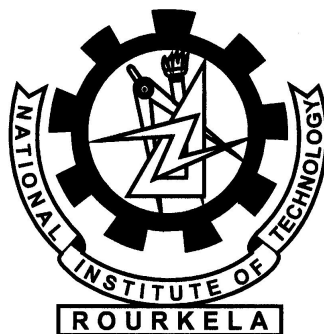# An Online English Auction Scheme

Rajnish Kumar

(Roll No: 213CS2161)

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

An Online English Auction Scheme

Thesis submitted in partial fulfillment

of the requirements for the degree of

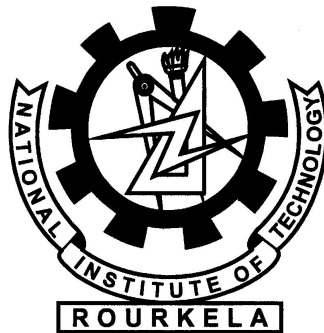## Master of Technology

in

Computer Science and Engineering

by

Rajnish Kumar

(Roll No: 213CS2161)

under the guidance of

Dr. Sujata Mohanty

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

Declaration of Authorship

3

I, **Rajnish Kumar** hereby declare that neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere. If it is found the I will be responsible for this.

Rajnish Kumar

Dedicated to my parents and teachers

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

Certificate

This is to certify that the work in the thesis entitled **" *An Online English Auction Scheme*"** submitted by **Rajnish Kumar** is a record of an original research work carried out by him under our supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science and Engineering, National Institute of Technology, Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Dr.Sujata Mohanty
Assistant Professor
Department of CSE
National Institute of Technology
Rourkela-769008

Place: NIT,Rourkela-769008
Date: 24 - 06 - 2015

Acknowledgment

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

I wish to thank all faculty members and secretarial staff of the Compure Science and Engineering Department for their valuable cooperation.

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

When I look back at achievements in my life, I can see a clear trace of my family's worries and devotion everywhere. My dearest mother, whom I owe everything I have achieved and whatever I have become; my beloved father, for always believing in me and inspiring me to dream big even at the toughest moments of my life; and my brother ; who has always supported me during my difficult periods.

Rajnish Kumar

Abstract

Online English auction is most familiar and mostly used online auction process in the present scenario. It is the most efficient auction process which gives most desirable results in terms of revenue . Our scheme involves three parties, namely the Registration Manager(RM), Auction Manager(AM), and Bidder(B). The Registration Manager publicizes the parameters to register the bidders, allowing them to participate in the bidding process. It also protects the bidding rights and manages the information on the key. The Auction Manager is responsible for conducting the bidding after the registration is over. Our proposed scheme satisfies the following features such as anonymity, no framing, unforgeability, non-repudiation, fairness, public verifiability, one-time registration, and easy revocation. The scheme uses Discrete Logarithmic Problem (DLP) and Secure Hash Algorithm (SHA-1) as hash function.

Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Description
B	Bidder
AM	Auction Manager
RM	Registration Manager
DLP	Discrete Problem
SHA	Secure Hash Algorithm

Chapter 1

Introduction

Online Auction

Security Loopholes

Motivation

Objective of Research

Organization of Thesis

Chapter 1

Introduction

1.1   Online Auction

Online auctions overcome traditional auctions and usually the number of bidders are in large number. In both online and traditional auctions, bidders and sellers buy and sell products and services. Bid price at the start of bidding process are less but they increase gradually to meet market demand. Online auctions are available across the whole world through internet and the time span of auctioning of a product ranges from one to ten days normally.

Online auctions have become popular because of the following reasons:

- There is no limitation of time.

- Time limits are flexible as anytime a bidder can go for bidding if it is in process.

- There are no such limitations of geography.

- Social interactions are high in Online auctions.

- The number of sellers and bidders are in large number, which gives a bidder an opportunity to select the item which is desirable to him/her. Also the sellers make huge profit due to large number of bidder participation.

1.2   Types of Online Auction

1.2.1   English Auction

In English bidding the bid starts from a minimum value and price of the item increases in ascending order. The bidder with highest amount of bid is declared as the winner when the auction ends and the price to be paid by the bidder is the highest bid made by him/her.

Sometimes, The seller sets a minimum price for bid from which the bid starts which is called as base price or reserve price. The English Auction is most popular for the reason that, it uses a process that people can understand which helps in reducing transaction costs[11]. In Online English auctions the physical presence of the bidders is not required so it overcomes the traditional English auction. Even though it is a vulnerable to various forms of forgery its popularity has increased in recent years.

There are three variations in English Auction as follows:

- The base/reserve price is not revealed sometimes at the start of the auction[20].

- Sometimes, instead of being called out, the bids are with signals such as lightening the candle in physical environment.

- Sometimes, before dropping out of bidding the bidders must announce that he/she is backing off of the auction process. This is known as open-exit auction.

1.2.2 Dutch Auction

Dutch auctions are the exactly opposite of English auctions. In the case of English auction the bid starts from minimum amount but in the case of Dutch auctions the bid starts from highest amount and the price is is systematically lowered until the first buyer accepts the price to pay. On an average it is found that in this type of auction the accepted price is 30 percent higher then other auction schemes[2].

There are mainly four variations in Dutch Auctions such as:

- **Basic Dutch Auction :** In this type of format, the only one product is offered for sale not multiple ones. The starting bid price is very high and it is lowered until a bidder is intrested to buy the product at that price [19].

- **Second-Item Auction :** In this format of dutch auction, a predetermined number of equal products are available. Bidders then bid with the price and amount of that item. At last, the bids are collected, a clearing price is determined on the basis that the supply of product equals demand or not. Each bidder then pays the same bid price for their bid quantity. This format of auction is very powerful and simple to use, but it has one major drawback that bidders only get to place only one bid.

- **Supply/Demand Auction :** In this format, the bidders and the sellers place a single bid with a price and quantity. Bidders bid on what they would like to buy at, sellers on the other hand look at what price/quantity they would like to sell at. When all the bids are collected from both bidders and sellers, a final price is determined where supply equals demand. This format is effective when the number of buyers and seller are large.

- **Advanced Dutch Auction :** In this type of auction, bidders are allowed to create an entire demand curve instead of limiting them to a single value so that multiple bids can be placed by a bidder.

1.2.3 Sealed first price/Blind auction

In this type of auction all the bidders submit their bid price which is called as sealed bid, In this case the bid price is known to the corresponding bidder himself not other bidders[17]. The bidder with highest submitted bid price wins the bid and the final price of the item becomes the bid price of that bidder. But in this case, since the bidders are unable to know the bid price of other participants they can not adjust their bid price accordingly.

There are five variations in Blind Auction as follows:

- The can be known or unknown number bidders[18].

- There may not be any starting price so that an item will be sold definitely.

- The bid price of winner may be announced to be verified by other biddrs that their price of bid was less then winner. Bid price of non winning bidders may also be made public.

- The negotiation on the final bid price may or may not be entertained by auctioneer.

1.2.4 Vickrey auction

This type of auctions are similar to the Blind Auctions. But the only difference is that the winner pays the bid price of second highest bidder.

1.3 Sill Bidding

A shill refers to someone who purposely gives the impression that he or she is an enthusiastic independent customer of a seller that he/she is secretly working for[2]. A shill usually bids in an auction which is conducted by a particular seller. The bid frequency of a shill is usually very high. A shill can have no or few wins.

1.4 Security loopholes

1 **Anonymity:** During the auction process, the identity of a bidder should not be determined by any other bidder and also the Auction Manager[9].

2 **Traceability :** When the auction ends, the winner of the bidding process should be identified.

3 **No framing :** Using the identity of any bidder no any other bidder can participate in the bidding.

4 **Unforgeability :** There should not be any case of bid forgery.

5 **Non-repudiation :** The bidder who wins the bid cannot deny his/her price of bid after the winner is announced.

6 **Fairness :** The requests for bidding by any bidder should be dealt in fair manner by Registration Manager at any cost.

7 **Public Verifiability :** At the end of the auction, the identity of winner and the final bid price must be be verified by any other bidder.

8 **Unlinkability among different rounds of auction :** During the different rounds of auction, there could be no one who can draw any conclusion about the link of any other individual participant[3].

9 **Linkability in a round of auction :** During a particular round of auction, any bidder could be in a position to know the number of bids offered by a particular bidder and also the bid price.

10 **Efficiency of bidding :** Complexity of bidding process and costs transmission during the auction should be minimized.

11 **One-time registration :** Initially, the bidder needs to be registered to the Registration Manager.After the registration, the bidder can participate multiple bidding.

12 **Easy revocation :** The bidding rights of any bidder could be easily and efficiently revoked by Registration manager.

1.5   Participants in Online Auctions

1 **Registration Manager(RM) :** The bidder's registration key and his/her identity is kept secret by Registration Manager, it also manages and stores the information on the key. When the auction ends, the Registration Manager forwards the information and identity of winner to the seller of the product when the auctioneer requests[1].

2 **Auction Manager(AM) :**After the registration process, the Auction Manager takes the charge of conducting the bidding process[8].

3 **Bidder(B) :** Participant in the auctioning process.

1.6   Stages of Online Auction

There are five stages of Online Auction as follows[7][16] :

1 **Bidder's Registration :** Identity information of bidder and registration key is posted to registration manager.

2 **Generation of auction keys :** When a request for an auction comes, the Registration Manager produces auction keys for each bidder.

3 **Auction setup :** Auction manager gets the keys of all available legitimate bidders from the Registration Manager's bulletin board and the auction starts.

4 **Bidding stage :** Bidding starts using the public key of Auction Manager and private key of bidder and also signature is calculated.

5 **Verification stage :** The legitimacy of the bidder is verified.

6 **Announcing the winning bidder :** After the whole process, the Auction Manager and Registration Manager both post the information of winner on the bulletin board for the other bidders to verify whether the bid if fair or not.

1.7 Digital Signature

In conventional signature the signature is not a separate document rather it is a part of the document. But in digital signature, the signature is a separate document. The signer sends two documents: the message and the signature. Both documents are received by the receiver and the receiver verifies the signature whether it belongs to the sender or not[5]. The another difference between a conventional signature and digital signature is that we can duplicate the conventional signature but in digital signature it is not possible unless there is a factor of time (for instance time-stamp). Digital signature provides message authentication, message integrity and non-repudiation using a trusted party. Hash functions are used to preserve the message integrity.

The signature process includes three steps:

- Key generation.

- Signing.

- Verification.

1.7.1 Attacks on Digital Signature

1)Key-Only Attack: In this type of attack, the intruder has the access of only public information published by the sender. To forge the message, the intruder needs to create the signature and convince the receiver that the message is coming from the sender[13].

2)Known –Message Attack: In this type of attack, the intruder has the access of one or more message signature pair or we can say that, the intruder has the access of some documents already signed by the sender[14]. After getting the message signature pairs, the intruder tries to create another message and forge sender's signature.

3)Chosen-Message Attack : In this type of attack, when the sender signs one or more messages for the intruder, the intruder tries to create another message of his/her wish, and forges the sender's signature in it[15].

1.8 Motivation

In this advanced era, people have become so much dependent on the technology and everyone wants to save the time. Due to this, online auctioning has become very much popular these days. Since e-commerce and online money transaction has become so much popular it has made online auctioning process so easy and user friendly.

There are many limitations of traditional auctions such as geographical boundary, each bidder's physical presence, time limit and a small target audience. This has to be dealt with due to increase in the number of buyers. In online auction process the major concern has become security because of the increase in forgery over the internet. Earlier methods are having shortcomings related to the internet security. Shill bidding has also become one of the key factors affecting online auctioning process. Thus an efficient and secured auction process is required.

1.9 Objectives of Research

- To propose an efficient Online English Auction Scheme.

- To propose an Online English Auction Scheme which is secured and nullifies the security loopholes.

- To propose an Online English Auction Scheme which is free from Shill Bidding.

1.10 Organisation of Thesis

The rest of Thesis is organized as follows :

Chapter 2: In this chapter, A survey of Online English Auction scheme by Wu et al. is discussed.

Chapter 3:In this chapter, we have shown our proposed Online English Auction scheme.

Chapter 4:In this chapter, we have shown implementation and result implementation. We have also mentioned the security analysis in this chapter.

Chapter 5:In this chapter, we have shown the conclusion and future work.

Chapter 2

Literature Survey

Chapter 2

Literature Survey

2.1 Review of Wu et al. Scheme:

This scheme consists of three participants namely Registration Manager, Auction Manager and the Bidder. Here the RM is responsible for the identity of the bidder and corresponding registration key as well as key management storage of information[3]. When the auction ends, the Registration Manager should forward the information about the winning bidder and his/her identity to the seller of the product, at the request of the user. Whereas, the Auction Manager takes the charge of auction after the registration process and conducts the auction and Bidder is participant in the auction process.

The auction process consists of six phases namely Initial stage, Bidders' registration stage Auction setup, Bidding stage, Verification stage and Announcement of the winning bidder.

2.1.1 Bidding parameters

p : p is a large prime number.

q : q is prime factor of (p-1).

g : A generative number of the order q.

B_i : Bidder number i.

SK_i : Private key of B_i.

RK_i : Registration key of B_i.

SK_{AM}: Private key of the Auction Manager.

PK_{AM}: Public key of the Auction Manager.

r_j : A random number selected by the Auction Manager during j^{th} auction.

g_j : Auction Manager's public information in the jth auction.

$v_{i,j}$: A parameter selected and made public by the Auction Manager in the ith auction so that others can verify bidder B_i .

$C_{i,j}$: The bidder B_i's proof the he/she has participated in j^{th} auction.

$(W_{1j}, W_{2j}$: A point arbitrarily selected and made public by the Auction Manager in the jth auction for others to Verify bidder's certificates.

2.1.2 Bidding Stages

1 **Initial Setup :**

- The Registration Manager publicizes p, q, g and $h(.)$ where p is a very large prime number, q is prime factor of (p-1), g is a generative number of the order q and $h(.)$ is one way hash function.

- The Auction Manager during this stage performs three steps as:

  Step 1 : The Auction Manager establishes a bulletin board which is read only. It verifies the information of all bidders during auction. The Auction Manager also conserves the updating rights[1].

  Step 2 : The Auction Manager selects its private key $SK_{AM} \in Z_q^*$, and calculates its public key as follows:

  $$PK_{AM} = g^{SK_{AM}} mod\, p \tag{2.1}$$

  Step 3 : Finally, The Auction Manager(AM) publicizes PK_{AM} .

2 **Bidder Registration :** In this stage each bidder who wants to join the auction process, he/she must follow the following three steps of registration :

  Step 1 : Each bidder has to select a private key $SK_i \in Z_q^*$ and calculate its corresponding registration key as follows:

  $$RK_i = g^{SK_i} mod\, p \tag{2.2}$$

  Step 2 : Bidder also selects an integer $t \in Z_q^*$ and calculates the information verification of RK_i ,(γ_i and ε_i) as calculated below:

  $$\gamma_i = h(g^t mod\, p) \tag{2.3}$$

$$\varepsilon_i = (t + SK_i\gamma_i) \tag{2.4}$$

Finally, the bidder forwards the following parameters $(RK_i, \gamma_i, \varepsilon_i)$ to the Registration Manager.

After receiving the parameters sent by the bidder such as $(RK_i, \gamma_i, \varepsilon_i)$ the Registration Manager can determine the legitimacy if i^{th} bidder based on the equation given below:

$$\gamma_i' = h(g^{\varepsilon_i}RK_i^{-1})mod\,p \tag{2.5}$$

If the equation 2.5 holds, the Registration key RK_i of ith bidder is verified as a valid key. Now, the identity information of ith bidder as well as the registration key of corresponding bidder B_i (RK_i), is stored in the user registration database and is sent to the Auction Manager. This completes the registration process for the bidder B_i.

3 **Auction Setup :** The AM makes the set of all registered bidders who have been already registered as $U = B_1, B_2, ..., B_n$ where n is the no of registered bidders. The Auction Manager follows the following steps when an auction is requested for the auction setup. Let us assume that the auction below is at j^{th} bid.

Step 1 : The Auction Manager selects an integer $r_j \in Z_q$ and calculates its public information g_j as follows:

$$g_j = g^{r_j}mod\,p \tag{2.6}$$

Step 2 : The Auction Manager calculates S_i and $\partial_{i,j}$ for all i^{th} bidder B_i as:

$$S_i = RK_i^{SK_{AM}}mod\,p \tag{2.7}$$

$$\partial_{i,j} = RK_i^{r_jh^j(S_i)}mod\,p \tag{2.8}$$

Step 3 : Now, the Auction Manager randomly selects $W_{1,j}, W_{2,j} \in Z_p^*$, and finds a straight line $L_{i,j}$ using the points $(0, \partial_{i,j})$ and $W_{1,j}, W_{2,j}$, then identifies $(V_{i,j}, 0)$, the intersecting point of the x-axis and $L_{i,j}$, as :

$$v_{i,j} = (W_{1,j}\partial_{i,j}) * (\partial_{i,j} - W_{2,j}^{-1})mod\,p \tag{2.9}$$

Step 4 : Finally, the Auction Manager posts ($W_{1,j}, W_{2,j}, g_j, v_{1,j}, v_{2,j}, ..., v_{n,j}$) for verification.

4 **Bidding Stage :** For any bidder B_i to participate in j^{th} auction, the bidder B_i must follow the steps given below :

Step 1 : The bidder calculates S_i using the AM's public key PK_{AM} as :

$$S_i = SK_{AM}^{PK_{AM}} mod \, p \tag{2.10}$$

Step 2 : By using the private key of ith bidder SK_i and previously calculated value of S_i, the bidder calculates its auction certificate $C_{i,j}$ as follows:

$$C_{i,j} = g_j^{SK_i h^j(S_i)} mod \, p \tag{2.11}$$

Step 3 : Now, the bidder selects an integer $t \in Z_q{}^*$, fixes a price of bid as $bidi, j$, after this the bidder calculates the corresponding signature ($a_{i,j}$ and $b_{i,j}$) as :

$$a_{i,j} = h((g_j^t mod \, p) \| bid_{i,j} \tag{2.12}$$

$$b_{i,j} = (t + SK_i h^j(S_i) a_{i,j}) mod \, q \tag{2.13}$$

At last, each bidder publicizes ($C_{i,j}$,$bid_{i,j}$,$a_{i,j}$,$b_{i,j}$), which completes the bidding process.

5 **Verification Stage :** During the verification stage it is necessary that any bidder participating in the bidding process should verify the bidder and bidding amount.The values publicized by each ith bidder such as ($C_{i,j}$,$bid_{i,j}$,$a_{i,j}$,$b_{i,j}$), can be verified by any other bidders as follows:

Step 1 : The legitimacy of $C_{i,j}$ can be verified by following equation :

$$a_{i,j} = h((g_j^{b_{i,j}} C_{i,j}^{-a}{}_{i,j})) \tag{2.14}$$

If the above equation is satisfied, then $C_{i,j}$ is verified as a valid auction certificate and the bid price of B_i is accepted.

Step 2 : Auction information verification $v_{i,j}$ is calculated using (0,$C_{i,j}$) and ($W_{1,j}$,$W_{2,j}$) as follows:

$$v'_{i,j} = (W_{1,j}C_{i,j}) * (C_{i,j} - W_{2,j})^{-1} \quad (2.15)$$

Finally, after comparing the values v and v' , if they are equal then the bid price $C_{i,j}$ is declared as the price bid by the legitimate bidder.

6 **Winner Announcement Stage :** When bidding completes, the Auction Manager obtains the information on the highest bid and forwards $(h^j(S_i)r_j)^{-1} of i^{th}$ bidder to the Registration Manager. Now, RK_i is calculated by RM using $C_{i,j}$ and $(h^j(S_i)r_j^{-1})$. The result is saved in the database by RM, which confirms the bidder identity and then the Registration Manager informs manufacturer about winner of that item.

2.1.3 Mathematical Preliminaries

1 **Discrete Logarithmic Problem (DLP)** In mathematics, a discrete logarithm is an integer k solving the equation $a^k = b$. Here b and k are elements of a finite group. Discrete logarithms are the finite-group-theoretic correlation of ordinary logarithms, for two real numbers a and b, it solves the same equation, where the base of the logarithm is a and b is the value whose logarithm is being taken. It is believed that computing discrete logarithms is very difficult[5]. No such powerful general method for computing discrete logarithms on traditional computers is known, and public key cryptography based algorithms use DLP based security by assuming that it has no efficient solution. In short, we can say that for any $y \in Z_p^*$, it is computationally in-feasible to derive 'x' such that $y = g^x mod p$.

2 **One Way Hash Function** One way hash functions are the functions which after being applied to an element it is computationally in-feasible to get the original element. The One way hash function used in the above described bidding process is as follows:

$$h^j(k) = h(k, h^{j-1}(k) \quad (2.16)$$

Where,

$$h^0(k) = k \quad (2.17)$$

Chapter 3

Proposed Scheme for Online English Auction

System Parameters

Bidding Stages

Correctness Verification

Chapter 3

An Online English Auction scheme

3.1 Proposed Scheme

The proposed Online English auction protocol consists of a Registration Manager (RM), an Auction Manager (AM) and bidder(B). The RM publicizes the public parameters to register the bidders, allowing them to participate in the bidding process. The RM also protects the information about the bidders identity as well as for the manages and stores the information on the key . When the registration process is over control of the auction process goes to the AM. AM gets the registration keys of each corresponding bidders from the RM, and at the end of the auction AM sends the winning bidder's identity to the Auction Manager. Bidder participates in the bidding and produces its own ticket for the bidding and sends to Auction Manager. The scheme consists of five phases namely Initial stage, Registration phase, Auction setup, Bidding and verification and winner announcement phase.

3.1.1 System Parameters

p : A large prime number.

q : A prime factor of $(p-1)$.

g : A generative number of order q.

B_i : i^{th} bidder.

SK_{AM} : Auction Manager's private key.

PK_{Am} : Auction Manager's public key.

SK_i : i^{th} bidder's private key.

RK_i : i^{th} bidder's registration key.

m : message (price of bid).

$h(.)$: SHA-1 hash function.

TK_i : Bidder's bid ticket produced by the Auction Manager.

3.1.2   Bidding Stages

The proposed scheme consists of five stages.

1 **Initial stage:**

First of all, the Registration Manager publicizes the public parameters such as p and q, where p is a large prime number, q is a prime factor of (p-1), g is the generative number of order q and h(.) is SHA-1 hash function.

Secondly, the AM selects its private key $SK_{AM} \in Z_q{}^*$ and calculates its own public key as :

$$PK_{AM} = g^{SK_{AM}} mod\, p \tag{3.1}$$

At last PK_{AM} is made public by the Auction Manager.

2 **Registration Stage :**

During this phase each bidder calculates its registration key RK_i using its own private key $SK_i \in Z_q^*$ as follows :

$$RK_i = g^{SK_i} mod\, p \tag{3.2}$$

Also, each bidder selects $k \in Z_q^*$ and calculates :

$$L_i = h(g^k) mod\, p \tag{3.3}$$

$$M_i = (k - SK_i L_i) mod\, q \tag{3.4}$$

Now, the bidder forwards the parameters (RK_i, L_i, M_i) to the Registration Manager. After getting these parameters sent by the bidder, the Registration Manager checks the legitimacy of each i_{th} bidder. For this, the Registration Manager calculates :

$$L_i' = h(g^{M_i} RK_i{}^{L_i}) \tag{3.5}$$

If the Registration Manager finds that $L_i = L_i'$, then the bidder (B_i) is considered as the legitimate bidder and registration key (RK_i) of each bidder is sent to the

Registration Manager's database otherwise, the registration is unsuccessful and is rejected.

3 **Auction Setup Stage:**

This stage involves two steps as :

Step 1 : The Registration Manager sends the registration key RK_i of each bidder to the Auction Manager.

Step 2 : After getting the registration keys of each bidder, the AM calculates the bidding ticket for each bidder as:

$$TK_i = h(RK_i PK_{AM}) mod p \qquad (3.6)$$

After creating the ticket of the bidder, the Registration Manager sends it to the corresponding bidder.

4 **Bidding and Verification Stage:**

During the bidding phase, each bidder selects $w \in Z_q^*$ and calculates $k = g^w mod p$, the value of 'k' is made as public and encrypts the message 'm'(price of the bid) as:

$$C_i = E_k(m) \qquad (3.7)$$

Now, the bidder calculates the following parameters :

$$r_i = g^w mod q \qquad (3.8)$$

$$l = g^{TK_i} mod q \qquad (3.9)$$

$$e_i = h(r_i) \qquad (3.10)$$

$$S_i = (e_i TK_i + w) mod q \qquad (3.11)$$

After calculating the above parameters, the bidder sends (C_i, l, e_i, S_i) to the the auction manager for verification.

After receiving the parameters (C_i, l, e_i, S_i),the Auction Manager computes:

$$r'_i = (g^{S_i} l^{-e_i}) mod q \qquad (3.12)$$

After computing the above equation, the Auction Manager also checks whether

$e_i = h(r_i^{'})$ or not. If satisfies then the bid is legitimate. Also, the Auction Manager declares C_i of each bidder as public after the end of each round of auction.

4 **Winner Announcement Stage :**

After the end of the auction, the Auction Manager decrypts the message(m) as :

$$m = D_k(C_i) \tag{3.13}$$

And, the bidder with highest bidding price is declared as winner.

3.1.3 Correctness Verification

The Registration Key RK_i is a valid Registration key and B_i is the legitimate bidder can be proved by following correctness equation:

$$
\begin{aligned}
L_i^{'} &= h((g^{L_i} RK_i^{M_i}) mod\, p) \\
&= h((g^{k-SK_iL_i}.g^{SK_iL_i}) mod\, p) \\
&= h(g^{k-SK_iL_i+SK_iL_i}) mod\, p \\
&= h(g^k) mod\, p \\
&= L_i
\end{aligned}
$$

The legitimacy of the bid can be proved by following correctness equation

$$
\begin{aligned}
r_i^{'} &= (g^{S_i} l^{-e_i}) mod\, q \\
&= (g^{e_i TK_i + w}.g^{-TK_i e_i}) mod\, q \\
&= (g^{e_i TK_i + w - e_i TK_i}) mod\, q \\
&= (g^w) mod\, q \\
&= r_i
\end{aligned}
$$

31

Chapter 4

Implementation & Results
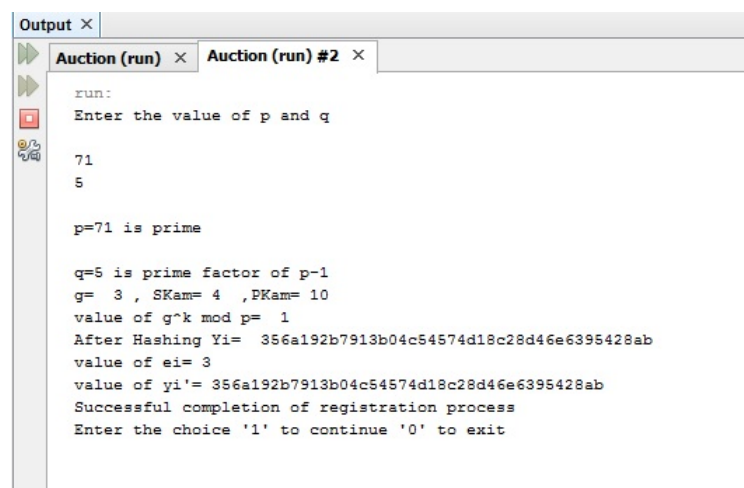
Implementation

Security Analysis

Chapter 4

Implementation & Results

This chapter gives overview about implementation and security analysis. Section 4.1 explains about implementation. and Section 4.2 explain about security analysis.
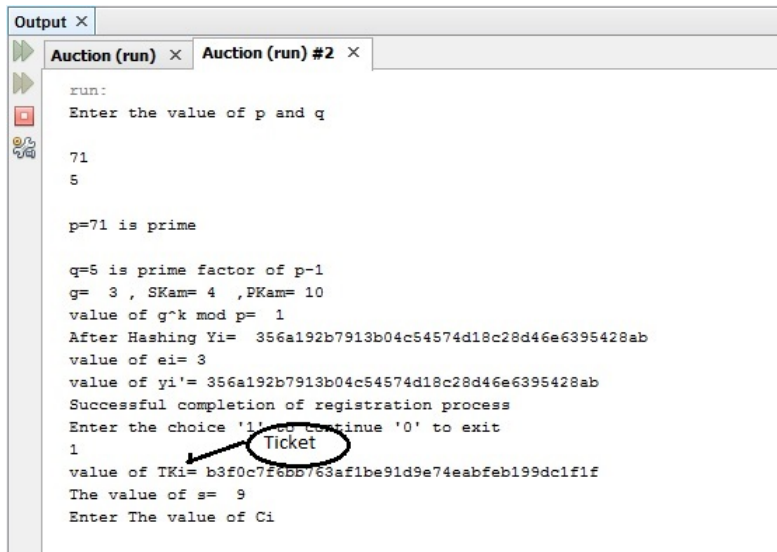
4.1 Implementation

The proposed algorithm has been implemented on java platform and the following snapshots show its implementation:

Figure 4.1 shows the successful completion of the registration process, Figure 4.2 shows the ticket issuing by the Auction Manager after successful registration, Figure 4.3 shows the successful completion of bidding process and Figure 4.4 shows the database of the Auction Manager.

Figure 4.1: Registration Process
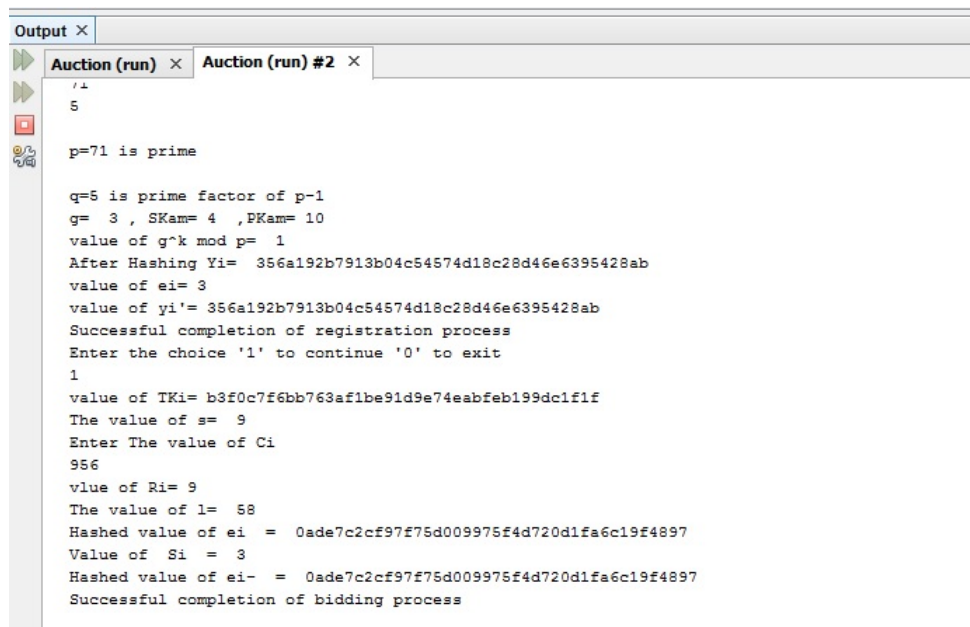
```
Output ×
  Auction (run) ×   Auction (run) #2 ×
      run:
      Enter the value of p and q

      71
      5

      p=71 is prime

      q=5 is prime factor of p-1
      g=  3 , SKam= 4  ,PKam= 10
      value of g^k mod p=  1
      After Hashing Yi=  356a192b7913b04c54574d18c28d46e6395428ab
      value of ei= 3
      value of yi'= 356a192b7913b04c54574d18c28d46e6395428ab
      Successful completion of registration process
      Enter the choice '1' to continue '0' to exit
      1                      Ticket
      value of TKi= b3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f
      The value of s=  9
      Enter The value of Ci
```
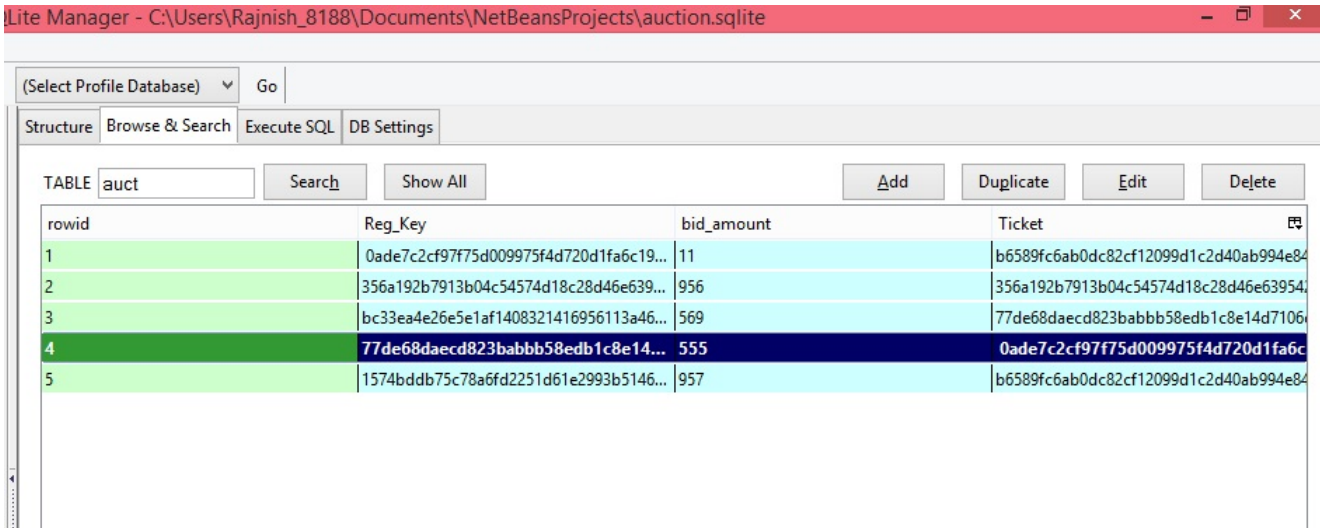
Figure 4.2: Ticket Issued by AM(TK_i)

```
Output ×
  Auction (run) ×   Auction (run) #2 ×
      71
      5

      p=71 is prime

      q=5 is prime factor of p-1
      g=  3 , SKam= 4  ,PKam= 10
      value of g^k mod p=  1
      After Hashing Yi=  356a192b7913b04c54574d18c28d46e6395428ab
      value of ei= 3
      value of yi'= 356a192b7913b04c54574d18c28d46e6395428ab
      Successful completion of registration process
      Enter the choice '1' to continue '0' to exit
      1
      value of TKi= b3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f
      The value of s=  9
      Enter The value of Ci
      956
      vlue of Ri= 9
      The value of l=  58
      Hashed value of ei  =  0ade7c2cf97f75d009975f4d720d1fa6c19f4897
      Value of  Si  = 3
      Hashed value of ei- =  0ade7c2cf97f75d009975f4d720d1fa6c19f4897
      Successful completion of bidding process
```

Figure 4.3: Successful Bidding

34

Figure 4.4: AM's database

4.2 Security Analysis

1 **Anonymity :** Since, the method uses registration key which is calculated using the secret key (SK_i) of the each bidder, therefore no one can identify the identity of the bidder .

2 **Unforgeability :** In our method, no one can forge with the signature because the method is based on DLP. For any $y \in Z_p^*$, it is computationally infeasible to derive 'x' such that $y = g^x mod p$. In our method, 'w' is kept secret by the bidder. so, it is infeasible to get r_i calculated by the bidder.

3 **Non-repudiation :** The winner can not deny his/her bidding prices when the winner is announced, because each bidder receives a ticket which is calculated by his/her registration key and is known to both Registration Manager and Auction Manager.

4 **Public verifiability :** Any bidder can verify the ticket of another bidder whether it is issued by AM or not because RK_i is known to everyone. Also the bid price is shown along with the TK_i of corresponding bidder by Auction Manager on the bulletin board, so that other bidders can know the prices of that bidder.

5 **One-time registration :** After being registered with the Registration Manager, the bidder can participate in any number of auctions because any Auction Manager in link with that RM can get the RK_i of that bidder and send the ticket to start the

bidding process.

6 **No framing :** In our method no one can participate in the bidding using the identity information of another bidder because the registration key is known to the Auction Manager, Registration Manager and the bidder himself. The ticket produced by the Auction Manager is based on the registration key of the bidder and the public key of the Auction Manager.

7 **Fairness :** Since the AM gets only registration key RK_i of each bidder and RM keeps all other identity information of the bidder with himself so, there is no question for the AM to not to deal in fair manner.

Chapter 5

Conclusion and Future Work

Contribution

Future Work

Chapter 5
Conclusion and Future Work

In this thesis, an efficient Online Auction Scheme has been proposed using Discrete Logarithmic Problem(DLP), Digital Signatures and hash functions to meet the security features such as Anonymity,Unforgeability,Non Repudiation,Public Verifiability,One time Registration, No-framing,and fairnes in the bidding process.

In future the remaining loopholes Unlinkability among different rounds of Auction and linkability in a round of the Auction will be discussed to fulfill the all security loopholes in an Online English Auction.But , when all security loopholes are discussed ,it comes with a cost of more complex scheme and the scheme does fail in therms of avoiding Shill Bidding.

Bibliography

[1] 1) Tzer-Shyong Chen, An English auction scheme in the online transaction environment, Department of Information Management, Tunghai University, 181 Taichung-Kang Road, Section 3, Taichung 40744, Taiwan, ROC. February 2004.

[2] Wenli Wang,Zoltan Hidvegi, Andrew B. Shill bidding in Online English auction. Whinston,Decision and Information Analysis, Goizueta Business School, Emory University, Atlanta, GA, 30322 ,Center for Research on Electronic Commerce, Department of MSIS, The University of Texas at Austin,2). january 2001.

[3] 3) Yu-Fang Chung , Yu -Ting Chen , Tzer-Long Chen , Tzer-Shyong Chen. An agent-based English auction protocol using Elliptic Curve Cryptosystem for mobile commerce .10.1016/j.eswa.2011.02.039.

[4] 5) Kazumasa Omote and Atsuko Miyaji. A practical English auction with one time registration., vol.24, 2005, pp 74-88.

[5] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.

[6] Chida K, Kobayashi K, Morita H. Efficient sealed-bid auctions for massive numbers of bidders with lump comparison. Proceedings of ISC 2001; 2001. pp 408-19.

[7] Franklin M, Reiter M. The design and implementation of a secure auction service. IEEE Trans Software Eng 1996;5(22):pp 302-12.

[8] Mullen T, Wellman M. The auction manager: market middleware for large-scale electronic commerce. Proceedings of the Third USENIX Workshop on Electronic Commerce; 1998. pp 49-60.

[9] Nguyen K, Traore J. An online public auction protocol protecting bidder privacy. Proceedings of Australasian Conference on Information Security and Privacy 2000; 2000: pp 427-42.

[10] Omote K, Miyaji A. A practical English auction with simple revocation. IEICE Trans Fundam May 2002;E85-A(5), pp. 1054-61.

[11] Wu, T. C., Chen, K. Y., Lin, Z. Y. (2002). An english auction mechanism for internet environment. In ISC 2002: pp 331–337.

[12] Tzong-Sun Wu , Chien-Lung Hsu, Kuo-Yu Tsai, Han-Yu Lin, Tzong-Chen Wu.Convertible multi-authenticated encryption scheme.Information Sciences 178 (2008): pp 256–263.

[13] L. Harn, T. Kiesler, New scheme for digital multisignature, IEE Electronics Letters 25 (15) (1989), pp. 1002–1003.

[14] F. Hou, Z. Wang, Y. Tang, Z. Liu, Protecting integrity and confidentiality for data communication, in: A. Puliafito, S. Papavassiliou (Eds.), Proceedings of Ninth IEEE International Symposium on Computers and Communications (ISCC), vol. 1, IEEE Computer Society, 2004, pp. 357–362.

[15] K. Ohta, T. Okamoto, A digital multisignature scheme based on the Fiat–Shamir scheme, in: H. Imai, R.L. Rivest, T. Matsumoto (Eds.), Advances in Cryptology – ASIACRYPT'91, Springer-Verlag, 1992, pp. 139–148.

[16] Wu Tzong-Chen, Chen Kui-Yu, Lin Zuo-Yi. An English auction mechanism for internet environment. ISC 2002, 2002, pp.331-7.

[17] Graham, Daniel A. and Marshall, Robert C. Collusive Bidder Behavior at Single-Object Second-Price and English Auctions. Journal of Political Economy, 1987,95(6),pp. 1237–1239.

[18] K. Viswanathan, C. Boyd, and E. Dawson, "A Three Phased Schema for Sealed Bid Auction System Design," in Proceedings of ACISP 2000 –Australasian Conference on Information Security and Privacy (E. Dawson, A.Clark, and C. Boyd, eds.), vol.

1841 of Lecture Notes in Computer Science, pp. 412–426, Springer- Verlag (Berlin), 2000.

[19] M. Franklin and M. Reiter, "The Design and Implementation of a Secure Auction Service," IEEE Transactions on Software Engineering, vol. 22, pp. 302–312, May 1996.

[20] Wang and H. Leung, Anonymity and Security in Continuous Double Auctions for Internet Retails Market, in the 37th Hawaii International Conference on Systems Sciences, 2004.