Development of an ECDLP based Traceable Blind Signature Scheme And its Application to E-Auction

Rohit Kumar Das

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

Development of an ECDLP based Traceable Blind Signature Scheme And its Application to E-Auction

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

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Rohit Kumar Das

(Roll No: 212CS2365)

under the guidance of

Dr. Banshidhar Majhi

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

May, 2014

Dedicated to my family and friends

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

Certificate

This is to certify that the work on the thesis entitled "***Development of an ECDLP based Traceable Blind Signature Scheme and its Application to E-Auction***" submitted by ***Rohit Kumar Das***, bearing roll number ***212CS2365***, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology* in *Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Banshidhar Majhi
Professor
Department of CSE
National Institute of Technology
Rourkela-769008

Acknowledgment

First of all, I would like to thank, the Almighty God, without whose blessings I wouldn't have been writing this "thesis".

I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Banshidhar Majhi, who has been the guiding force behind this work. I want to thank him for introducing me to the field of Electronic Commerce and giving me the opportunity to work under him. Without his invaluable advice and assistance, it would not have been possible for me to complete this thesis. I consider it my good fortune to have got an opportunity to work with such a skillful person.

My hearty thanks go to Prof. Sujata Mohanty for showing me innovative research directions for conducting the research successfully. I am indebted to all the professors, co-researchers, batch mates and friends at National Institute of Technology Rourkela for their active or hidden cooperation.

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. I cannot resist myself quoting my thanks to the developers of LaTeX compiler for making the thesis writing an experience indeed.

When I look back at my accomplishments in life, I can see a clear trace of my family's concerns everywhere. My dearest mother, whom I owe everything I have achieved, my beloved father, for always believing in me and inspiring me, and my sister, who is always my silent support throughout my life. This thesis is a dedication to them who did not forget to keep me in their hearts when I could not be beside them.

Rohit Kumar Das

Abstract

With the increase in internet users, E-Commerce has been grown exponentially in recent years. E-Auction is one among them. But its security and robustness is still a challenge. The electronic auction centers remain to be insecure and anonymity, bid privacy and other requirements are under the threat by malicious hackers. Any auction protocol must not leak the anonymity and bid privacy of an honest bidder. Keeping these requirements in mind, we have proposed a new electronic auction scheme using blind signature. Moreover our scheme is based upon elliptic curve cryptography which provides similar level of security with comparatively smaller key size. Due to the smaller key size, the space requirement can be reduced which further allows our E-Auction scheme to implement in a mobile application which has a constrained environment like low bandwidth, memory and computational power.

Blind signature is a special kind of digital signature where the message privacy can be retained by blinding the message and getting a signature on that. It can be universally verifiable and signer can't repudiate of signing the document. Moreover it also satisfies the integrity and authenticity of the message. Due to these features of a blind signature, it can easily be applied on an E-Auction scheme. So we have proposed an efficient blind signature protocol according to the requirements of E-Auction which is based upon the hard problem of solving elliptic curve discrete logarithm problem(ECDLP). Then we have successfully applied it in our E-Auction scheme.

In this thesis, we developed an Elliptic Curve Discrete Logarithm Problem (ECDLP) based blind signature scheme which can be implemented on our E-Auction protocol. Both the schemes are proved to be resistant to active attacks and satisfies the requirements which are necessary for online auction.

***Keywords*:** Cryptography, E-Auction, Blind Signature, Elliptic Curve Cryptography

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this chapter we have discussed about the fundamental ideas and terms related to cryptography which are necessary for completion of the dissertation. We have also define briefly digital signature and its services and subsequently describe blind signature which is a variation of digital signature and its properties. Further we have elaborated the necessity and properties of E-Auction and finally the layout of the thesis is given.

1.1 Introduction to Cryptography

We are living in an electronic world where information plays a crucial role. We need data in our day to day activities. Data are like an inevitable need of our life these days. At the same time its security is of great concern. In this electronic era data need to be protected from third parties with whom we may not want to disclose our information. In early days people used to write a message and cover the message itself with something in order to protect the message from any adversary. This technology is known as steganography. Then people adopt a more relevant and secure technology called cryptography.

Cryptography is the technology to transform a message to an unintelligible one in order to make it secure and immune to attacks by any adversary. During communication it pays high attention on the transmission of the message and should

be reluctant to any kind of attack by the adversaries. Mathematical theory and computer science practice are the heart of modern cryptography; cryptographic algorithms are based on computational hardness, making such algorithms infeasible for any adversary to break in practice. Theoretically it is possible to break such a system but it is infeasible to do so by any known practical means. There are so many computationally hard algorithms which seem to be unbreakable like integer factorization, discrete logarithm problem. But with time, technology is getting advance and many techniques are vulnerable to attacks. Hence researchers are constantly trying to develop new algorithms like Elliptic Curve discrete logarithm, Hyper Elliptic Curve, Quantum Theories etc..

While communicating a message we deal with three main aspects of security, first Confidentiality i.e hiding the content of the message from an unauthorized person, second Integrity i.e the content of the message should not be modified by an unauthorized person and third Availability i.e the message should be available to the authorized person when desired. There are two parties involve in a typical message transmission, the sender and the receiver(s). The sender encrypt the plain text message to get a cipher text message and send the same over a communication channel. Then the receiver decrypt the cipher text message to get back the plain text message. Any eavesdropper unable to decrypt the message if the encryption algorithm is strong enough. There are broadly two types of cryptographic technique exist. .

Symmetric key/Private key cryptosystem, where the sender and the receiver(s) share the same key and is hidden to others. The examples of such system includes Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish etc. These systems are usually faster. Here the major problem is the key distribution and key agreement when everyone wants to communicate with each other. Suppose there are n members in a group who wants to communicate with each other. Then they will need $n(n-1)/2$ numbers of keys. Moreover both the parties need to

pre agree on the secret key prior to the communication. It seems inefficient with regard to key distribution and key agreement and to avoid these drawbacks Diffie and Hellman [7] proposed a scheme where both the sender and the receiver can agree on a secret key without prior communication and that led to another kind of cryptosystem called Asymmetric key/ Public key cryptosystem.

In Asymmetric key/Public key cryptosystem, every sender and receiver require a set of two keys, a private key and a public key. The sender encrypt the plain text message using the public key of the receiver and the receiver decrypt the cipher text message using his private key which is known only to him. An eavesdropper can't decrypt the cipher text message because he doesn't have the private key of the receiver. The examples of such system includes RSA, Rabin cryptosystem, ElGamal, Elliptic curve, Hyper Elliptic curve cryptosystem etc. The major drawback associated with these systems is the computational cost and hence they are usually slower as compared to Symmetric key system. One of the basic security services, confidentiality in public key system is achieved through encryption/decryption algorithm which is known as encipherment whereas integrity, authenticity and nonrepudiation is achieved through another mechanism called Digital Signature.

1.2 Digital Signature

A conventional signature is requirement of proof to the recipient that the document is originated from a valid entity. A digital signature is the counter part of the conventional signature where some mathematical function is used to calculate the signature from the desired message and can be verified by the verifiers. A digital signature requires a public key system where the signer signs the message with his private key and the verifiers verify it using the signer's public key [8]. Digital Signature is one of the security mechanisms that satisfies the following security services.

- **Authenticity:** The authenticity of the message or data origin authentication

can be achieved by digital signature as the message signed using A's private key can only be verified using A's public key.

- **Integrity:** The integrity of the message can be preserved if we sign a document because if we modify the message the signature will also be changed and will not be the same during verification.

- **Nonrepudiation:** Though directly we can't achieve nonrepudiation through digital signature, but with a trusted third party nonrepudiation can be achievable.

Some well-known digital signature primitives are RSA digital signature scheme, ElGamal digital signature scheme, Schnorr digital signature scheme, Digital Signature Standard, Elliptic Curve digital signature scheme [9]. We can achieve additional security services by applying additional functionalities to digital signature. Confidentiality is not provided by digital signature. It can be provided by applying another layer of encryption/decryption. Similarly in real life situations we don't want to reveal the content of the message to the signer in order to maintain the confidentiality of the message. In such cases a Blind signature serves the purpose.

1.3 Blind Signature

Blind signature is a variation to the digital signature where the signer is unaware of the content of the message to be signed by him. In order to protect the confidentiality of the message,

- The sender uses a blinding factor to blind the message and send it to the signer to get the signature.

- Signer puts his signature on the blinded message and returns the blinded message signature pair.

- Sender unblinds the blind signature to get a valid signature on the original message which can be publicly verified.

David Chaum [10] introduced blind signature for the purpose to provide anonymity to the spender in an electronic cash system. A blind signature prevents the signer from observing the message signed by him. So it will be impossible for the signer to associate the signature and the original message even later. Blind signature is essential where privacy is of great concern for example Electronic Cash, Electronic Voting, Electronic Auction etc. Blind signature scheme can be used to achieve the unlink-ability property which prevents the signer to link to a previously signed blind message to a corresponding un-blind message. The general public key algorithms those are used for digital signature can be used for blind signature with some modification in order to achieve desired functionality.

1.4 Level of Security in Cryptography

In public key cryptosystem encipherment mechanism is used to provide confidentiality where as Digital signature is used to provide authenticity, integrity and nonrepudiation in general. Any cryptographic algorithm can be computed in terms of security bits and that depends on the level of security. The level of security is broadly divided in to the following three categories.

- **Integer Factorization Problem:** Given only a Composite number n, which is the product of two large prime numbers p and q then it will be difficult to factorize n. Eg. RSA, Rabin cryptosystem.

- **Discrete Logarithm Problem:** Given an integer x relatively prime to n and g is a primitive root of n, it is difficult to find y such that $x = g^y(\underline{m}odn)$. Eg. Diffie Hellman, ElGamal cryptosystem, DSA. .

- **Elliptic Curve Discrete Logarithm Problem:** Given a point $P = k.G$,

where G is the generator, it is difficult to find the scalar k. Eg. Elliptic Curve Cryptography.

1.5 Introduction to E-Auction

Advancement of science and technology has replaced most human procedures into electronic ones and E-Auction is one among them. E-auction is an important financial transaction to establish the price of commodities over a distributed environment. Typically in an electronic auction system there are three parties involved namely bidders, auctioneer and a third party who provides an environment to conduct the auction. The auctioneer provides all the detailed information about his goods, commodities or services to the third party which publishes it on the internet. Then bidders can submit their bid for the product which is advertised within a specified period. The auction is transparent, all interested parties are allowed to participate the auction in a timely manner [3–5].

Internet provides us a unique distributed environment where an auction can be performed. The wide use of Internet makes it possible to conduct online distributed auction instead of centralized auction. Centralized auction has several demerits like, physical limitation, geography, time, transparency and is difficult to reach to wide mass etc. To overcome these drawbacks E-auction scheme was introduced. But E-Auction has some challenges like Bidder's anonymity, bid privacy etc. In this thesis we have tried to give a solution that satisfies most properties of an E-Auction there by avoiding the typical problems associated with it.

There are two major forms of the electronic auctions.

Forward Auction: In this auction style several buyers bid for one seller's goods. In such kind of auction bidders compete to pursue the product by repetitively bidding over a bid value within a stipulated time period. The highest bid will be the final bid and the bidder will be determined as the winner.

Reverse Auction: In this auction style several sellers bid for one buyer's order.

In a reverse auction, a single buyer makes potential sellers aware of their intent to buy a specified good or service. During the course of the actual reverse auction event, the sellers bid against one another.

This thesis gives a generalized approach for conducting E-Auction and hence can be applicable to both auction styles. Moreover E-Auction schemes can be divided in to four basic types.

1. **English Auction:** It is also known as open outcry auction. In this type of auction bidders proffer successively until there is only one bidder left with the final bidding value. The highest bid is considered as final bid and has to be paid by the bidder in order to possess the item.

2. **Dutch Auction:** It is also known as open outcry descending auction. As the name suggests, it works in a reverse manner of English auction. Here auctioneer starts with a very high price and lowers the price subsequently. The bidder who calls out first will accept the current bid and pays the amount in order to possess the item.

3. **Sealed Bid Auction:** Here every bidder submits their single bid without the knowledge of other bidders' bid. The auctioneer declare the result after a stipulated time. The bidder with the highest bid can possess the item by paying his bid amount.

4. **Vickrey Auction:** It is similar to sealed bid auction except the bidder with the highest bid will win but pays the second highest bid. This scheme is named so after William Vickrey, an economist who won noble prize for his seminal, 1961 paper on auction theory.

According to the properties of Sealed bid auction it is always easy to implement it in an electronic auction. Open outcry auction scheme suffers either with communication cost or Security issues. In this thesis we have given a generalize

approach for all types of auction schemes, but it is more focused towards sealed bid auction.According to [1,2], there are different properties needed to satisfy to conduct online auction.

1. **Anonymity:** Each Bidder's information must be concealed. The identity of one bidder should not be traced down by any other bidder.

2. **Non repudiation:** Bidders must not be able to deny on their bids after the declaration of the result. No bidder can repudiate on their winning bid after result declaration.

3. **Unforgeability:** No one should be able to make a fake bidder id in order to participate in the auction and disturbs the auction proceeding.

4. **Traceability:** In special circumstances, it must be possible to identify the winning bidder only after the result declaration.

5. **Public Verifiability:** The identity of a valid bidder can be verifiable. The originality of the bidding message and accuracy of the tender must also be verifiable by any one.

6. **Integrity:** The tender or the bid message must not be modified during the auction process. No one should be able to modify the bid once submitted by the bidder including the bidder.

7. **Fairness:** The bidding values must not be disclosed to anyone. They must be kept private by the auction center. Every procedure involves in the auction must be fair and emphasis should be given on the privacy.

8. **Authentication:** The authenticity of a valid bidder must be identified and at the same time the authenticity of the auction center must be identified by the every bidder.

Electronic Auction expanded the range of commodities that can be sold or purchased in a much orderly manner irrespective of the geographical locations and physical limitations. As we will analyze later, in this thesis we have presented a generalize approach which satisfies all the above properties. It is always necessary for any online auction model to satisfy the properties mentioned above in order to implement it securely and efficiently. Here we have used a blind signature scheme to implement an E-Auction model.

1.6 Motivation

In this digital world with wide use of internet e-commerce has become an integral part of everyday life. E-Auction is one of them and more and more organizations are interested in this field due to its reduced cost, human effort and heavy popularity. As these systems are not restricted to physical limitations and geographical presence, they can be easily conducted over anytime and anywhere. The efficiency of evaluation along with the fairness can be greatly enhanced through E-Auction systems. Any unfair competition and manipulation of results can be restricted and through information regarding the auction proceeding can be published in order to keep the process transparent.

With these features, the challenge to develop a secure bidding system motivated us while keeping all the restrictions in mind that must be imposed on such a system. Researchers are constantly working in this field to develop an electronic bidding system that satisfies most properties to make it more secure. It is very hard to satisfy all the property for an electronic bidding system. Moreover the efficiency of these systems play a vital role in real life. Hence an elliptic curve implementation will be of great use. There are other schemes which rely on discrete log problem but they are computationally more costly as compared to elliptic curve. Hence in this dissertation work we have presented a cryptographic protocol to build an online bidding system which satisfies most properties of an e-auction system and

implemented through a blind signature scheme based on elliptic curve discrete log problem.

The blind signature itself satisfies some properties like anonymity, which are necessary for an online bidding system. We have shown how complete anonymity can be achieved without any repudiation and thus providing an efficient solution to develop a protocol to build electronic auction system which is the sole purpose of this thesis.

1.7 Objective and Statement of Purpose

As indicated in the previous section, the objective here is to build an online bidding system which is secure and must be efficient. For efficiency we have adopted an elliptic curve blind signature approach instead of a discrete log based blind signature. Hence from it we can deduce the problem statement as
"To propose an electronic auction system Using blind signature protocol with controlled traceability."

1.8 Layout of The Thesis

In this thesis, first we have proposed a simple and efficient blind signature protocol using elliptic curve discrete logariyhm problem and then implemented it to develope an electronic auction scheme. We have analyzed the security of our schemes and then provided the computational cost of those protocols. We have performed a comparative analysis of our schemes with existing schemes and shown the results. The thesis is organized as follows:

In chapter 2 we will describe the mathematical concepts related to our work and illustrate the elliptic curve cryptography, its application and benefits.

In chapter 3 we will present the literature review based on electronic auction and its requirements. Apart from that we will also review blind signature schemes and

its properties.

In chapter 4 we will propose an efficient algorithm for blind signature using elliptic curve cryptography and also develop a new secure electronic auction protocol using that blind signature.We will analyze security issues related to it and campare the result with other schemes.

In the end chapter 5 concludes our dissertation.

Chapter 2

Introduction to Elliptic Curve Cryptography

In this chapter we have describe some of the basic mathematical concepts related to the dissertation. The elliptic curve crypto system is discussed in detail and the elliptic curve discrete logarithm problem is studied along with its security hardness. Different parameters for elliptic curve digital signature is analyzed and finally a comparative analysis of the key size required for different algorithms is tabulated.

2.1 Mathematics Behind Cryptography

There are several public key cryptosystems that have been proposed and researchers are still studying on some with great detail. Elliptic curve cryptosystem is one of them and has gained a lot of attentions for the benefits it has promised over other cryptosystems.Every cryptosystem depends on the computational intractability of certain mathematical problems and with technological advancement over the time many systems either have been broken or the key size has been increased. With increased key size those systems do not work efficiently in a conventional machine. There are three types of systems which are considered to be safe, secure and efficient as mentioned in the previous chapter and are Integer factorization problem (IFP), Discrete Logarithm Problem (DLP) and Elliptic Curve Discrete Logarithm Problem (ECDLP). The advantages of using an ECC based cryptosystem is the smaller key

size, reduced storage and transmission requirement [11] (a 160 bit ECC public key should provide comparable security strength to a 1024 bit RSA public key).

2.2 Basic Facts About ECC

Elliptic curve cryptography was first proposed by Neal Koblitz and Victor Miller independently in the year 1985. It is based on the intractability of solving the elliptic curve discrete logarithm problem in the underlying field.

2.2.1 Finite Field

A finite field consists of a finite set of elements F, together with two binary operations, addition and multiplication on F, that satisfy certain arithmetic properties. The number of elements in the finite field is called the order of the field. There exists a finite field of order q, if and only if q is a prime power. Such a finite field is represented as F_q. If $q = p^m$, then p is called the characteristic and m is called the extension degree F_q. Usually either $q = p$, where p is an odd prime or $q = 2^m$, where m is any positive integer. If $q = p$, the finite field is called a prime field and if $q = 2^m$, it is called a binary field.

2.2.2 Elliptic Curve over Finite Fields

An elliptic curve is a cubic equation in two variables which can be defined over a finite field F_p (prime field where p is an odd prime) or F_{2^m} (binary field with only two values, 0 & 1). In this section we have discussed only about elliptic curves over prime fields. If $E(F_p)$ is an elliptic curve over finite field, then $\#\ E(F_p)$ is the number of points on the elliptic curve and is called the order of the elliptic curve. The elliptic curve consists of a discrete set of points which satisfy the following equation over a finite field F_p,

$$y^2 = (x^3 + ax + b) \underline{\mathrm{m}} odp \tag{2.1}$$

where a, $b \in F_p$ and $4a^3 + 27b^2 \neq 0(\underline{m}odp)$. For cryptography the elliptic curve should be a nonsingular curve i.e the above equation should hold good such that $4a^3 + 27b^2 \neq 0(\underline{m}odp)$ and has three distinct roots(real or complex). An elliptic curve also has a special point which is called point at the infinity and is denoted as O.

2.2.3 Operations on Elliptic curve

The specific properties of a nonsingular curve allow us to define an addition operation on two points of the elliptic curve $E(F_p)$ to give a third elliptic curve point. This is possible because of a rule called chord and tangent rule. With this point addition operation, it forms a group with all the points on the elliptic curve $E(F_p)$ along with the point at infinity O, which serves as its identity. The addition operation can be best explained geometrically.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two different points on an elliptic curve and $R = (x_3, y_3)$ is the sum of P and Q. R can be defined by drawing a line through P and Q which will intersect the curve in a third point. By taking the reflection of that point on the x-axis, we will get the desired point R which is the sum of P and Q. It is depicted in Figure 2.1.

Let $P = (x_1, y_1)$ is a point on the elliptic curve and $R = (x_3, y_3)$ is the double of P. The point double operation can be best explained geometrically by drawing a tangent to the point P which will intersect at another point on the curve. Taking the reflection of that point on the x- axis, we will get the desired point R which is the double of P. It is depicted in Figure 2.2.

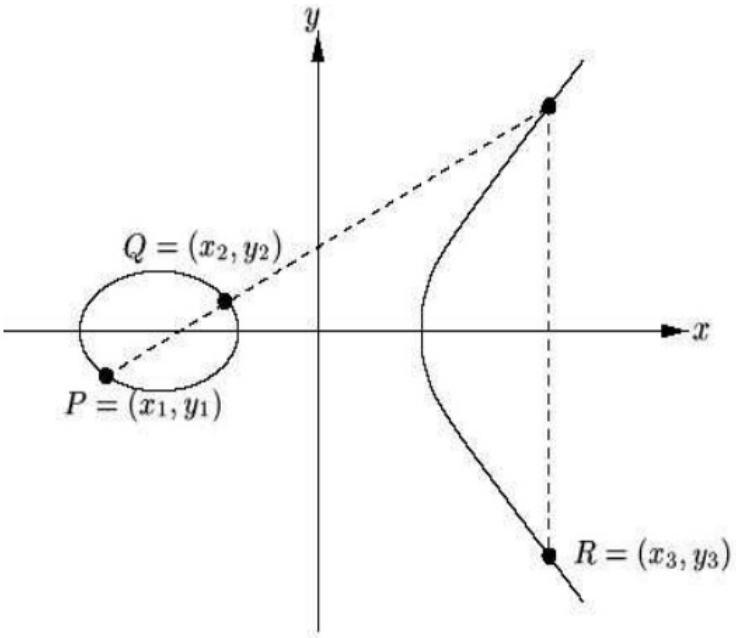

Figure 2.1: Addition of two points P and Q: R=P+Q

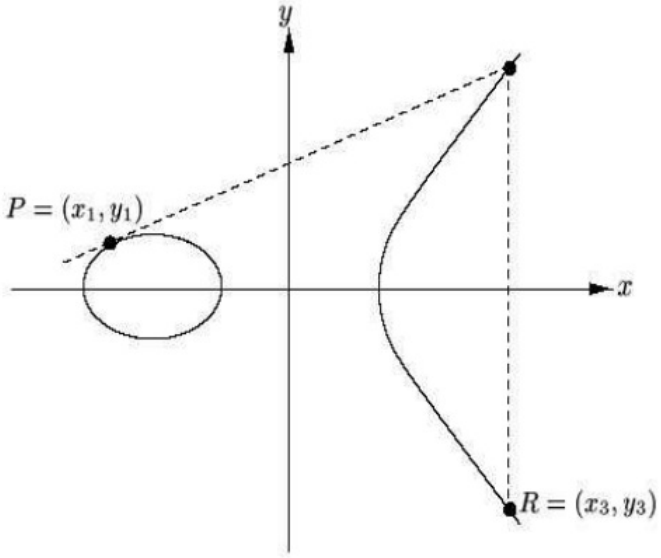

Figure 2.2: Doubling a point P: R=P+P=2P

The algebraic formula for point addition and point double can be derived from the above geometrical description.

- $P + O = O + P = P$ for all P $\in E(F_p)$
- If $P = (x, y) \in E(F_p)$, then $-P = (x, -y)$ where $-P$ is called the negation of P such that $P + (-P) = (x, y) + (x, -y) = O$.
- (Point Addition) If $P = (x_1, y_1) \in E(F_p)$ and $Q = (x_2, y_2) \in E(F_p)$, where $P \neq \pm Q$. Then $P + Q = (x_3, y_3) \in E(F_p)$, where

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

and

$$y_3 = \lambda \cdot (x_1 - x_3) - y_1 \tag{2.3}$$

where

$$\lambda = (y_2 - y_1)/(x_2 - x_1) \tag{2.4}$$

- (Point Doubling) $P = (x_1, y_1) \in E(F_p)$, where $P \neq (-P)$. Then $2 \cdot P = (x_3, y_3) \in E(F_p)$, where

$$x_3 = \lambda^2 - 2x_1 \tag{2.5}$$

and

$$y_3 = \lambda \cdot (x_1 - x_3) - y_1 \tag{2.6}$$

where

$$\lambda = \left(\frac{3{x_1}^2 + a}{2y_1}\right) \tag{2.7}$$

The point addition and point doubling operation require few arithmetic operations like addition, subtraction, multiplication, division in the underlying field F_p. Scalar multiplication in ECC is the repetition of the point addition operation by a scalar number of times over the finite field F_p,

$$kP = P + P + ...P(ktimes) \tag{2.8}$$

2.3 Why ECC?

Elliptic curve cryptography has become the lure among the research community and security firm because of its immense advantage and safety. While discrete logarithm problem can be solved using sub exponential time running algorithm (Number Field Sieve, pollard's rho method), an elliptic curve discrete log problem is resistant to any such attack. Moreover a public key cryptosystem which is based on integer factorization or DLP requires higher size of keys as compared to the ECDLP based system with the same level of security. This makes elliptic curve cryptosystem more efficient than any other public key primitives. Due to the smaller size key, ECC can be applied in smart cards and wireless communication systems, where the devices have less memory, bandwidth, and computational power.

Table 2.1: Comparable key sizes (in bits) [30]

Strength	ECDLP	DLP/IFP
80	160	1024
112	224	2048
128	256	3072

Elliptic curve can be very helpful in resource constrained environment like smart card, wireless communication which are constrained to memory, bandwidth, computation power etc. because of its smaller key size.

2.4 summary

This chapter provides an overall mathematical concepts required for our research work to successfully complete the dissertation. We have described elliptic curve cryptography and its benefits.

Table 2.2: Recommended minimum key sizes (in bits) [30]

Year	Strength	ECDLP	DLP/IFP	Keysize ratio
upto 2010	80	160	1024	1:6
2011-2030	112	224	2048	1:12
2030+	128	256	3072	1:20

Chapter 3

Literature Survey

In this chapter we have studied and discussed various existing E-Auction protocols and their processes. The drawbacks of several schemes have been analyzed and briefly depicted. We have also find out the use of blind signature in E-Auction scheme and its merits and demerits.

3.1 Literature Review

An auction can be divided in to four basic types, English auction, Dutch auction, Sealed bid Auction and Vickrey auction. In English auction all the bids are opened and every bidder must bid a higher amount than the previous bidding amount. The one with the highest is the winner. Dutch auction is the reverse of the English auction where all the subsequent bid must be lower than the previous bid amount. The one with the lowest is the winner. In sealed bid auction all the bids are hidden until the auction is over. In the opening phase the bids are disclosed and the winner is decided. Vickrey auction is similar to sealed bid auction but here the bidder with the highest bid will win and will pay the second highest bid amount. Most E-Auction protocols are implemented through Sealed bid auction scheme because of the convenience. Several E-Auction protocols have been designed so far but its security is still a challenge. The growing demand as well as the tradeoff between security and efficiency always boost researchers to constantly work on this field. Its

always been very difficult to satisfy all the required properties of an online auction scheme, still researchers have extensively studied this area and proposed several different protocols.

Franklin and Reiter proposed a sealed-bid auction protocol [12] where a malicious bidder cant deny on his bid. They have used a verifiable signature scheme to justify their protocol. In [13], Kudo proposed a sealed-bid auction method with a time server where after a certain time period the sealed bids are opened and evaluated. In [14], Kikuchi, Hakavy and Tygar proposed an electronic auction scheme to improve the privacy of bids such that the winner will be determined and known only by the auctioneer. Chang C. C. and Chang Y. F. [15] proposed three anonymous auction protocols to ensure bidders privacy. Here they have used a deniable authentication scheme to check the validity of the bids where every bidder can bid arbitrarily and anonymously. However, Jiang et al. [16] pointed out some security weakness in Chang C. C. and Chang Y. F. scheme where bidder cannot detect the tampered response message from the auctioneer. Hence Jiang et al. proposed an improved scheme which prevents tampering attacks. Subsequently, Chang C. C. and Chang Y. F. also provided an improved method for further enhancement [17].

In [18], Liaw et al. proposed an electronic online auction protocol to solve the problem of the bidders deposit payment with a deposit deducting certificate. In their scheme four parties were involved (Bidder, third party, Auctioneer and Bank). However Chia-Chi Wu et al. [19]found some security drawbacks where the bidding receipt can be forged by the bidder to claim that he is the valid auction winner. Moreover it was unable to preserve the privacy of the bidders. Bidders information leaked to other parties involved in the auction which doesnt preserve the anonymity property. Even malicious bidders can forge the bid receipt sent by the third party and can claim that he is a valid winner.

Therefore Wu et al. [19] designed an electronic auction protocol that improvises Liaw et al. [18] scheme and was comparatively more secure and efficient. They have

used symmetric key encryption instead of asymmetric key encryption to enhance the efficiency. But the security of their scheme totally rely on the trust of the third party as it has all the information about the bidders which may affect in the subsequent auction. Much more emphasis has been given to the third party instead of sharing the load. A bidder has to register every time he need to bid which may be an overhead to both the bidder and the auctioneer. Moreover all the bidding price and the sequence numbers are published on the web which leaked the private information about losing bidders. If the third party is corrupted he may provide all the information about a bidder either to a dishonest auctioneer or bidder. Furthermore their security relies on the difficulty of solving the discrete logarithm problem for the sealed bid. There exist some sub exponential running time algorithm to solve discrete log problem. Therefore we have given an approach to implement an electronic online auction using elliptic curve discrete logarithm problem. We have further used a blind signature scheme which is nothing but only a variation of digital signature to design an E-Auction protocol.

As we have already mentioned, in order to effectively design a secure and efficient online electronic auction protocol it has certain properties which need to be satisfied. The following are some of the requirements which must be fulfilled [15, 18, 19].

- **Anonymity:** The real identity of the bidder shouldnt be disclosed. The main objective of anonymity is to hide the bidder-bid relationship in order protect bidders personal information.

- **Un-forgeability:** The bidders, auctioneer or the auction host must not be able to forge the bid otherwise they can be impersonated.

- **Non-Repudiation:** None of the parties be able to deny on their action. The winning bidder must not be able to deny after submitting the bid. Similarly the auction host must not be able to deny an honest bidders bid receipt.

- **Public Verifiability:** There must be some mechanism through which all the

parties can be publicly verified which includes evidence of registration, bidding and winning bid.

- **Traceability:** The winning bidder must be identifiable after the auction. It is necessary because in some situation bidder might not pay the winning bid amount after winning the auction.
- **Robustness:** The auction proceeding must not be interrupted by corrupt bidders which may alter the auction result.
- **Fairness:** The auction process need to be fair enough so that no malicious bidder can collude with the auction host or the auctioneer to affect the honest bidders.
- **Privacy:** The bidders information must not be leaked in order to preserve the privacy of the losing bidder. Moreover the bank account number and other financial details should not be known to the auctioneer.
- **Confidentiality and Integrity:** In some auction (sealed bid, Vickrey) the bid amount must be confidential until the bidding phase is over. The bid message must not be modified during the transmission.
- **One Time Registration:** Every bidder can register only once and bid in all subsequent auction without re-registering.

3.2 Blind Signature

Blind signature is nothing but a variation of the digital signature where the signer is unaware of the content of the message. Furthermore anyone can verify the signature on the message after unblinding it. David Chaum [10] introduced blind signature to resolve the issue. According to Chaum, a sender can get a valid signature from a signer without disclosing the content to the signer who signs the document. The

signature can be publicly verified without knowing the secret of either party. The process is illustrated below.

- Let B is a blinding function on message m, and B' is the inverse blinding function known only to the sender such that $B(m)$ is a blind message sent to the signer.
- Let S is a signing function known only to the signer who puts his sign on the blind message $B(m)$ and S' is the inverse signing function which is publicly known. $S(B(m))$ is the signature on the blind message and sent back to sender.
- Sender unblinds the blind message using his secret function B' and got the valid signature on the message as $B'(S(B(m))) = S(m)$.
- The signed message can be verified by anyone by applying the public key of the signer as $S'(S(m)) = m$.

The following figure depict the general procedure of a blind signature protocol.

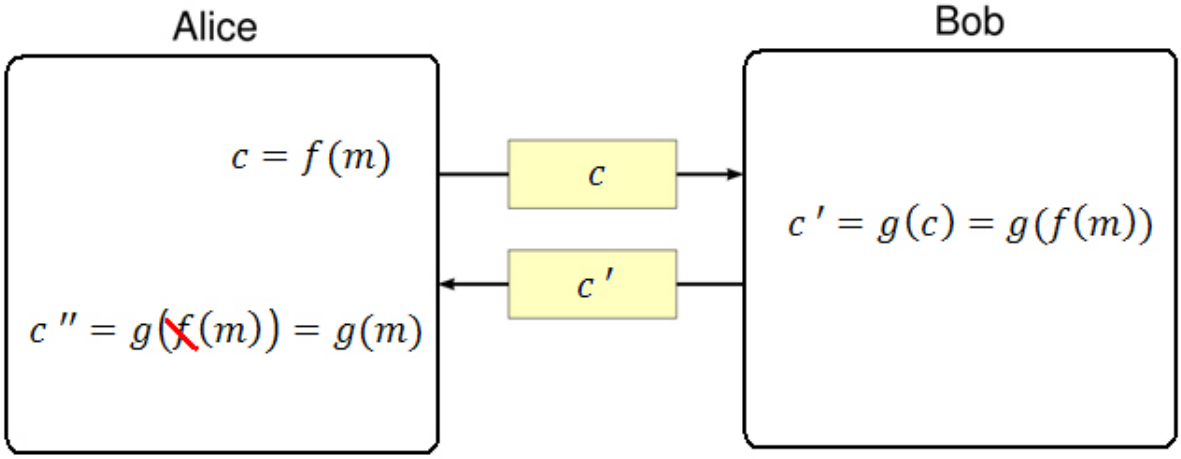

Figure 3.1: Mechanism of Blind Signature

A blind signature has the following properties [20–22] which need to be satisfied and for this reason we can use it in designing an E-Auction protocol.

- **Blindness:** The signer should be unaware of the content of the message while signing.
- **Correctness:** The signers public key must be used to verify the blind signature.
- **Authentication:** A valid signature implies that the message has been originated from a valid source.
- **Integrity:** No one should be able to modify the content of the message during the transmission, otherwise it will not generate a valid signature.
- **Non-Repudiation:** The signer cant deny after signing a document if it generates a valid signature.
- **Un-forgeability:** A valid signer can only generate a valid signature. None other than the signer can generate a valid signature.
- **Non-Reusability:** Once a signature has been used to sign a document, it cant be used to sign another message.
- **Untraceability:** After publishing the message-true signature pair, even the signer will not be able to link to a message-blind signature pair.

According to the above properties, we can use a blind signature protocol to design an E-Auction scheme but with some modification. Usually blind signature are designed to be untraceable and finds many application like E-Voting, E-Cash etc. But an E-Auction scheme requires controlled traceability. We must be able to trace the bidder when he doesnt pay after winning the auction. Again the auctioneer must not be able to trace the bidder and his bid amount (message) when the auction closes. For this reason a modified blind signature protocol has been proposed and is applied in the auction protocol.

In 1994 Carmenish proposed a blind signature scheme which was based on discrete logarithm problem [23]. But in 1995 Harn [24] find out that the previous scheme doesnt satisfies the untraceability property. The signer could trace the blind signature by using all the public parameters used in particular transaction and the message-signature pair open to the public. Hoster [25] disagreed with Harn and claim that the cryptanalysis of Carmenish made by Harn is incorrect because the signer will find two pair of signature when he will try to trace it. Later Lee et al. [26] claimed that Hosters cryptanalysis is wrong and it could be possible to trace the blind signature by the signer as he can keep all the parameters after signing the blind message. In 2005 he proposed a modified scheme to overcome the lacunas of the base paper.

These days elliptic curve cryptography has been widely popular due to its added advantages as mentioned in the previous chapter. The first blind signature scheme on elliptic curve was proposed in 2003 which was based on Schnorr blind signature scheme [27] and they have shown that the space requirement have been reduced drastically in their scheme. They have demonstrated that in their proposed scheme only 34% space was needed and total execution time was 6 times faster than the previously proposed discrete log (DLP) based blind signature protocol. It is also believed that elliptic curve discrete log problem (ECDLP) is harder to solve as compared to integer factorization and discrete logarithm problem (DLP). Moreover elliptic curve method provides almost same level of security as that of its counterpart but with much less key size. As mentioned in the previous chapter 3072 bits RSA key is required for a level of security which 256 bit ECC key can achieve.

An efficient identity based blind signature scheme without bilinear pairing was proposed by He et al. [28] in 2011. They used elliptic curve to design their protocol in order to save the size of the signature and the running time. Their scheme was proved to be secure in random oracle under the ECDLP.

In 2013 Nayak et al. proposed an untraceable blind signature scheme [29] and shown that his scheme is computationally more efficient than He et al scheme [28]. The author proved that it was untraceable and even the signer can't trace the message-signature pair after declaring the parameters for verification. As we have seen for electronic auction traceability is one of the requirements. Hence in the next chapter we have proposed another blind signature with controlled traceability to facilitate electronic auction.

3.3 Summary

In this chapter we have studied and analyzed the literature related to blind signature and E-Auction. Further we have described the blind signature, its properties and how it can be applied to design an E-Auction protocol. We have also depicted electronic auction and its requirements. In the next chapter we will propose a new E-Auction protocol using blind signature based on ECDLP.

Chapter 4

Proposed Work

In this chapter we have proposed a secure and efficient E-Auction protocol using blind signature based on elliptic curve cryptography. There are many schemes on electronic auction which uses encryption method or digital signature based on discrete logarithm problem. But in order to save the size and running time with same level of security we have adopted an elliptic curve method to design an electronic auction protocol using blind signature. Blind signature has inherent properties which satisfy the requirements of E-Auction protocol. With a modified blind signature scheme we can achieve most requirements of an electronic auction. Hence first we have proposed a blind signature scheme and then applied it to develop an E-Auction protocol. Furthermore we have analyzed the security strength of our protocol and the computational complexity of our scheme in the subsequent sections.

4.1 Proposed Blind Signature Protocol

We have modified Nayak et al. [30] scheme in order to make it traceable. In our scheme there are two participants, signer and the requester(sender) who agree on an Elliptic curve $E_p(a, b)$ of order p. In our scheme there are 4 stages viz. Key Generation, Blinding, Signing, Unblinding-Verification as depicted in figure. The operations on each phase are described below. G : Base Point, such that $nG = O$
n : number of points on $E_p(a, b)$

O : Point at infinity

x, r : Random no. chosen by signer

a, b : Random no. chosen by sender

m : Message

SHA-1 : Hash Function

4.1.1 Key Generation

1. The signer generates two random number x and r in Z_p^*.

2. Calculate the following

$$Y = xG \tag{4.1}$$

$$H = rG \tag{4.2}$$

and

$$T = (H + Y) \tag{4.3}$$

Signer publishes his public parameters Y,H,T and keeps x and r private.

4.1.2 Blinding

1. Sender generates two random no. a and b in Z_p^*, where a is called the blinding factor.

2. Calculate

$$Q = bT \tag{4.4}$$

$$u_1 = SHA - 1(m) \tag{4.5}$$

$$u_2 = (u_1 - b) \cdot a^{-1} \tag{4.6}$$

$$K = bG \tag{4.7}$$

3. Sender sends u_2, the blind message to Signer.

4.1.3 Signing

1. After receiving u_2, Signer put his signature on it thereby calculating $z = (r + x) \cdot u_2$, z is the signature on the blind message.

2. Send back z to Sender.

4.1.4 Unblinding and Verification

1. After receiving z, Sender unblinds the message as,

$$Z' = (za + b)G \tag{4.8}$$

2. Sender publishes his public parameters Q and K and keeps a and b as private.

3. The blind signature for message m is (Z', Q, K, T, m) which can be verified as

$$Z' + Q - K = u_1 \cdot T \tag{4.9}$$

The mechanism is described in figure 4.1.

4.2 Analysis of the scheme

The security of the proposed scheme relied on the strength of the hash function and difficulty of solving ECDLP. We have considered a hash function to be collision resistant so that it will be difficult to find another message m' for the original message m , such that $SHA-1(m) = SHA-1(m')$. Our proposed scheme satisfies

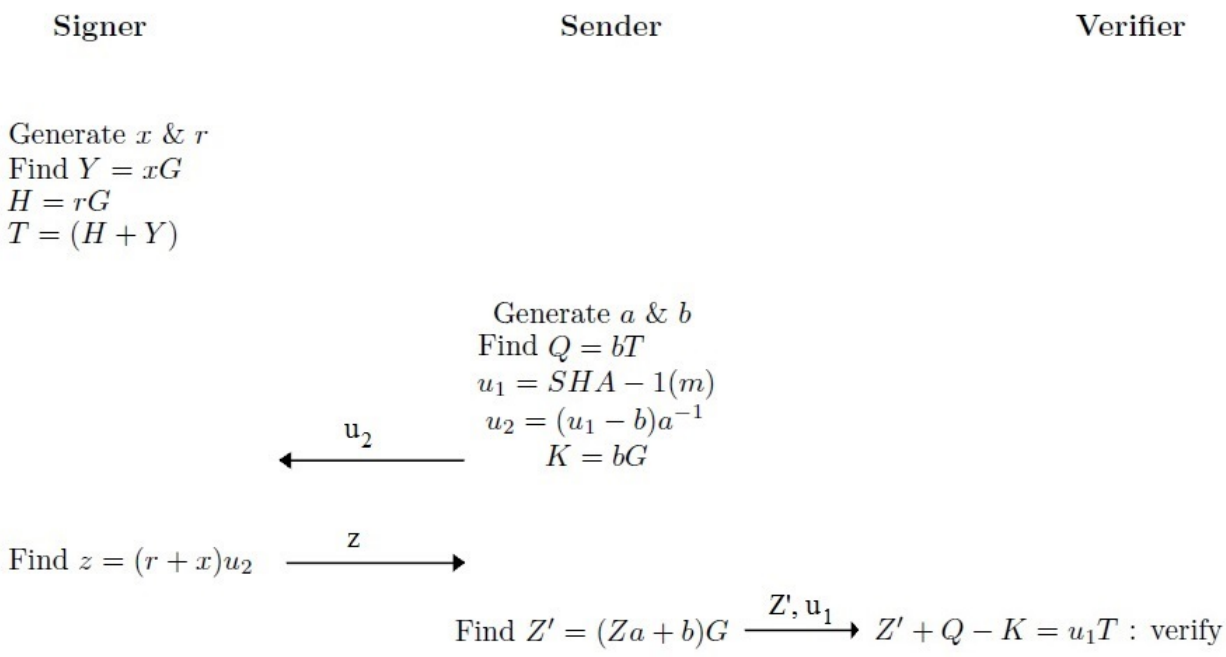

Figure 4.1: Blind Signature Protocol

the correctness, blindness and traceability property which we have proved in the subsequent sections. We have analyzed the computation cost of our proposed scheme and compare it with He et al. [28] and Nayak et al. [30].

4.2.1 Correctness

If the following equality holds then the signature is considered to be valid.
$Z' + Q - K = u_1T$

Correctness Proof

$$\begin{aligned} & Z' + Q - K \\ &= (za + b)G + Q - K \\ &= zaG + bG + Q - K \\ &= zaG + Q + K - K \end{aligned}$$

$$
\begin{aligned}
&= zaG + Q \\
&= (r + x)u_2aG + Q \\
&= (rG + xG)(u_1 - b)a^{-1}a + Q \\
&= (H + Y)(u_1 - b) + Q \\
&= (u_1 - b)T + Q \\
&= u_1T - bT + Q \\
&= u_1T - Q + Q \\
&= u_1T
\end{aligned}
$$

4.2.2 Blindness

The proposed scheme satisfies the blindness property as the value of a and b are known only to the sender and finding the value of b given T and Q depends on the difficulty of ECDLP. Even after publishing the value of u_1, one can't reveal the value of b or a. If someone got two message signature pair, (Z', u_1, Q, K) and (Z'^*, u_1^*, Q^*, K^*) it won't be possible to determine the blinding factor a. Hence our scheme provides complete blindness.

4.2.3 Traceability

As we have already mentioned, we need a traceable blind signature protocol to apply it in an E-Auction scheme. That's why we modify Nayak et al. [30] blind signature scheme which was claimed to be untraceable. Our proposed scheme satisfies traceability property as mentioned below.

When a blinded message is sent to the signer for his signature, he can keep a record of the value (u_2, z). When the requester reveals (Z', u_1) for the message m, signer can't be able to calculate a or b. But from $Z' = (za + b)$, he can get $Z' - K = zaG$ because $K = bG$ and is revealed by requester. Say $aG = P$, then $Z' - K = zP$. Now signer has $(Z' - K)$ and z, so he can find z'^{-1}. P' can be found as $z'^{-1}(Z' - K)$. Then he compares for every P', if $Z' - K = z'P'$ and can find the z for message

m. Hence the signer can trace a blind signature with $O(n^2)$ where n is no of blind signature signed by the signer. It can be used to trace the requester when needed.

4.2.4 Universally Verifiable

The blind signature can be verified by using the Signature pair (Z', K) and publicly available parameters (Q, T) for message m. Anyone can check its authenticity once the sender reveals the signature pair (Z', K). Hence our scheme is universally verifiable.

Now we can move forward to develop an electronic auction protocol and then analyze the security of both the schemes together at the end of this chapter.

4.3 Proposed E-Auction Protocol

Now we will propose an E-Auction protocol using the above blind signature scheme. Moreover we have used elliptic curve method to reduce the storage requirement and computation speed with similar level of security. ECDLP is considered to be harder to solve than integer factorization and DLP based technique. In most E-Auction scheme anonymity is a major problem. In our protocol we have presented a better solution as compared to existing schemes. There are 5 stages in our scheme viz. Advertisement, Registration Setup, Registration Confirmation, Bidding, Result Declaration. All the steps in each stage is described below.

There are four parties involved in our electronic auction protocol. They are namely Registration Manager(RM), The Third Party(TP) which can be acted as the Signer, Bidders which can be viewed as the Sender and the Auctioneer which can be thought of as the verifier in correspondence with our proposed Blind Signature protocol. Let us now discuss each phase separately with proper diagram wherever required.

4.3.1 Advertisement Phase

The auction will begin with an advertisement by the auctioneer. The base point G over an elliptic curve is chosen. If s_u is the private key of the auctioneer and $p_u = s_u G$ is the public key then the auction message M is signed by auctioneer as $S_{s_u}(M)$ and send it to the Third Party to publish it on the web. It can be verified by using his public key p_u.

4.3.2 Registration Setup Phase

Every bidder need to register themselves before bidding. To maintain the anonymity of individual bidder, each bidder need to register themselves with a registration manager. They need to employ the following steps.

1. The Registration Manager(RM) generates his private keys t and x_n randomly. Then find

$$S = tG \tag{4.10}$$

and

$$Y_n = x_n G \tag{4.11}$$

He publishes S and Y_n which are his public keys.

2. Similarly Bidder generates his private keys a, b, c and x_s randomly in Z_p^*. Then calculates

$$Y_s = x_s G \tag{4.12}$$

and sends Y_s to the Registration Manager(RM).

3. The RM finds

$$K_1 = x_n Y_s \tag{4.13}$$

which is a secret key between RM and Bidder. RM sends back his public key Y_n to the bidder.

4. Bidder computes the same secret key K_1 as $K_1 = x_s Y_n$. Then he computes the following

$$R = c(S + G) \tag{4.14}$$

$$e = SHA - 1(Time||R) \tag{4.15}$$

$$e_1 = c^{-1}e \tag{4.16}$$

   Then encrypts $(Id, Time, e_1)$ using the secret key K_1 and sends it to the RM. As it is symmetric encryption, it will be fast.

5. After receiving the encrypted message, the RM will decrypt it using K_1^{-1} and computes s as follows

$$s = t - e_1 SHA - 1(Time)x_n \tag{4.17}$$

   Then signed s using x_n and send $signed_{xn}(s)$ to the bidder.

The information flow of the phase is depicted in figure 4.2.

4.3.3 Registration Confirmation Phase

1. The Third Party(TP) generates his private keys x and r randomly in Z_p^* and computes his public keys as follows

$$Y = xG \tag{4.18}$$

$$H = rG \tag{4.19}$$

$$T = (H + Y) \tag{4.20}$$

   and publishes his public parameters Y, H and T.

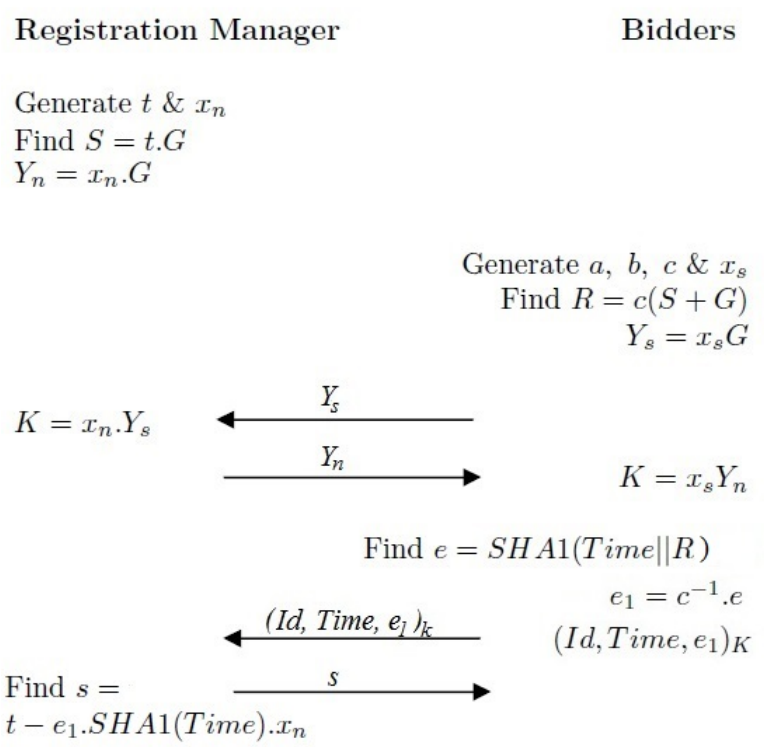

Figure 4.2: Registration Setup

2. After receiving s from the RM, bidder needs to decrypt it using K_1^{-1} and then calculates the signature s' as follows

$$s' = (s + 1)c - e.SHA - 1(Time).x_s \tag{4.21}$$

and sends $(s', e, Time)$ and Y_s to the Third Party(TP).

3. The TP verifies the signature s' as follows

$$e = SHA - 1(Time, s'G + e.SHA - 1(Time).(Y_s + Y_n)) \tag{4.22}$$

If the above equality holds true then the TP finds K_2 the secret key as

$$K_2 = xY_s \tag{4.23}$$

Then generates a pseudonym pn, encrypts (pn) using K_2,put his signature $Sign_x(s', e, Time)$ and sends back $(Y, (pn)_{K_2}, Sign_x(s', e, Time))$ to the bidder.

4. After receiving the message, bidder verifies the signature using Y, computes the secret key K_2 and decrypts the encrpyted message to retrieve pseudonym pn.

The steps involved in this phase has been depicted in figure 4.3.

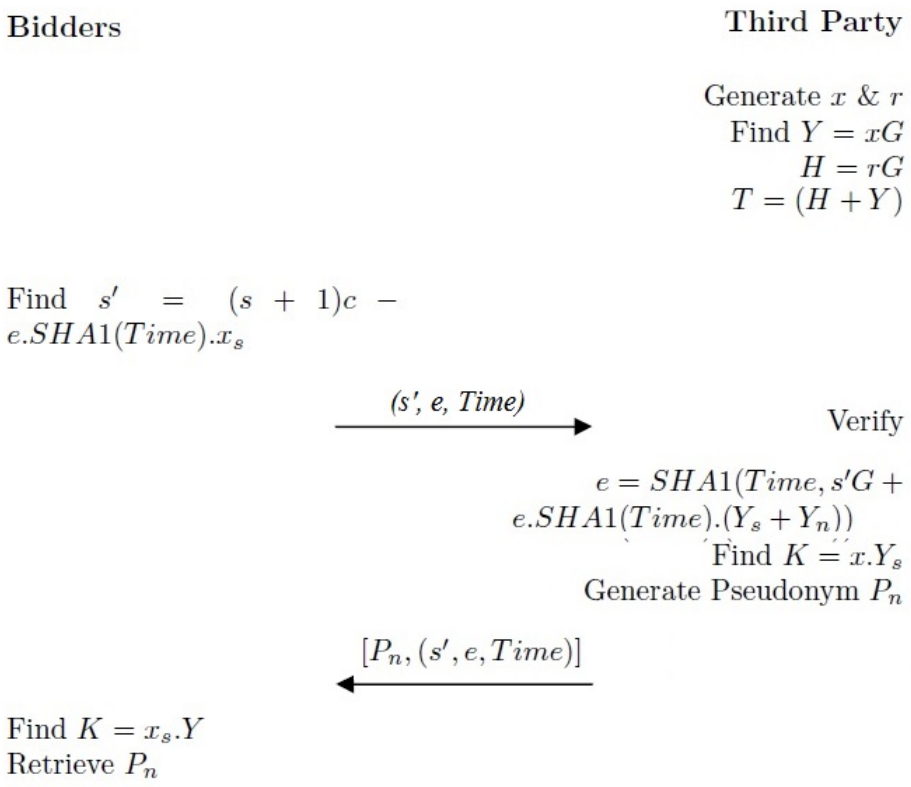

Figure 4.3: Registration Confirmation

4.3.4 Bidding Phase

1. Bidder computes his public key Q as

$$Q = bT \tag{4.24}$$

and publish it. Then he needs to blind his bid value. But before blinding he finds the $SHA-1$ of his *bid*, say u_1. Then blinds u_1 using the blinding factor

a and his private key b as follows.

$$u_2 = (u_1 - b).a^{-1} \tag{4.25}$$

Then finds $K = bG$ and sends the blind bid message u_2 to the Third Party to get his signature.

2. The Third Party calculate the signature on the blind message as

$$z = (r + x).u_2 \tag{4.26}$$

but doesn't know anything about the original bid value. Then he sends the blind signature z to the bidder.

3. Bidder unblinds the signature to get the original one. He computes as

$$Z' = (za + b)G \tag{4.27}$$

and publishes the signature (Z', u_1, K).

4. Anyone can verify the signature. If the following equality holds then the signature is indeed valid.

$$Z' + Q - K = u_1.T \tag{4.28}$$

Note that the bidder didn't reveal the *bid*, yet it can be verified.

The bidding process is illustrated in figure 4.4.

4.3.5 Winner Determination Phase

1. Every bidder send their encrypted *bid* message to the Third Party along with the signed message Z' and the pseudonym $Sign_x(pn)$ issued to them by the TP.

$$[Sign_x(pn), (bid, Z', Q, K)_{K_2}] \tag{4.29}$$

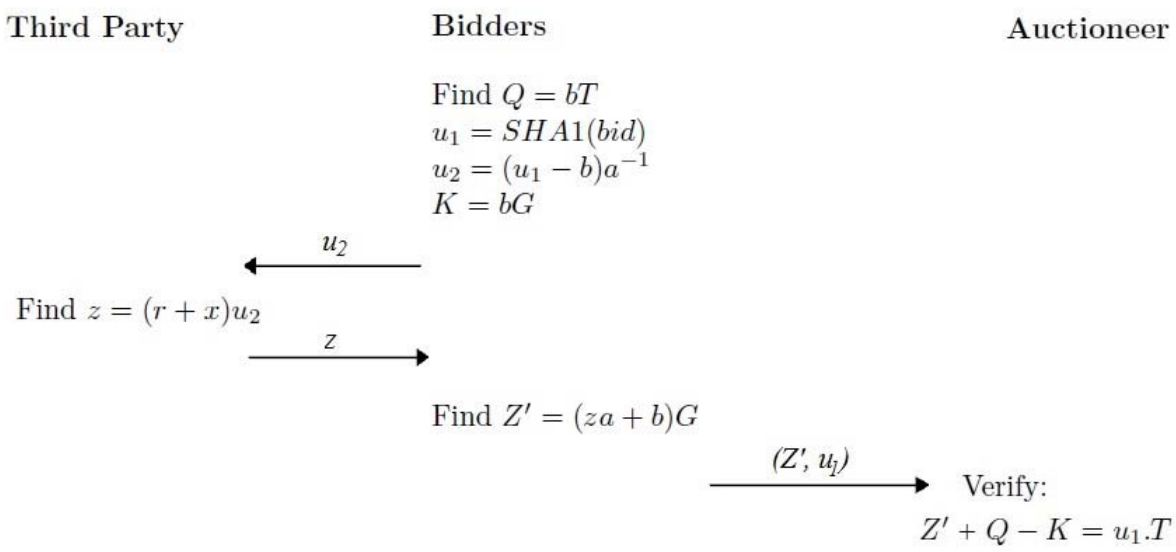

Figure 4.4: Bidding Phase

2. After receiving the message, the Third Party checks for $Sign_x(pn)$, then use the secret key K_2 related to the pseudonym to decrypt the message and retrieve the *bid* and Z'.

3. The Third party finds $SHA-1(bid) = u_1'$ and verify if $Z' + Q - K = u_1'T$. If satisfied then he accepts the bid and finds the max_bid. The TP sends $(max\_bid_{K_2}, Sign_x(pn))$ to the bidder and publishes the (max_bid, Z', Q, K) so that it can be verified by anyone.

4. Now the bidder can claim himself as the winner.

4.4 Analysis and Result

In this section we will analyze the security and efficiency of our protocol. We have also analyzed the requirement evaluation of our protocol. Then we have compare our protocol with other existing protocols.

4.4.1 Registration Correctness

We have already proved the correctness of the blind signature. Here we will prove the registration correctness of the bidder. In order to verify the authenticity of the bidder, anyone including the Third Party can verify the signature $(s', e, Time)$.
If

$$e = SHA-1(Time, s'G + e.SHA-1(Time)(Y_s + Y_n)) \tag{4.30}$$

then the signature is a valid one and he can be authenticated. The proof is shown below.

We know that

$$s = t - e_1.SHA-1(Time).x_n \tag{4.31}$$

and

$$s' = (s+1)c - e.SHA-1(Time).x_s \tag{4.32}$$

Putting the value of s in the above eqn.

$$\begin{aligned} s' &= (t - e_1.SHA-1(Time).x_n + 1)c - e.SHA-1(Time)x_s \\ &= (t+1)c - e.c^{-1}.c.SHA-1(Time).x_n - e.SHA-1(Time)x_s \\ &= (t+1)c - e.SHA-1(Time)(x_n + x_s) \end{aligned}$$

Again $Y_s = x_sG$ and $Y_n = x_nG$

Now

$$\begin{aligned} &s'G + e.SHA-1(Time)(Y_s + Y_n) \\ &= s'G + e.SHA-1(Time)(x_s + x_n)G \end{aligned}$$

Putting the value of s' in the above eqn. , we get

$$\begin{aligned} &= (t+1)c.G - e.SHA-1(Time)(x_n + x_s)G + e.SHA-1(Time)(x_s + x_n)G \\ &= (t+1)c.G \end{aligned}$$

Again

$$\begin{aligned} R &= c(S+G) \\ &= c(tG+G) \\ &= (t+1)c.G \end{aligned}$$

Hence

$$s'G + e.SHA-1(Time)(Y_s + Y_n) == R$$
$$SHA-1(Time, R) = e$$

4.4.2 Security Analysis

The security of our protocol depends on the strength of one directional hash function(SHA,MD) and the hardness of ECDLP. Then we will discuss some of the attacks which are withstand by our protocol. Our protocol can withstand some active attacks and are analyzed below.

- **Forgery Attack**

  Given Y and G finding x from $Y = xG$ is difficult due to the ECDLP. Hence the private component can never be calculated. Hence it will be difficult for the attacker to unblinds the message because of the private components a and b. So he can never found u_1. Moreover we have assumed our hash function is collision resistant. So from the *bid* message, it is easy to find the message digest u_1 but from u_1 it is difficult to find the *bid* message as the hash function is non-invertible. Moreover from the blind message an attacker needs to choose two values from a, b and u_1 randomly to find the other value which is infeasible. so given a valid signature (Z', u_1, K, bid), it is impossible to find another valid signature (Z'', u_1', K', m') which satisfies the verification condition.

- **Key Only Attack**

  In order to successfully lunch the key only attack, the attacker needs to get a valid signature. If he gets one then also he can not unblind the signature as he doesn't know the blinding factor and the private key of the requester i.e a and b. The difficulty of finding b depends on the ECDLP and finding the value of a depends on integer factorization which are considered to be hard problem in cryptography.

- **Known Message Attack**

  In known message attack, the attacker generates a valid signature for his own message m'. Here he has access to two or more message-signature triplet say (Z', u_1, m') and (Z'', u_1', m''). Here the attacker can generate another signature $Z_s = Z' + Z''$ for message m if he can find $h(m) = h(m') + h(m'')$ which is very difficult if the hash function is preimage resistant. Moreover he also needs to find the value of u_2 which required to find a and b. The problem now depends on solving ECDLP which is considered to be very hard.

- **Chosen Message Attack**

  In chosen message attack, the attacker can make the signer sign two message m' and m'' for him. Then he can calculate a new signature $Z_s = Z' + Z''$. If the attacker can find $h(m) = h(m') + h(m'')$ and the blind message u_2 for his message m then he can forge the message signature. But it is very difficult to find the hash value of a message m which is same as the hash value of the given messages m' and m''. The difficulty also depends on solving the ECDLP to get b in order to find the blind message u_2.

- **Eavesdropping Attack**

  If attacker wants to eavesdrop on the communication between any bidder and Registration Manager or Third Party for his benefits, it will not be an advantage for him as the data flow are encrypted with the Session keys K_1 and K_2 and signed by the respective entities. Due to confidentiality and authenticity, the attacker will not be benefited.

- **Replay Attack**

  An attacker cannot retrieve the *id* of any bidder as the message sent to the Registration Manager is encrypted with the session key K_1. He won't be able to find either e_1 or s. Similarly due to the session key K_2 between bidder and Third Party, he won't be able to find the pseudonym *pn*. So the attacker can't replay any of the message.

- **Impersonate Attack**

  It will not be possible to impersonate either the bidder or the registration manager or the Third Party because all have used either their session key to encrypt the message or the public key to sign the message. The session key is generated from the private component of both the parties involved in the communication. So it will be known only to them which prevent malicious persons to impersonate honest members involved in the auction.

- **Identity Theft Attack**

  In our proposed scheme we are not using bidder's *id* for authentication. Instead we are using the time stamp (Time) for authentication which prevents the bidder from the risk of identity theft. Even the pseudonym *pn* provided by the Third Party is only known to them. However in case the third party is

corrupted, he may reveal the pseudonym *pn* but still the real identity of the bidder is concealed.

4.4.3 Requirements Analysis and Evaluation

There are certain requirements which need to be fulfilled while developing an E-Auction protocol. We will analyze all these requirements briefly in the subsequent sections.

- **R1 Anonymity**

  The information about every bidder must be hidden from others. For this purpose we have developed an E-Auction protocol in which every bidder must register their real identity with a Registration Manager who is not an active member of the auction. It only keeps the identity of the bidders. The Third Party will authenticate each bidder and assign a pseudonym. Every bidder blind their *bid* value and send it to the TP to get his signature. So all the information about the bidder including his *bid* value is hidden from everyone until the auction is closed. In the winner determination phase the bidder sends his *bid* value only to the TP to determine the max_bid. So anonymity is preserved for all bidders even if the TP is corrupted. Because he has only the pseudonym and bid value which can't be linked to find the real identity of the bidder.

- **R2 Unforgeability**

  An attacker may try to forge the *bid* but fails due to the blinded *bid* which needs to solve ECDLP to find b and a. Moreover all the necessary information are encrypted with the session key and/or signed by the sender. Hence forgery attack is not possible which is also depicted in the Security Analysis.

- **R3 Non-Repudiation**

  The bidder as well as the TP must not be able to deny of their act. The bidder cannot deny of casting the *bid* because the signature Z' can be verified by using the eqn. $Z' + Q - K = u_1 T$ where Q is the public key of bidder. Similarly the TP can not deny of receiving the *bid* as the same signature is also verified by using his public key T.

- **R4 Public Verifiability**

  The signature Z' can be verified by everyone after publishing the signature parameter (Z', Q, K, T, u_1). Moreover the final winner *bid* can also be verified by everyone once the TP publish the (Z', max_bid). Because anyone can now find $u_2 = SHA - 1(max\_bid)$ and verify the signature Z'. The authenticity of every bidder can also be verified by anyone.

- **R5 Traceability**

  The winning bidder or any bidder who doesn't follow the auction rule can be identifiable using the traceability property as previously described in the proposed blind signature protocol section.

- **R6 Fairness and Robustness**

  This protocol satisfies the fairness property because even if the malicious bidder or auctioneer collude with the TP, they will not gain any information about the honest bidder that can harm him in the continuing or future auction.

- **R7 Privacy**

  Our protocol maintain the privacy of every bidder during the auction. It also preserves the privacy of the losing bidder even after the winner determination

phase in the auction.

- **R8 Integrity and Confidentiality**

  The integrity and confidentiality of the protocol is achieved through blind signature and the session key. No one can find the *bid* value before the winner determination phase due the blindness property. No one can change the *bid* value once signed by the TP else the signature cannot be verified. The strength depends on the ECDLP and the hash function.

- **R9 One Time Registration**

  In our scheme the bidder needs to register himself every time for a fresh auction. If the bidder registers every time then he will get a different s and s' for different e. So it will be difficult to link the bidder and preserves his anonymity else one can easily link the bidder and affect the future auction outcome.

4.5 Result Analysis

We evaluate the efficiency of our blind signature protocol and compare it with two recent schemes. Let I denotes the modular inverse operation, M denotes the point multiplication and H denotes the hash operation. Our scheme is far more computationally feasible than the other two schemes. The total computational load on our scheme is 4M+2H+1I. The result is shown in Table 4.1.

The proposed E-auction protocol is computationally slightly more costly with higher security and it fulfills all the requirements needed to be satisfied by an E-Auction protocol. Moreover it saves considerable amount of space in terms of key size as it is implemented through elliptic curve. The comparison result is shown in Table 4.2.

T(exp)- Exponential Time, T(S)- Symmetric Key Time, T(ME)- Modular

Table 4.1: Computational Time of different Blind Signature Protocols

Schemes	Blinding	Signing	Verifying
He *et al.* [28]	5M+2H+11	1M	2M+3H
Nayak *et al.* [29]	6M+1H	0M	3M
Proposed scheme	2M+1H+1I	0M	2M+1H

Exponentiation Time, T(h)- Hashing Time, T(SM)- Scalar Multiplication Time, T(PA)- Point Addition Time

Table 4.2: Comparison of Computational cost of different E-Auction Schemes

Schemes	Advertisement	Registration	Bidding	Winner Determination
Liaw *et al.* [18]	nT(exp)	2nT(exp)+5nT(h)	5nT(exp)	0
Wu *et al.* [19]	nT(exp)+nT(h)	2nT(exp) +2nT(S)+nT(h)	nT(ME)+ 4nT(exp)	nT(exp)+ nT(ME)+2nT(S)
Chen *et al.* [31]	T(exp)+T(ME)	2nT(exp)+ 4nT(ME)+2nT(h)	6nT(exp)+ 7nT(ME)+2nT(h)	2nT(ME)+ 2nT(exp)
Proposed scheme	T(exp)+T(h)	6nT(SM)+ 2nT(PA)+2nT(exp) +4nT(S)+5nT(h)	4nT(SM)+ 2nT(PA)+nT(h)	nT(SM)+ 2nT(PA)+4nT(S) +2nT(exp)+nT(h)

In Table 4.3 we have given the requirement evaluation result. Our scheme satisfies all the requirements which are needed for an electronic auction except the last as mentioned in the previous section.

Table 4.3: Requirement Analysis and Comparision

	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9
Liaw *et al.* [18]	√	√	×	√	√	×	×	√	×
Wu *et al.* [19]	√	√	√	√	√	√	×	√	×
Chen *et al.* [31]	√	√	√	√	√	√	√	√	×
Proposed scheme	√	√	√	√	√	√	√	√	×

Chapter 5

Conclusion

In this thesis we have proposed an electronic auction scheme using a blind signature protocol. As we know a blind signature is a different form of digital signature, we have first proposed a blind signature protocol according to the requirements of E-Auction and then employ it to design an electronic auction scheme. We have implemented both the protocols which are based upon elliptic curve cryptography. Our proposed blind signature is far more efficient than the competent schemes which we have shown in the result. Moreover an ECC based protocol is more efficient in terms of space complexity with a similar level of security. Hence we have adopted ECC to design an E-Auction protocol which produces considerable result with better security. The efficiency can further be improved using VLSI implementation and we can also include the transactional flow in our proposed E-Auction scheme with some extra computational cost.

Bibliography

[1] Yu Liu, "A new secure and efficient M+1st price auction scheme based on ECC system," Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on, vol., no., pp.489,492, 20-22 Aug. 2009

[2] Byoungcheon Lee, Kwangjo Kim and Joongsoo Ma, Efficient public auction with one-time, registration and public verifiability, Progress in Cryptology INDOCRYPT, Vol. 2247, pp. 162-174 January 2001.

[3] KazumasaOmote, A study on electronic auctions, Japan Advanced Institute of Science and Technology, March 2002.

[4] Kleusberg, Peter (2009). E-Collaboration und E-Reverse Auctions. Saarbrcken. p. P.16-25.

[5] Engelbrecht-Wiggans, Peter (2006). E-Sourcing in Procurement. Management Science. p. P.581.

[6] Wyld, David C. (2012). REVERSE AUCTIONS 101. Louisiana: Southeastern Louisiana University.

[7] W. Diffie and M. E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6):644654, 1976.

[8] B. A. Forouzan. Cryptography & Network Security (1st edition). McGraw-Hill, Inc., 2008.

[9] W. Stallings. Cryptography and Network Security - Principles and Practice (3rd edition).Prentice Hall, 2003.

[10] D. Chaum. Blind Signatures for Untraceable Payments. In Advances in Cryptology:Proceedings of CRYPTO 82, pages 199203, 1982

[11] V. S. Miller. Use of Elliptic Curves in Cryptography. In Lecture notes in computer sciences; on Advances in cryptology - CRYPTO 85, volume 218, pages 417426, 1986.

[12] Franklin M K, Reiter M K. The design and implementation of a secure auction service. IEEE Transactions on Software Engineering, May 1996, 22(5): 302312.

[13] Kudo M. Secure electronic sealed-bid auction protocol with public key cryptography. IEICE Transactions on Fundamentals, Jan. 1998, E81-A(1): 2027.

[14] Kikuchi H, Hakavy M, Tygar D. Multi-round anonymous auction protocols. IEICE Transactions on Information and Systems, Apr. 1999, E82-D(4): 769777.

[15] Chang C, Chang Y F. Efficient anonymous auction protocols with freewheeling bids. Computers & Security, 2003, 22(8): 728734.

[16] Jiang R, Pan L, Li J H. An improvement on efficient anonymous auction protocols. Computers & Security, 2005, 24(2): 169174.

[17] Chang C C, Chang Y F. Enhance anonymous auction protocols with freewheeling bids. In Proc. the 20th International Conference on Advanced Information Networking and Applications (AINA 2006), Vienna, Austria, Vol. 1, Apr. 2006, pp.353358.

[18] Liaw H T, Juang W S, Lin C K. An electronic online bidding auction protocol with both security and efficiency. Applied Mathematics and Computation, 2006, 174(2): 14871497

[19] C. C. Wu, C. C. Chang and I. C. Lin, New Sealed-Bid Electronic Auction with Fairness, Security and Efficiency, Journal of Computer Science and Technology, vol. 23, no. 2, (2008), pp. 253.

[20] D. Chaum. Blind Signature Systems. US patent 4759063, July 1988.

[21] Z. Shao. Improved User Efficient Blind Signatures. Electronics Letters, 36(16):13721374, 2000.

[22] D. H. Yum and P. J. Lee. Generic Construction of Certificateless Signature, volume 3108 of Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2004.

[23] J. L. Camenisch, J. M. Piveteau, and M. A. Stadler. Blind Signatures Based on the DiscreteLogarithm Problem. InAdvances in Cryptology- EUROCRYPT94, pages 428432. Springer, Berlin, 1994.

[24] L. Harn. Cryptanalysis of the Blind Signatures based on the Discrete Logarithm Problem. Electronics Letters, 31(14):11361137, 1995.

[25] P. Horster, M. Michels, and H. Petersen. Cryptanalysis of the Blind Signatures based on the Discrete Logarithm Problem. Electronics Letters, 31(21):18271828, 1995.

[26] C. Lee, M. Hwang, and W. Yang. A New Blind Signature based on the Discrete Logarithm Problem for Untraceability. Applied Mathematics and Computation, 164(3):837841, 2005.

[27] S. A Vanstone. Elliptic Curve Cryptosystem - The Answer to Strong, Fast Public-key Cryptography for Securing Constrained Environments. Information Security Technical Report, 2(2):78 87, 1997.

[28] D. He, J. Chen, and R. Zhang. An Efficient Identity-based Blind Signature Scheme without Bilinear Pairings. Computers and Electrical Engineering, 37(4):444450, 2011.

[29] Sanjeet Kumar Nayak, "Blind Signature Schemes using Elliptic Curve Cryptography", Master's Dissertation, National Institute of Technology, Rourkela, pp. 1-61, 2013.

[30] S. K. Nayak, B. Majhi, and S. Mohanty, "An ECDLP based untraceable blind signature scheme," Second IEEEInternational Conference on Circuits, Power and Computing Technologies (ICCPCT), pp. 829 - 834, 20-21 March 2013.

[31] Y. F. Chung, Y. T. Chen, T. L. Chen and T. S. Chem, An agent-based English auction protocol using Elliptic Curve Cryptosystem for mobile commerce, Expert Systems with Applications, vol. 38, no. 4, (2011), pp. 9900