the requester publishes the message-signature pair to the public, the signer cannot link the message with the signature [1, 4, 8].
- Confidentiality: No one except the authenticated usedr can modify the contents of the message. [9]

  Operations of a standard blind signature scheme is shown in fig.1.1.

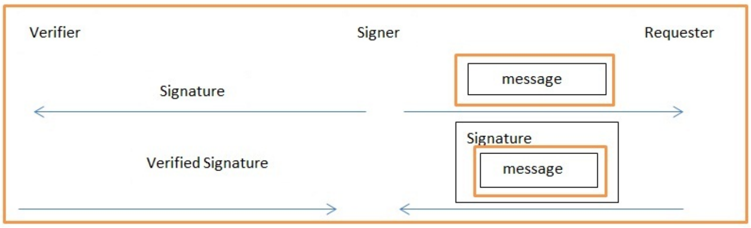

Figure 1.1: Operation of a Blind Signature Scheme

1.1.4 Applications of Blind Signature

E-cash:

e-cash was introduced by David Chaum as an anonymous cash system [10].It is interesting to know that ecoins are blind signatures.

e-cash is a three party protocol, in which a customer or the requester requests for money withdrawal to his/her bank or the signer for buying products from the merchant [11, 12].The signer verifies the authenticity of the requester and then sends signed tokens to the requester.The requester sends the tokens to the merchant and the merchant give the token to the bank for verification of the tokens. So we can see one transaction can give one valid token packet or one valid signature. For multiple transaction the corresponding signatures or the e-coins will be different. But, nowadays many requester becomes malicious and spends the e-coins for multiple times. This is known as the double spending problem.Though blind signature provides untraceability or unlinkability but sometimes it is necessary to reveal the identity of the requester.To do so,one requester should not blind all the internal structure of the message.It should blind the outer part of the message so that by using the public parameters the signer can able to trace the identity of the malicious requester.This is kind of blind signature is known as restrictive blind signature.

E-voting:

In a e-voting system [1, 8, 13–15], a voter first registers himself/herself in a voting system and then sends the blinded vote to the voting system.The voting system then sends the vote to the ballot system.There it is verified whether the voter is a registered or valid voter or not.If yes then the ballot center gives its signature on the vote envelope and send it to the counting system.So the ballot system here gives his signature on the vote envelope without knowing the contents of the envelope.This shows the blindness property. And when the vote is being disclosed the ballot system will unable to link the signature and the vote to a particular instance.This shows the untraceability or unlinkability property of the blind signature.

1.1.5 Variations of Blind Signature

Restrictive Blind Signature:

Restrictive blind signature means that a requester can blind the documents but with some restrictions. It is a protocol which says that any user can request for a blind signature on a document form a valid signer. But it has certain limitations as compared to the normal blind signature. Like normal blind signature the user can blind the message in any way but the choice of the message is restricted and must follow certain rules so that the original message and the blinded message are isomorphic. [4, 5, 16, 17] The blind signature ensures that the signature generated by the signer for one transaction can only be used once.But if the requester becomes malicious and tries to replay the signature again after some time duration then the identity of the requester should be revealed.This can be done by applying restrictive blindness to the normal blind signature scheme.**Revocable Anonymity:**

In any communication,protecting the contents is not enough.Sometimes it is required to keep the identity of the recipient as private.In the context of electronic commerce,If no anonymity is provided then the users preferences can be known .With this information anyone can know the profile of users and send them targeted advertisements or can sell the profiles to other commercial units. The buyer will get problem by this as they want to do the transactions anonymously. Blind signature allows a user to do any transactions anonymously. But in case of any legal disputes e.g money laundering,the identity of the malicious user need to be revealed.This is known as revocable anonymity i.e to revoke the anonymity when needed [18, 19, 21, 22].

Fair Blind Siganture:

Though it is another variation of blind signature, it can be obtained from the restrictive blind signature also.In a fair blind signature protocol a single trustee or multiple trustees may get involved in the system.It is also used to revoke the anonymity of malicious users and the trustte used to do that. To do so,the trustee view all the parts of the blinding process [13, 23]. For this reason the trustee need to be remain online all the time, which compromises the efficiency of the system. Later many fair blind signatures [14, 15] are developed in which the trustee need to keep a public-private key pair. The trustee can only involved in the tracing protocol and by using the key pairs he can trace the identity of the malicious user.

Partial Blind Signature:

To achieve revocable anonymity,another variation of blind signature called as partial blind signature is also used [5, 17].To trace the identity of the malicious user, the signer need to keep some data in the databse during the transaction. This will increase the space of the database. When the requester tries to use the signature twice, the signer checks the database to identify that requester. But to search the databse eachtime is not so feasible. Partial blind signature overcomes this problem. In a partial blind signature protocol,the signer and the requester have some common agreed information. The requester can blind the message but the common agreed information need to be remain unblind. By using the common information the signer can trace the identity of the requester when needed.The concept of partial blind signature was developed by Abe and Okamato [17].

1.2 Motivation

The motivation for this project came from the growing need for a full proof signature verification scheme which can assure untraceability property , conditional anonymity, maximum possible security from the existing schemes. The idea behind the project is also to confirm that the proposed scheme can provide comparable results and if possible better performance than already proposed signature verification schemes.

1.3 Related Work

Blind Signature was first developed by David Chaum in 1982 [2, 9].He developed the blind signature scheme based on factorization problem.He used the RSA signature schemes to implement the signature scheme.

David Chaum's Blind Signature Scheme

Let Bob → the signature requester

Alice → the signer

Alice: Signer

1. Chooses two prime numbers p and p and calculates $n = p \times q$.
2. She calculates $\Phi(n) = (p-1)(q-1)$.
3. She chooses e as the public exponent and calculates d such that $e \times d = 1 \ mod \ \Phi(n)$.
4. She publishes (e, n) as the public keys and keeps d as the private key.

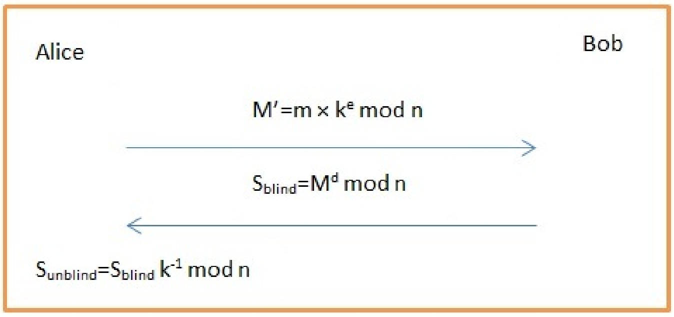

Figure 1.2: Operation of Chaum's Blind Signature Scheme

Bob: Requester

1. Bob chooses a message m to get signed.
2. He chooses k as the blinding factor to blind the message m.

Here M': the blinded message

S_{blind}: the blind on blinded message

$S_{unblind}$: the signature on the actual message

Here the security of the signature scheme depends on the blinding factor k and n.If somebody gets the blinding factor k and be able to factorize n then he/she can get the valid signature from Bob pretending like an authenticated requester.

Blind signature provides sender's privacy at the time of any transactions. Any blind signature scheme should satisfy the unforgeability property which says, except the valid signer no one can produce a valid signature and if a message is signed for multiple times then the corresponding signature will be different. The signature produced in one transaction must be valid for one time only. If the requester becomes malicious tries to use the signature twice then the identity of the requester should be revealed. The above scenario can be well explained by an example of e-cash where the blind signature is widely used. In an e-cash system we know that e-coins are signed blindly. These are bit strings so it can be easily copied and can be spent more than once by the requester. This is known as double spending problem and this should be checked by the signer.

To overcome this problem Chaum developed on-line signature scheme in which the bank or the signer check online whether the the e-coins are spent before or not by checking its database online. But the main drawback is to check the database online is time taking and not feasible enough. To overcome this, Chaum and Pedersen proposed an off-line e-cash system in 1992 using RSA and factoring problem [24]. The scheme proposed by them was able to identify the requester who double spends the e-coins but it occurred after the fact. The scheme could not prevent double spending rather it detects the double spender after the fact. Here the bank used the cut-and-choose method to check whether the requester is a malicious one or not. The bank signs many more e-coins for the user and later ask the user randomly to specify the structure of some of the e-coin. If the user fails to do that then the user is a malicious one.

But the main drawback of this technique is that the workload between the user and the signer increases and the space required to store all the information about the e-coins also increases. Later many methodologies were developed without using the cut-and-choose technique. The proposed schemes were based on factorization problem but in case of factorization problem the security of the scheme lies on a single number.

To overcome this problem Charmenisch *et al.* developed a new blind signature scheme in 1994 based on the discrete logarithm problem [25]. Here the security of the scheme lies in difficulty in solving the discrete logarithm problem. But in 1995, Harn [22] pointed out that Charmenisch *et al.*'s scheme does not satisfy the untraceability property of a blind signature scheme. In his cryptanalysis , he pointed out that the signer in the Carmenisch *et al.*'s scheme can trace the blind signature. By using all the public parameters used in a particular transaction and the message signature pair revealed to the public by the requester, the signer can trace the blind signature. Hoster [20] was complete disagreed with Harn and he claimed that harn's cryptanalysis is wrong upon Cramenisch *et al.*'s scheme. He explained that when the signer tries to trace the blind signature he will find two pairs of signature which satisfies the Harn's equations. So the signer cannot trace blind signature generated by him. But later in Lee *et al.* [10]claimed that Hoster cryptanalysis was wrong. Based on Harn's cryptanalysis Lee *et al.* state that any signer can store all the relevant parameters when the requester requests for the blind signature and can trace the owner of the signature . Lee *et al.* proposed a scheme in 2005 in order to overcome the security limits of Carmenisch *et al.*'s scheme. But in the same year Ting Wu and Jin-Rong Wang [26] pointed out that though Lee *et al.*'s scheme satisfies the untraceability property, the proof of untraceability is not correct and the cost of the scheme is higher than the Carmenisch's scheme . So they proposed an improvement over the Lee *et al.*'s scheme. But in 2007 Lin *et al.* [27] claimed that both of the schemes are not secure enough to resist the attack proposed by them. Lin *et al.* design and attack on both of the scheme and showed that any requester can get more than one valid signature by performing only one transaction which violates the security requirement of blind signature. In Chapter 3 we have proposed an universal forgery attack on Carmenisch *et al.*'s scheme and proved that by choosing some random parameter anyone can forge a valid signature. Later many methodologies were developed based on DLP .

Moreover, many variations of the blind signature scheme were found later like fair blind signature [13, 16, 23], proxy blind signature [7, 28], partial blind signature [17, 29], restrictive blind signature [29]. Among all these the restrictive blind signature scheme proposed by Stefan Brand [30] was widely accepted in the field of e-cash. In literature many schemes are there and they satisfy the untraceability property. But to satisfy the untraceability property with minimum cost is most challenging. The schemes satisfying untraceability have to sacrifice either efficiency or the security. Moreover, all the schemes can trace the identity after the fact. Those schemes cannot prevent the double spending.

To overcome the above drawbacks Stefan Brand proposed a Untraceable off-line restrictive blind signature scheme which can prevent double spending at a minimum cost. This system is equally efficient as the online traceable system.But in this thesis work we have proposed a DLP based blind signature scheme and have proposed an improvement over the Lee *et al.*'s scheme to make this scheme secured against the attack proposed by Lin *et al.*.

1.4 Problem Statement

The objectives of this thesis are:

- To propose a DLP base blind signature scheme, resistant against universal forgery attack.
- To propose some methodologies to prevent the attack proposed on Lee *et al.*'s blind signature scheme by Lin *et al.*

1.5 Thesis Organization

The rest of the thesis is organized as follows.

Chapter 2 describes 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.

Chapter 3 describes the proposed normal blind signature scheme and the Carmenish *et al.*'s scheme [25].We have proposed an universal attack [31] on the Carmenish *et al.*'s scheme.

Chapter 4 describes the Lee *et al.*'s blind signature scheme [10] and the proposed improvement over it to prevent the attack proposed by Lin *et al.* [27].

Chapter 2

Mathematics Of Cryptography

Discrete Logarithm Problem

Miller-Rabin Primality Test

Generation of Prime Numbers

Hash Fuctions

Chapter 2
Mathematics of Cryptography

2.1 Discrete Logarithm Problem

Discrete logarithms were used mainly in computations of finite fields and elliptic curves. Discrete logarithm problem has significant importance in the field of cryptography as the complexity lies in solving the discrete logarithm problem.In case factorization problem,the security of the whole system lies on a single number n.If the attacker can factorize the number n the it will break the security of the system. Whereas, a discrete logarithm problem says it is very easy to compute $a = g^x$ given x and g,where g is the public parameter and x is the private parameter, but it is very difficult to compute x,given a and g,which are public parameters.Here g is the primitive element and it is the element of a cyclic finite gorup [4].
Let $G(q)$ is a group and $G(q)^*$ is the multiplicative subgroup in which all the elements are having their multiplicative inverse.Here q is a prime number.An element g is called as primitive element such that $g \in G(q)$ and it generates the cyclic multiplicative subgroup $G(q)^*$ of the group $G(q)$.Any element$a \in G(q)^* = G(q) - 0$, the discrete logarithm of a with respect to g is that integer x, $0 \leq x \leq q - 1$, for which $a = g^x$.Here $x = log_g^a$. The DLP is very easy to implement and it is used mostly in E-cash system.

2.2 Miller-Rabin Primality Test

In the field of cryptography prime numbers are mostly required. Many methods are there to generate the prime numbers like Fermat's or Mersenne's or Safe prime method. But if at any instance , these methods have failed to create a prime number then problems will arise. To overcome these problems, Cryptography provides many primality testing methods. One of the methods that we have used in our implementation part is Miller Rabin's primality test. Miller Rabin method is a probabilistic algorithm. Miller Rabin primality test is the combination two other probabilistic methods which are Fermat test and Square root test [4]. In this method we write n-1 as the product of an odd number m and a power of two. $n - 1 = m \times 2^k$ As we know, the Fermat test in base a can be written as $a^{n-1} = a^{m \times 2^k} = a^{[m]}$ In the above step instead of calculating a^{n-1} mod n in one step, we are doing it in k+1 steps. The benefit is square root test is performed in each step. If at any step the square root test fails to satisfy then we declare the number as composite.

2.3 Generating Prime Numbers

For generating prime numbers we have used Mersenne Prime method. It has the formula $M_p = 2^p - 1$. As per the formula if p is a prime number then M_p was thought to be prime [4].

2.4 Hash Function

We need the one way hash function to generate the message digest of the message. The message and the message digest is equivalent to a document and the corresponding finger print. We calculate the message digest in order to achieve message integrity. To create the message digest the message is passed through a cryptographic hash function. There are many hash functions designed by Ron Rivest. These hash functions are used to create the message digest. These are referred to as $MD2$, $MD4$, $MD5$. MD stands for message digest. We have used the MD5 hash function to create the message digest. $MD5$ takes the message as the input and divides the message into blocks of 512 bits and creates a digest of 128 bits [4].

Chapter 3

A Novel Blind Signature Scheme Based On DLP

Introduction

Review of Carmenish et al.s blind signature scheme

Forgery attack on Carmenish et al.s blind signature scheme

The Proposed Scheme

Security analysis and performance evaluation

Chapter Summery

Chapter 3

A Novel Blind Signature Scheme Based On DLP

3.1 Introduction

Blind Signature is a two party protocol, in which a requestor sends a request to a signer to give his signature on a message without knowing the message details and a valid signer uses his secret key to sign the document. In order to forge a valid signature, an attacker must know the secret key of the signer. Here we have represented a kind of universal forgery attack in which an attacker,without knowing the secret key of the signer can forge a valid signature by selecting some random parameters. We have developed the universal forgery attack on Carmenisch *et al.*'s blind signature scheme. In this chapter,we have analyzed the possibilities of forging the blind signature scheme and moreover, an improved blind signature scheme is designed.The proposed scheme has been compared with Carmenisch *et al.*'s blind signature scheme and found to have less computational complexity, less execution time and resistivity against the universal forgery attack.

3.2 Review of Carmenish *et al.*'s Blind Signature Scheme

Let p, q be two large primes such that $q|p-1$, and $g \in Z_p^*$ with order q. The signer's secret and public keys are $x \in Z_q$, $y = g^x mod\, p$ respectively.
Carmenisch *et al.*'s scheme is listed as follows:

1. The signer randomly chooses $\hat{k} \in Z_q$ and computes $\hat{r} = g^{\hat{k}} mod\, p$, then he

sends $\hat{r}$ to the requester.

2. The requester randomly chooses $a, b \in Z_q$ and computes $r = \hat{r}^a g^b mod\, p$, then he blinds the message m by computing $\hat{m} = am\hat{r}r^{-1} mod\ q$. After that, he transmits $\hat{m}$ to the signer.

3. The signer computes $\hat{s} = x\hat{r} + \hat{k}\hat{m}\ mod\ q$ and forwards it to the requester.

4. The requester derives s by computing $s = \hat{s}r\hat{r}^{-1} + bm\ mod\ q$.

   Finally, the requester gets the blind signature (r, s) of the message m, satisfying $g^s = y^r r^m\ mod\ p$.

3.3 Universal Forgery attack on Carmenish *et al.*'s Blind Signature Scheme

In this section, we followed the universal forgery attack developed by Baozheng, Congwei [23].We applied the attack on Carmenisch *et al.*'s scheme to show that the scheme is not secured enough to resist this attack. Let's assume that Eve is an attacker. She can forge a valid signature pair (r_1, s_1) of M using the following steps.

1. Chooses two random numbers $a, b \in Z_q^*$.
2. Computes $r = g^{a^{-1}} y^b$
3. Computes $s = -a^{-1}b^{-1}g^{a^{-1}}y^b$
4. Computes $m = -b^{-1}g^{a^{-1}}y^b$

Now. We show that (r_1, s_1) is a valid signature on the message M. As,

$$\begin{aligned} y^r r^m &= y^r (g^{a^{-1}} y^b)^{-b^{-1} g^{a^{-1}} y^b} \\ &= y^r g^{-a^{-1} b^{-1} g^{a^{-1}} y^b} y^{-b b^{-1} g^{a^{-1}} y^b} \\ &= y^r g^{-a^{-1} b^{-1} g^{a^{-1}} y^b} y^{-g^{a^{-1}} y^b} \\ &= y^r g^{-a^{-1} b^{-1} g^{a^{-1}} y^b} y^{-r} \\ &= g^s \end{aligned}$$

From the above steps we can see that the random parameters (r_1, s_1) satisfies the verification equation of Carmenisch *et al.*'s blind signature scheme. To avoid this kind of attack, the solution is to use hash function in the blinding phase.So the verification equation would look like $g^s = y^r r^{h(m)}$.It may be possible that the attacker would choose the random parameter $h(m)$ to satisfy the verification equation but can never get the message M from $h(M)$ as h(.) is a one way hash function. Keeping the above point into consideration,we have proposed a blind signature.

3.4 The Proposed Scheme

The proposed blind signature scheme consists of two parties, namely, a requester(R) and a signer(S).The requester sends a message M in a blinded form to the signer to get the signature.The signer generates the signature for the message M without knowing it's contents and sends the signature to the requester. After getting the blinded signature from the signer, the requester unblinds it to get the original signature for its message M. If we summarize the above steps then the scheme consists of following five phases: Key generation (for signer and the receiver), Set up, Blinding, Signing process, Verifying and Unblinding.

Key generation: The signer randomly selects two distinct large prime numbers p and q , a group generator g from which is a group of prime order q and computes $n = p * q$. The signer selects a number x as the secret key from Z_n^* and computes $y = g^x mod n$ .Selects a random number w from Z_n^* . The signer publishes n, g, y

Figure 3.1: Operation of the Proposed Blind Signature Scheme

as the public key and keep x, w as the private key. The requester randomly selects s, u, v from Z_n^* and computes

$$I = g^u \, mod \, n \tag{3.1}$$

The requester publishes I as the public key and keeps s, u, v as the private key. In addition, let H be a public one-way hash function.

Set up: The signer computes z, b as per the following equations by using the public key I of the requester.

$$z = I^x \, mod \, n \tag{3.2}$$

$$b = I^w g \, mod \, n \tag{3.3}$$

The signer sends (z, b) to the requester.

Blinding Phase: The overall process of Proposed Scheme is shown in Fig.1. The requester computes the following parameters.

$$C = H(M \| z \| b) \tag{3.4}$$

$$C_b = Cu^{-1} \, mod \, n \tag{3.5}$$

Then the requester sends the blinded message C_b to the signer.

Signing Phase: After receiving the parameter C_b from the requester, the signer computes the signature r as follows.

$$r = (C_b x + w) \, mod \, n \tag{3.6}$$

The signer sends the signature r to the requester.

Verification and Unblinding Phase: When the requester gets the signature r from the signer it verifies the authenticity by checking the following condition.

$$(I^r g) = Z^{C_b} b \, mod \, n \tag{3.7}$$

If the above verification equation holds, then the requester unblinds the signature by computing r_b as per the following equation.

$$r_b = (ru + v) \, mod \, n \tag{3.8}$$

The (r, r_b) is the signature on message M.

3.5 Security Analysis and Performance Evaluation

In this section, we have analyzed the security of the proposed scheme and the scheme is compared with the existing scheme [25].Moreover, it is verified that the proposed scheme can withstand the universal forgery attack. Correctness of the proposed scheme is also done. Also we have presented a comparative analysis in terms of computational complexity.

3.5.1 Security Analysis

Correctness

The signature generated by the proposed scheme is indeed a valid one.

Proof:

$$\begin{aligned}
I^r g &= (g^u)^r g \, mod \, n && \text{[As derived from eq.3.1]} \\
&= g^{u(C_b x + w)} g \, mod \, n && \text{[As derived from eq.3.14]} \\
&= g^{u C_b x} g^{uw} g \, mod \, n && \\
&= I^{x C_b} b \, mod \, n && \text{[As derived from eq.3.1, eq.3.3]} \\
&= z^{C_b} b \ mod \, n && \text{[As derived from eq.3.2]}
\end{aligned}$$

□

Theorem 1: ***The proposed scheme can withstand the blindness property.***

Proof: The impaired vision of blind signature schemes ensures that the signer is ignorant of the message M in the signing phase. In the proposed scheme, the message M is also protected with the random number u in the signing phase as shown is eq.[3.5]. The signer only knows the temporary variable C_b as shown is eq.[3.5], but not the message M. The signer can't factor C_b to obtain M because he does not know u.

Theorem 2: ***The signature generated by the proposed scheme is untraceable.***

Proof: The term Untraceability indicates that the signer of the blind signature is unable to link the message-signature pair after the same has been revealed to the public. Here when the signer gives his signature on the blind message C_b, it is encoded in a manner unknown to him. Incase the same encrypted set of message and signature reaches him, he would not be able to identify whether it was originally sent by him or not. This theorem shows that the proposed scheme holds the untraceability property. Here as per the signers view the signature on the message is r. But after getting the signature on the blind message, the requester unblinds the signature and the message .So r_b is the unblinded signature. As per the eq.[3.6], the parameters C_b ,w are random. So for any two messages M_1 and M_2, the value of C_b will be different and the value of w will also be different, as a result, the value of r will be different. If the value of r is different for any two messages M_1 and M_2, then r_b will be different as in eq.[3.8], (r, u, v) all are random. So when the requester, after getting the actual signature rb on the original message M, sends the message signature pair(M, r_b) to the signer, then he will not be able to recognize his own signature on the message as the value of r and r_b must be different.

Theorem 3: ***The proposed scheme withstands the forgeability attack.***

Proof: The adversary can never forge the signature of the signer. From all the public parameters n, g, z, b, y provided by the signer , it is possible to find out the secret key w, x of the signer as shown in eq.[3.2,3.3].The adversary cannot compute x from publicly available parameters y and z as it is equals to solve the discrete logarith problem.Similarly, from the publicly available parameter b, the adversary cannot compute the secret key w.So,for an adversary,it's very difficult to get the secret keys from the publicly available parameters, as the security lies in the complexity of solving discrete logarithm problem. Until and unless he gets the secrete keys x, w of the signer he can never forge the signature r of the signer as shown in eq.[3.6].

Definition 1: *Universal forgery attack:* The unforgeability property of blind signature protocol says that, except a valid signer no one can generate a valid signature.A valid Signer can only produce the valid signature by using his/her private keys.So,to forge a signature,the private key of the signer is required. But in case of universal forgery attack [23] anyone can generate a valid signature without using the private keys of the signer and can reveal the message contents of the requester.In this attack any attacker can produce a valid signature by choosing some random parameters satisfying the verification equation.

Theorem 4: ***The Proposed scheme can withstand the universal forgery attack.***

Proof: In this scheme we are blinding the message digest C rather than the message M itself. Though by selecting some random parameters, the attacker Eve can forge the signature but she can never get the message M as here we have used the one way hash function in creating the digest of the message.

3.5.2 Performance Evaluation:

The computational complexity of any cryptographic algorithm mainly depends upon on four major operations, namely, number of inverse operation, number of hash function, number of exponential and number of multiplication operation. Ignoring the time for performing addition and subtraction operation in the analysis process, the following notations are used to analyze the performance of the proposed scheme with comparison to the existing scheme.

- T_E is the time complexity of modular exponentiation

- T_M is the time complexity of multiplication
- T_H is the time complexity of hash function
- T_I is the time complexity of inverse function

Phases	Carmenisch *et al.*'s Scheme [25]	Proposed Scheme
Key generation and set up	$2T_E$	$3T_E$
Blinding	$T_I + 4T_M + 2T_E$	$T_I + T_H + T_M$
Signing	$2T_M$	T_M
Verification	$3T_E + T_M$	$2T_E + 2T_M$
Unblinding	$3T_M + T_I$	T_M

Table 3.1: Computational complexity analysis

In the proposed scheme the requester sends a file M which contains the message, to the signer to get the signature r for it. We have compared various phases of the proposed scheme with Carmenisch *et al.*'s scheme [25] and the compared performance evaluation is shown in table 3.1.

From Table 3.1, it is clear that the proposed scheme consists of minimum no. of operations. Hence the computation cost of the proposed scheme is much less.

3.6 Chapter Summery

This Chapter summerizes, if a requester wants to get the signature on its message M without revealing the contents of the message to the signer,then he/she can get that. The scheme proposed in this Chapter,consists of less computational complexity. It would be a better alternative for some organizational operations, as through this, the security requirements of integrity, confidentiality, authenticity, and non-repudiation can be simultaneously achieved with low computation and communication cost. This scheme can be applicable to real life scenarios such as e-commerce applications.

Chapter 4

An Improvent Over Lee *et al.*'s Scheme

Introduction

Review of Lee-Hwang-Yang blind signature scheme

Review of the attack proposed by Lin et al.*s on Lee* et al.*s blind signature scheme*

Proposed Methodologies

Chapter Summery

Chapter 4

An Improvement Over Lee *et al.*'s Scheme

4.1 Introduction

In 2005, Lee *et al.* proposed a blind signature scheme, satisfying the two basic properties of blind signature, which are blindness and untraceability. An improved and simplified version of the Lee *et al.*'s scheme [10] was proposed by Wu and Wang [26]. In 2008, Lin *et al.*, proposed an attack [27] on both Lee *et al.*'s and Wu and Wang's scheme and showed that both of the schemes are not secure. They designed an attack on both the schemes such that a signature requester can obtain two different valid signatures for two different messages from one transaction, which contravene the security of the blind signature. In this chapter, we proposed some methodologies through which the signer can prevents the signature requester from getting more than one valid signatures by performing only one round of the protocol.

4.2 Review of Lee-Hwang-Yang Blind Signature Scheme

In this section we briefly review the blind signature proposed by Lee *et al.*'s [10]. The scheme consists of two parties namely the signer and a group of signature requester. The requester requests the signer to get a signature on the message m. Here the signer is unaware of the message contents which satisfies the blindness property of a blind signature. The details of the Lee *et al.*'s scheme is given below. Initially the signer chooses two large prime numbers p and q where $q|(p-1)$ and a generator g of order q from Z_p^*. The signer selects an integer x and keeps it as the secrete key. The signer computes $y = g^x \, mod \, p$ and publishes it along with p, q, g as the public key. The signer chooses four random numbers $(\hat{k_1}, \hat{k_2}, b_1, b_2)$ from Z_q and computes $\hat{r_1} = g^{\hat{k_1}} \, mod \, p, \hat{r_2} = g^{\hat{k_2}} \, mod \, p$ such that $GCD(\hat{r_i}, q) = 1$.

The signer sends the parameters $(\hat{r_1}, \hat{r_2}, b_1, b_2)$ to the requester. When the requester receives $(\hat{r_1}, \hat{r_2}, b_1, b_2)$ from the signer, he chooses five random numbers(a, b, c, d, e) and keeps them as the secret parameters. The requester then computes $r = (r_1 r_2)^d \, mod \, p$ where $r_1 = \hat{r_1}^{ab_1} g^c \, mod \, p$ and $r_2 = \hat{r_2}^{bb_2} g^e \, mod \, p$. Then the requester blinds the message m by computing $\hat{m_1} = m\hat{r_1}r^{-1}/2 \, ad \ mod \, q$ and $\hat{m_2} = m\hat{r_2}r^{-1}/2 \, bd \ mod \, q$ and sends $(\hat{m_1}, \hat{m_2})$ to the signer. After getting the parameters $(\hat{m_1}, \hat{m_2})$ from the requester, the signer computes the corresponding signature $\hat{s_1}$ and $\hat{s_2}$ for $(\hat{m_1}, \hat{m_2})$ as follows and sends $(\hat{s_1}, \hat{s_2})$to the requester.

$$\hat{s_1} = x\hat{r_1} + \hat{k_1} b_1 \hat{m_1} \, mod \, q \tag{4.1}$$

$$\hat{s_2} = x\hat{r_2} + \hat{k_2} b_2 \hat{m_2} \, mod \, q \tag{4.2}$$

When the requester receives the parameters (s_1, s_2) from the signer, he computes the signature s as follows.

$$s_1 = \hat{s_1}\hat{r_1}^{-1} r/2 + cdm \, mod \, q \tag{4.3}$$

$$s_2 = \hat{s_2}\hat{r_2}^{-1} r/2 + edm \, mod \, q \tag{4.4}$$

$$s = (s_1 + s_2) \, mod \, q \tag{4.5}$$

Then the requester publishes $(m \, , \, r \, , \, s)$ to the public. One can verify the triplet by checking the verification equation $g^s \equiv y^r r^m \, mod \, p$.

4.3 Review of the attack proposed by Lin *et al.*'s on Lee *et al.*'s Blind Signature Scheme

Form the cryptanalysis of Lee *et al.*'s blind signature scheme, Lin *et al.* concluded that, if the requester becomes malicious, he/she can sends two different messages m_α,m_β to get two different signatures s_1,s_2 from the signer respectively by performing only one transaction [27]. The proposed attack is described below.

Instead of computing $r_1 = \hat{r_1}^{ab_1} g^c \, mod \, p$ and $r_2 = \hat{r_2}^{bb_2} g^e \, mod \, p$ and $r = (r_1 r_2)^d$

in the scheme of section 2, the requester computes $r_1 = (r_1^{ab_1} g^c)^d \, mod \, p$ and $r_2 = ({r_2}^{bb_2} g^e)^d \, mod \, p$ as he doesn't need r in the attack. The requester then computes $\hat{m_1} = m_\alpha \hat{r_1} r_1^{-1} ad \, mod \, q$ and $\hat{m_2} = m_\beta \hat{r_2} r_2^{-1} bd \, mod \, q$ and sends (m_1, m_2) to the signer. The signer computes s_1, s_2 and sends it to the requester.

$$\hat{s_1} = x\hat{r_1} + \hat{k_1} b_1 \hat{m_1} \, mod \, q \tag{4.6}$$

$$\hat{s_2} = x\hat{r_2} + \hat{k_2} b_2 \hat{m_2} \, mod \, q \tag{4.7}$$

Then the requester computes

$$s_1 = \hat{s_1} \hat{r_1}^{-1} r_1 + cdm_\alpha \, mod \, q \tag{4.8}$$

$$s_2 = \hat{s_2} \hat{r_2}^{-1} r_2 + edm_\beta \, mod \, q \tag{4.9}$$

By doing this the requester gets two message signature pairs (m_α, r_1, s_1) and (m_β, r_2, s_2), satisfying two verification equations $g^{s_1} \equiv y^{r_1} {r_1}^{m_\alpha} \, mod \, p$ and $g^{s_2} \equiv y^{r_2} {r_2}^{m_\beta} \, mod \, p$.

4.4 Proposed Methodology

In Lee *et al.*'s Scheme the requester sends $(\hat{m_1}, \hat{m_2})$ to the signer, where $\hat{m_1}$,$\hat{m_2}$ are the blinded form the same message contents m .Here only the blinding process is different for them. The requester does this, just to check the message integrity. When the signer gets these two parameters $\hat{m_1}$,$\hat{m_2}$ form the requester, he sends two different signatures $\hat{s_1}$,$\hat{s_2}$ to the requester as shown in eq[5.6 and 5.7]. The motive behind sending two blinded form of the message to the signer may be to check whether the message contents from these two signature is same or not. If a requester becomes malicious and sends two different message in two different blinded form to the signer, then it is the duty of the signer to recognize that and if he finds that the requester have used two different message contents in $\hat{m_1}$ and $\hat{m_2}$ then he simply dismiss the transaction.

Case I:

To do so, the signer can add one authentication equation of the message after when he gets the $\hat{m_1}$,$\hat{m_2}$ parameters from the requester.

As we know,

$$\hat{m_1} = m\hat{r_1}r^{-1}/2\,ad\;mod\,q \tag{4.10}$$

$$\hat{m_2} = m\hat{r_2}r^{-1}/2\,bd\;mod\,q \tag{4.11}$$

from the above two equations one can derive m as follows.

$$m = \hat{m_1}\hat{r_1}^{-1}r/2(ad)^{-1}\,mod\,q \tag{4.12}$$

$$m = \hat{m_2}\hat{r_2}^{-1}r/2(bd)^{-1}\,mod\,q \tag{4.13}$$

From the above two equations, the signer knows the parameters (r_1, r_2, m_1, m_2) only (r, a, b, d) are unknown to him.

Let the signer replaces,

$$r_1/2(ad)^{-1} \;=\; c_1$$

and

$$r_2/2(bd)^{-1} \;=\; c_2$$

So the eq[4.12 and 4.13] become

$$m = \hat{m_1}\hat{r_1}^{-1}c_1\,mod\,q \tag{4.14}$$

$$m = \hat{m_2}\hat{r_2}^{-1}c_2\,mod\,q \tag{4.15}$$

For some set of values of (c_1, c_2) the eq.[4.14 and 4.15] will be same if the message contents is same for $\hat{m_1}$ and $\hat{m_1}$ as per Lee *et al.*'s scheme described in section 4.2. So the signer can add the following authentication equations,once he receives the parameters $(\hat{m_1}, \hat{m_2})$ to check the message integrity.

$$m \;=\; \hat{m_1}\hat{r_1}^{-1}c_1\,mod\,q$$

$$m = \hat{m_2}\hat{r_2}^{-1}c_2\, mod\, q$$

As per Lin *et al.*'s scheme described n section 3.3

$$\hat{m_1} = m_\alpha \hat{r_1}{r_1}^{-1}\, ad\ mod\, q$$

$$\hat{m_2} = m_\beta \hat{r_2}{r_2}^{-1}\, bd\ mod\, q$$

So,

$$m_\alpha = \hat{m_1}{r_1}^{-1}r_1\,(ad)^{-1}\ mod\, q \tag{4.16}$$

$$m_\beta = \hat{m_2}{r_2}^{-1}r_2\,(bd)^{-1}\ mod\, q \tag{4.17}$$

From the above two equations, the signer knows the parameters $(r_1, r_2, \hat{m_1}, \hat{m_2})$ only. r_1, r_2, a, b, d are unknown to him.
Let the signer replaces,

$$r_1/2(ad)^{-1} = c_1$$

and

$$r_2/2(bd)^{-1} = c_2$$

So the eq.[4.16 and 4.17] become

$$m_\alpha = \hat{m_1}{r_1}^{-1}c_1\, mod\, q \tag{4.18}$$

$$m_\beta = \hat{m_2}{r_2}^{-1}c_2\, mod\, q \tag{4.19}$$

For some set of values of (c_1, c_2) the eq.[4.18 and 4.19] will never be same if the message contents is not same for $\hat{m_1}$ and $\hat{m_2}$ as per Lin *et al.*'s scheme described in section 4.3.
So, here the parameters $(\hat{m_1}, \hat{m_2})$ will fail to satisfy the authentication equations [4.12 and 4.13]sets by the signer. So the signer will dismiss the transaction.

4.5 Chapter Summery

In this chapter we have verified that the attack proposed by Lin *et al.*'s on Lee *et al.*'s scheme can be prevented. If a requester becomes malicious and tries to get two valid signatures for two different messages from one transaction, then the signer can prevent this by checking the authentication equations or by giving only one signature s for $(\hat{m_1}, \hat{m_2})$ instead of giving two signatures s_1 and s_2 as in Lee *et al.*'s scheme.

Chapter 5
Conclusion and Future Work

The proposed blind signature schemes are indeed valid ones as they satisfy the blindness, unlinkability and unforgeablity property. The proposed schemes are more secure than the normal blind signature scheme as one of the scheme is resistant against the universal forgery attack and the other one is resistant against the attack proposed by Lin *et al.* on Lee *et al.*.As the proposed schemes satisfies the untaceability and blindness propoerty, it can be widely used in real life scenarios like e-commerce applications and online bidding. The proposed scheme can further be implemented in differenet variations of blind signature as proxy blind signature,restrictive blind signature, fair blind signature, partial blind signature, restrictive partial blind signature and so on.

Bibliography

[1] D.Pointcheval and J.Stern. Security arguments for digital signatures and blind signatures. *JOURNAL OF CRYPTOLOGY*, 13(3):361–396, 2001.

[2] D. Chaum. *Blind signatures for untraceable payments*, volume 82, pages 199–203. Plenum Publishing, 1983.

[3] J. X. Zhao H. Q.Wang and L. J. Zhang. Blind signature scheme based on elgamal signature equation. *Nanjing University of Posts and Telecommunication*, 25(4):65–69, 2005.

[4] B.A.Farouzan. *Cryptography & Network Security*. Tata McGraw-Hill Publishing Company Limited, Inc.,New York, 2007.

[5] E. Mohammed, A.E. Emarah, and K. El-Shennawy. A blind signature scheme based on elgamal signature. In *EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA*, pages 51 –53, 2000.

[6] S.Mohanty and B.Majhi. A secure multi authority electronic voting protocol based on blind signature. In *Proceedings of the 2010 International Conference on Advances in Computer Engineering*, pages 271–273. IEEE Computer Society, 2010.

[7] S.Wang, F.Hong, and G.Cui. Secure efficient proxy blind signature schemes based dlp. In *Proceedings of the Seventh IEEE International Conference on E-Commerce Technology*, pages 452–455. IEEE Computer Society, 2005.

[8] G.Qadah and R.Taha. Electronic voting systems: Requirements, design, and implementation. *Computer Standards Interfaces*, 29(3):376–386, 2009.

[9] D.Chaum. Blind signature system. In *CRYPTO*, page 153, 1983.

[10] C.C.Lee, M.S.Hwang , and W.P.Yang. A new blind signature based on the discrete logarithm problem for untraceability. *Applied Mathematics and Computation*, 164(3):837–841, 2008.

[11] H.F.Huang and C.C.Chang. An untraceable electronic cash system using fair blind signatures. *E-Business Engineering, IEEE International Conference on*, 0:39–46, 2006.

[12] K.Chen W.Qiu and D.Gu. A new offline privacy protecting e-cash system with revokable anonymity. In *Proceedings of the 5th International Conference on Information Security*, pages 177–190. Springer-Verlag, 2008.

[13] J.M.Piveteau J.Camenisch and M.Stadler. An efficient fair payment system. In *ACM Conference on Computer and Communications Security*, pages 88–94, 1996.

[14] Y.Tsiounis Y.Frankel and M.Yung. *Indirect Discourse Proofs.*

[15] Jan Camenisch, Ueli Maurer, and Markus Stadler. Digital payment systems with passive anonymity-revoking trustees. *J. Comput. Secur.*, 5(1):69–89, 1997.

[16] Weidong and Qiu. Converting normal dlp-based signatures into blind. *Applied Mathematics and Computation*, 170(1):657–665, 2009.

[17] Masayuki Abe and Tatsuaki Okamoto. Provably secure partially blind signatures, 2000.

[18] D. Chaum, M. Jakobsson, R. L. Rivest, P. Y. A. Ryan, J. Benaloh, M. Kutylowski, and Ben Adida. Towards trustworthy elections, new directions in electronic voting. In *Towards Trustworthy Elections*, volume 6000 of *Lecture Notes in Computer Science*. Springer, 2010.

[19] D.Alessio and M.Joye. A simple construction for public-key encryption with revocable anonymity. In *Proceedings of the ninth ACM workshop on Digital rights management*, pages 11–16. ACM, 2010.

[20] M.Michels P.Hoster and H.Petersen. Comment:cryptanalysis of blind signatures bades on discrete logarithm problem. *Electronic Letters*, 31(21):1827, 1995.

[21] R.Wendolsky S.Kopsell and H.Federrath. Revocable anonymity. In *In Gnter Mller (Ed.): ETRICS 2006, Lecture Notes in Computer Science*, pages 208–222. Springer Verlag, 2006.

[22] L.Harn. Cryptanalysis of blind signatures bades on discrete logarithm problem. *Electronic Letters*, 31(14):1136–1137, 1995.

[23] Ernie Brickell, Peter Gemmell, and David Kravitz. Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *In Proceedings of the Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 457–466, 1995.

[24] D. Chaum and T. P. Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO 92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 1992.

[25] J.M Piveteau J.Camenisch and M. Stadler. Blind signatures based on the discrete logarithm problem. In *Advances in Cryptology - EUROCRYPT '94*, pages 428–432, 1994.

[26] T.Wu and J.R Wang. Comment: A new blind signature based on the discrete logarithm problem for untraceability. *Applied Mathematics and Computation*, 170(1):999–1005, 2009.

[27] C.I Wang C.I Fan, D. J. Guan and D.R.Lin. Cryptanalysis of lee-hwang-yang blind signature scheme. *Computer Standards & Interfaces*, 31(2):319–320, 2009.

[28] A.N.Oo and N.L.Thein. DLP based proxy blind signature scheme with Low-Computation. *Networked Computing and Advanced Information Management, International Conference on*, 0:285–288, 2009.

[29] X.F.Chen S.L Liu and F.G Zhang. Forgeability of wang-tang-li's id-based restrictive partially blind signature scheme. *J. Comput. Sci. Technol.*, 23(2):265–269, 2010.

[30] S.Brands. Untraceable off-line cash in wallets with observers. In *Advances in Cryptology - CRYPTO'93*, pages 302–318. Springer-Verlag, 1993.

[31] B. Yu and C. Xu. Security analysis on a blind signature scheme based on elgamal signature equation. In *Proceedings of the 2007 International Conference on Computational Intelligence and Security Workshops*, pages 741–744. IEEE Computer Society, 2007.

[32] J.Camenisch and T. Gro. Efficient attributes for anonymous credentials extended version. *IACR Cryptology ePrint Archive*, 2010:496, 2010.

[33] D. Chaum, R. L. Rivest, B. Preneel, A. D. Rubin, D. G. Saari, and P. L. Vora. Guest editorial: special issue on electronic voting. *IEEE Transactions on Information Forensics and Security*, 4(4):593–596, 2009.

[34] I.C.Lin, M.S.Hwang , and C.C.Chang. Security enhancement for anonymous secure e-voting over a network. *Comput. Stand. Interfaces*, 25(2):131–139, 2003.

[35] X.Hu and S.Huang. An efficient id-based restrictive partially blind signature scheme. In *Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing - Volume 03*, pages 205–209. IEEE Computer Society, 2010.