A Study on Electronic Auctions

by

Kazumasa OMOTE

submitted to
Japan Advanced Institute of Science and Technology
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

Supervisor: Associate Professor Atsuko Miyaji

School of Information Science
Japan Advanced Institute of Science and Technology

March, 2002

Abstract

An auction was originally a method to trade the special goods such as curios or antiques, which do not have a fixed price. In a wide interpretation, an auction is a kind of trade system in economic activities. We can see the various trade systems (auctions) in real world. For example, the trade of limited edition, stock trading, and a sale of personal computer are a kind of auction. An auction price would reflect a market price more clearly than a fixed price because it is decided by buyers. Many types of auctions are practiced in different situations.

During last decade, the Internet has rapidly spread, and thus it has quickened the growth of the trading on the Internet. The Internet allows a business to reach a large number of potential customers and suppliers in a shorter time and a lower cost. As a result, an auction business also expands rapidly on Internet (e.g. Yahoo auction[49]). An electronic auction has become a large system to trade any good. However, this rapid growth of electronic auction can cause different troubles. In realizing an electronic auction scheme, we need to consider from three points: bidder privacy, correctness of system, and efficiency.

In an electronic auction, it is important to satisfy anonymity for an authority in order to protect the information of who wants a good and a bidder's history of bidding. Such information may be bought and sold through illegal channels. Therefore, nobody should be able to gather the useful trading information with personal data. In anonymous bidding anybody should be able to verify the validity of a winner, while in secret bidding anybody should be able to verify the correctness of a winning bid. Furthermore, each bidder should be able to place a bid efficiently on Internet. In this thesis, we realize the following three kinds of auction schemes:

An English auction scheme: This scheme aims at both efficiency of bidding and anonymity of bidder. In an electronic English auction, efficiency of bidding is important because a bidder repeatedly places a bid in real time. Therefore the proposed scheme realizes the efficient bidding. Furthermore there is no single authority who can break anonymity of bidder.

A first-price sealed-bid (SB) auction scheme: This scheme aims at both a single auction manager and introducing a feature of entertainment. Many participants can enjoy the opening phase by decreasing winner candidates little by little. The cost of bids opening is more efficient compared with the other previous schemes. Anybody can publicly verify the auction results.

A second-price sealed-bid (SB) auction scheme: This scheme aims at secrecy of the highest bid with public verifiability. Secrecy of the highest bid should be satisfied in order to keep winner's privacy. Anybody can publicly verify that a winning bid is the second highest bid with keeping the highest bid secret.

Acknowledgments

I am most grateful to Associate Professor Atsuko Miyaji at Japan Advenced Institute of Science and Techology for her helpful comments and nice discussions for this work. I am grateful to Professor Tetsuo Asano, Professor Mineo Kaneko, Associate Professor Munehiko Hiraisih at Japan Advenced Institute of Science and Techology for their comments.

I am greatful to Professor Eiji Okamoto at Toho University, who gave me the opportunity to study in cryptography and encouragement. I would like to thank Associate Professor Hiroaki Kikuchi at Toukai University for his helpful discussion.

I greatly thank Associate Mitsuru Tada and Associate Masakazu Soshi for their much advice and helpful comments. I deeply thank Dr. Shigeki Kitazawa, Takeshi Okamoto, and Yuko Tamura for many discussions. I would wish to thank the colleagues at Miyaji laboratory. I would also with to thank all the people who supported my reseach.

Finally, I sincerely thank my parents, Kenji Omote, Chie Omote for their support and encouragement.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Auction

An auction was originally a method to trade the special goods such as curios or antiques, which do not have fixed price. In a wide interpretation, an auction is a kind of trade system in economic activities. We can see the various trade systems (auctions) in real world. For example, consider the trade of limited edition. The value of it may often go up little by little as time goes by. Such a good is traded in a high price. This style of trade is *English auction*. Nowadays the personal computer does not have the fixed price but the different reasonable price. The value of it often goes down little by little as time goes by. This style of trade is *Dutch auction*. An auction price would reflect a market price more clearly than a fixed price because it is decided by buyers. Also, consider the stock trading. The value of stock is unsettled and its trading price is decided by both buyer and seller. This trade style is both English auction and Dutch auction. When the stock is skyrocketing, its trade is English auction. On the other hand, when the stock is slumping, its trade is Dutch auction. That is why we can see various auctions in different situations.

English auction is the most familiar type. In an English auction, each bidder offers the higher price for a good one by one, and finally a bidder who offers the highest price gets a good in the highest price. In a Dutch auction, an auction manager (AM) reduces the price candidate for the good one by one, and a bidder who offers to accept the price for the first time gets a good. A first-price sealed-bid (SB) auction is that each bidder secretly submits a bid to the AM only once, and a bidder who offers the highest price gets a good. This style of auction is frequently used in nagotiation trading of construction work in Japan. These three kinds of auctions are comparatively popular.

On the other hand, an auction is also studied from the economic viewpoint, see, an adoption of *game theory*. A *second-price SB auction* was invented as an improvement of a first-price SB auction in 1961, which has a *dominant strategy* for bidding[48]. A second-price SB auction is that a bidder who offers the highest price gets a good in the second highest price. It is excellent from the economic viewpoints compared with a first-price SB auction. Furthermore, (M+1)st-price SB auction can simultaneously treat plural goods, and it is extension of the second-price SB auctoin. In the (M+1)st-price SB auction, the M highest bidders get goods in the (M+1)st highest bid price. Table 1.1 arranges three

Table 1.1: Auction types

	Public auction	Sealed-bid (SB) auction	
	English auction	First-price	Second-price
Bidding	Public	Secret	
Winner decision	Step by step	At once	
Winning bid	Highest		Second highest
Example	Stock trading in skyrocketing	Nagotiation trading of construction work	

kinds of auctions that we adopt.

During last decade, the Internet has rapidly spread, and thus it has quickened the growth of the trading on the Internet. The Internet allows a business to reach a large number of potential customers and suppliers in a shorter time and a lower cost. As a result, an auction business is rapidly expanded on Internet (e.g. Yahoo auction[49]). An electronic auction has become a large system to trade any good. However, this rapid growth of electronic auction can cause different troubles. We need to consider the following three points in realizing an electronic auction system.

Bidder privacy: In the case of on-line shopping over the Internet, a seller can store only the information about one buyer's purchase. However, in the case of electronic auction, a seller can store much information about many buyers' bidding because a lot of bidders participate in an auction to buy a good. If anonymity for an authority is not realized in an electronic auction, much information of who wants a good and a bidder's history of bidding is easily stored. Such information is valuable and can be easily gathered and selected. It may be bought and sold through illegal channels. For example, once a bidder participates in the expensive cosmetics auction, many direct mails (DMs) about different cosmetics may be sent to participants. Nobody should be able to gather the useful trading information with personal data.

Correctness of system: A bidder is anxious about the correctness of system. Generally, an electronic auction system uses a bulletin board on Internet like Yahoo auction. Nobody should be able to impersonate a certain bidder and all bids should be fairly dealt with. Futhermore, all bidders publicly should be able to confirm the results of auction on a bulletin board, which include a winning bid and a winner identity.

Efficiency: The computing ability of users is lower than that of AM. A bidder wants to quickly place a bid in an auction system. Also, it is not desirable that computing the reslts of auction takes too much time. So the light and speedy mechanism of auction is desired.

1.2 Desirable Properties

An electronic auction scheme should satisfy the following properties.

(a) **Anonymity:** Nobody including an authority can identify the loser bidders even after the opening phase.

(b) **Non-cancelability:** A winner cannot deny that she/he submitted the highest bid after the winner decision procedure. A winner is exactly identified.

(c) **Public verifiability:** Anybody can publicly verify that a winning bid is the highest value of all bids and publicly confirm whether a winner is valid or not.

(d) **Unforgeability:** Nobody can impersonate a certain bidder.

(e) **Robustness:** Even if a bidder sends an invalid bid, the auction process is unaffected.

(f) **Fairness:** All bids should be fairly dealt with.

(g) **Efficiency of bidding:** The computational and communicational amount in both bidding and verifying a bid is practical.

1.3 Basic Auction Protocol

A basic auction protocol has the following five procedures.

Initialization: The AM sets the system parameters and publishes them. Also, he publishes information about an auction (the namge of good, auction time, etc).

Bidder registration: A bidder sends the AM her/his public key to register.

Auction preparation: The AM computes the preparation data for each auction and a bidder may download her/his information for bidding.

Bidding: A bidder computes her/his bid information and places her/his bid.

Opening a winning bid: The AM computes only a winning bid with keeping the other bid secret. Note that a public auction (e.g. English auction) omits this procedure. Anyone can publicly verify the validity of a winning bid.

Winner decision: The AM identifies only a winner with keeping loser's anonymity. Anyone can publicly verify the validity of a winner.

1.4 Contribution of the Thesis

We realize the following three kinds of auction schemes.

Scheme I (see Chapter 4): We propose a practical English auction scheme, which has two authorities, the registration manager (RM) and the auction manager (AM). It satisfies the above seven properties, and additionally satisfies the following four properties:

(h) **One-time registration:** Any bidder can participate in plural auctions by only one-time registration. Even if a bidder is identified as a winner, she/he can participate in the next auction without repeating registration, maintaining anonymity for authorities.

(i) **Simple revocation:** A bidder can withdraw from an auction efficiently.

(j) **Unlinkability among plural auctions:** Nobody can link the same bidder's bids among plural auctions.

(k) **Linkability in an auction:** Anybody can link which bids are placed by the same bidder and knows how many times a bidder places a bid in an auction.

(ℓ) **Two independent authority's powers:** There is no single authority who can break anonymity and secrecy of bids.

This scheme solves two problems of the previous English auction scheme[31]. In the previous scheme, the computational and communicational costs for one bidding are much larger, and it is difficult to revoke a bidder. In an English auction, it is required to reduce the time in one bidding because a bidder repeatedly places a bid in real time, and the property of efficient revocation is important because a revocation of bidder is frequently conducted. Our English auction scheme uses two kinds of bulletin boards, and thus both of bidding and verification of bids are done quite efficiently and it is easy to revoke a bidder: the RM has only to delete a bidder from RM's bulletin board.

Scheme II (see Chapter 5): We propose an electronic first-price SB auction scheme, which satisfies the above basic seven properties, especially, realizing anonymity for a single AM. It also satisfies the following properties:

(m) **Secrecy of loosing bids:** The scheme should conceal all bids except for a winner. This property is desired in order to keep loser's privacy for the AM(s).

(n) **Entertainment:** Entertainment means that many bidders can enjoy the opening phase by decreasing winner candidates little by little.

(o) **Efficiency of opening:** The computational and communicational costs in bids opening bids is practical.

This auction scheme aims at strong anonymity of bidder. There exists only a single AM in this scheme and anonymity for a single AM is satisfied. Even after an auction the AM cannot know the loser's bid values directly. It also aims at entertainment without revealing loosing bids derectly though it opens only part of distribution of bids. Entertainment seen in a real English auction has not been discussed before. We introduce a new idea of entertainment to the opening phase by decreasing winner candidate little by little. Furthermore, our scheme realizes the efficient opening of bids like two previous scheme[5, 30].

Scheme III (see Chapter 6): We propose a second-price SB auction scheme, which satisfies the above seven basic properties and also satisfies the following properties:

(ℓ) **Two independent authority's powers:** There is no single authority who can break anonymity and secrecy of bids.

(m) **Secrecy of loosing bids:** The scheme should conceal all bids except for a winner. This property is desired in order to keep loser's privacy for the AM(s).

(o) **Efficiency of opening:** The computational and communicational costs in bids opening is practical.

(p) **Secrecy of the highest bid:** The scheme should not disclose the information about the highest bid value except that it is placed higher than the second highest bid value. This property is desired for winner's privacy.

We introduce three kinds of new techniques, the discriminant function of the p_0-th root, a verifiable w-th power mix, and a verifiable decryption mix, in order to realize secrecy of the highest bid with public verifiability. In a second-price SB auction, secrecy of bids are more important compared with a first-price one because each bid becomes the honest value for a bidder (this style of auction has a feature of incentive compatibility described in Section 6.2). Our electronic second-price SB auction scheme uses two kinds of AMs (AM1 and AM2) like the previous schemes[1, 30].

1.5 Overview of the Thesis

The thesis is organized as follows.

Chapter 2 gives notations and building blocks used in this thesis. It also summarize the signature based on a proof of knowledge (SPK), wihch gives several zero-knowledge proofs. Several techniques are realized by using such the SPKs for the sake of public verifiability.

Chapter 3 summarizes the previous electronic auction schemes, which include an English auction, a first-price SB auction and a second-price SB auction. We present three types of auctions, and describe five kinds of the previous concrete schemes and the drawbacks of them.

Chapter 4 investigates an English auction scheme. This scheme realizes efficient bidding for a bidder using two kinds of bulletin boards and the signature of knowledge. Also, our scheme realizes a practical English auction without using group signature.

Chapter 5 investigates a first-price SB auction scheme, which has only a single AM and realizes both perfect anonymity and entertainment of the opening phase. Such a single AM cannot break anonymity of bidders. Also, all participants can enjoy the opening of bids in an auction.

Chapter 6 investigates a second-price SB auction scheme. This scheme realizes secrecy of the highest bid with public verifiability. In order to satisfy both secrecy of the highest bid and public verifiability, we introduce the techniques the discriminant function of the p_0-th root, verifiable w-th power mix, and verifiable decryption mix. There is no single authority who knows the highest bid value, the identity of the second highest bidder, and loosing bid values.

Chapter 7 discusses three kinds of our proposed schemes from the viewpoints of several features, bidder privacy and correctness of a winning bid. We consider fairness of our

English auction scheme and the reasons why the second-price SB auction is unpopular.

Chapter 8 concludes this thesis and discusses the further research.

Chapter 2

Background

This chapter summarizes notations and building blocks. In this thesis, we use the following common notations.

I	:	the number of auction participants (bidders)
i	:	the index of bidders
$\mathcal{B}_i$	:	a bidder i ($i = 1, \ldots, I$)
AM	:	an auction manager
p, q	:	two large primes
$\mathbf{Z}_p$	:	a ring with p elements ($= \mathbf{Z}/p\mathbf{Z} = \{0, 1, \ldots, p-1\}$)
$\mathrm{ord}(g)$	:	order of an element g of a group
$\mathcal{H}()$	:	a collision resistant cryptographic hash function, $\{0,1\}^* \rightarrow \{0,1\}^k$, such as SHA-1[32] or MD5[39], where k is a security parameter (e.g. $k \approx 160$).

2.1 Dominant Strategy

The *dominant strategy* (optimal strategy) means that the best way for a player exists even if the other players take any strategy. If a bidder has the dominant strategy for bidding in an auction, she/he will follow the strategy faithfully without knowing other bidders' strategy. As a result, any bidder will satisfy the result of auction.

2.2 Bulletin Board System (BBS)

A bulletin board system (BBS) is a kind of public communication channel which can be read by anybody, but can be written only by an authority. An electronic auction such as Yahoo auction uses the BBS that is managed by an authority. In our schemes, the BBS publishes a pair of the bidder's names and the public keys, the data for a bidding preparation, the bidding data, the validity of auction results, and the computing process of bids. A bidder can easily download any data.

2.3 ElGamal Cryptosystem

An ElGamal cryptosystem is the primitive scheme based on the discrete logarithms problem (DLP) introduced by ElGamal[13]. Part of the security of the scheme actually relies on the Diffie-Hellman assumption, which implies the hardness of computing discrete logarithm[12].

Let p and q be large primes such that $q|p-1$. The key pair of a user in the ElGamal cryptosystem consists of a private key x (randomly chosen by the user) and the corresponding public key $y = g^x \pmod{p}$ for $g \in \mathbf{Z}_p$ with order q.

Given a message $m \in \mathbf{Z}_p$, encryption proceeds as follows: choose a random number $r \in \mathbf{Z}_q$ and generate the pair

$$E_y(m) = (G = g^r, M = my^r) \pmod{p}$$

as ciphertext. To decrypt the ciphertext $E_y(m)$, a user recovers the plaintext as

$$m = M/G^x \pmod{p},$$

using the private key x.

2.4 RSA Problem

RSA problem was introduced by Rivest, Shamir and Adleman[41]. Let n be a product such that $n = pq$. Given n, e and $y \pmod{n}$, it is infeasible to compute $x \in \mathbf{Z}$ such that $x^e = y \pmod{n}$.

2.5 Schnorr Signature Scheme

This signature scheme is introduced by Schnorr[44]. Assume that computing discrete logarithms is infeasible.

Let p and q be large primes such that $q|p-1$. The key pair of a user in the Schnnor signature consists of a private key x (randomly chosen by the signer) and the corresponding public key $y = g^x \pmod{p}$ for $g \in \mathbf{Z}_p$ with order q.

A pair $(c, s) \in \{0,1\}^k \times \mathbf{Z}_q$ satisfying $c = \mathcal{H}(g||y||g^s y^c||m)$ is a signature on a message $m \in \{0,1\}^*$. Schnorr signature scheme generates a signature on a message $m \in \{0,1\}^*$ by computing $t := g^r \pmod{p}$ for $r \in_R \mathbf{Z}_p$, $c := \mathcal{H}(g||y||t||m)$, and $s := r - cx \pmod{q}$. To verify a signature (c, s), anybody computes

$$c \stackrel{?}{=} \mathcal{H}(g||y||g^s y^c||m).$$

2.6 Signature based on a Proof of Knowledge (SPK)

We use the following four kinds of signatures based on s proof of knowledge (SPK) introduced by Camenish and Michels[7] as an anonymous signature scheme. These SPKs are based on the Schnorr signature scheme that is derived from an honest-verifier zero-knowledge proof of knowledge of the discrete logarithm.

2.6.1 Showing the knowledge of a discrete logarithm

This SPK is an adoption of a protocol for proving the knowledge of a discrete logarithm to the setting in which the group's order is unknown.

A pair $(c, s) \in \{0,1\}^k \times \mathbf{Z}_n$ satisfying $c = \mathcal{H}(g||y||g^s y^c||m)$ is a signature on a message $m \in \{0,1\}^*$ with respect to y, denoted

$$SPK[(\alpha) : y = g^\alpha](m).$$

An entity with a private key $x \in \mathbf{Z}_n$ such that $x = \log_g y$ can compute a signature $(c, s) = SPK[(\alpha) : y = g^\alpha](m)$ on a message $m \in \{0,1\}^*$ by computing $t := g^r \pmod n$ for $r \in_R \mathbf{Z}_n$, $c := \mathcal{H}(g||y||t||m)$, and $s := r - cx$. Then a set of (c, s) is verified by $c \stackrel{?}{=} \mathcal{H}(g||y||g^s y^c||m)$.

2.6.2 Showing the equality of two discrete logarithms

There exists the SPK for showing the equality of two logarithms in the case of which order of each base is unknown. A pair $(c, s) \in \{0,1\}^k \times \mathbf{Z}_n$ satisfying

$$c = \mathcal{H}(g_1||g_2||y_1||y_2||g_1^s y_1^c||g_2^s y_2^c||m)$$

is a signature on a message $m \in \{0,1\}^*$ with respect to y_1 and y_2, denoted

$$SPK[(\alpha) : y_1 = g_1^\alpha \wedge y_2 = g_2^\alpha](m).$$

Let $x \in \mathbf{Z}_n$ be a signer's private key with $y_1 = g_1^x$ and $y_2 = g_2^x$. Then a signature $(c, s) = SPK[(\alpha) : y_1 = g_1^\alpha \wedge y_2 = g_2^\alpha](m)$ on a message $m \in \{0,1\}^*$ can be computed as follows: compute $t_1 := g_1^r, t_2 := g_2^r$ for $r \in_R \mathbf{Z}_n$, $c := \mathcal{H}(g_1||g_2||y_1||y_2||t_1||t_2||m)$ and $s := r - cx$. Then a set of (c, s) is verified by $c \stackrel{?}{=} \mathcal{H}(g_1||g_2||y_1||y_2||g_1^s y_1^c||g_2^s y_2^c||m)$. Three or more equivalence of discrete logarithms can be shown as the SPK in the same way as the above.

2.6.3 Showing the knowledge of one out of two discrete logarithms

There exists the SPK for showing the knowledge of one out of two discrete logarithms in the case of which order of each base is unknown. A tuple $(c_1, c_2, s_1, s_2) \in \{0,1\}^k \times \{0,1\}^k \times \mathbf{Z}_n \times \mathbf{Z}_n$ satisfying $c_1 \oplus c_2 = \mathcal{H}(g_1||g_2||y_1||y_2||g_1^{s_1} y_1^{c_1}||g_2^{s_2} y_2^{c_2}||m)$ is a signature on a message $m \in \{0,1\}^*$ with respect to y_1 and y_2, and is denoted

$$SPK[(\alpha, \beta) : y_1 = g_1^\alpha \vee y_2 = g_2^\beta](m).$$

We assume that the signer knows $x \in \mathbf{Z}_n$ which $y_1 = g_1^x$. Then a signature $(c_1, c_2, s_1, s_2) = SPK[(\alpha, \beta) : y_1 = g_1^\alpha \vee y_2 = g_2^\beta](m)$ on a message $m \in \{0,1\}^*$ can be computed as follows:

- choose $r_1 \in_R \mathbf{Z}_n$, $r_2 \in_R \mathbf{Z}_n$ and $c_2 \in \{0,1\}^k$;
- compute $t_1 := g_1^{r_1}, t_2 := g_2^{r_2} y_2^{c_2}$ and $c_1 := c_2 \oplus \mathcal{H}(g_1||g_2||y_1||y_2||t_1||t_2||m)$; and

- set $s_1 := r_1 - c_1 x$ and $s_2 := r_2$.

In the case of signer's private key $x \in \mathbf{Z}_n$ with $y_2 = g_2^x$, the SPK is computed in the same way as the above. Then a set of (c_1, c_2, s_1, s_2) is verified by

$$c_1 \oplus c_2 \stackrel{?}{=} \mathcal{H}(g_1||g_2||y_1||y_2||g_1^{s_1} y_1^{c_1}||g_2^{s_2} y_2^{c_2}||m).$$

2.6.4 Combinational proof

There exists the SPK for showing the knowledge of one out of two discrete logarithms, which is equal to another discrete logarithm. A tuple $(c_1, c_2, s_1, s_2) \in \{0,1\}^k \times \{0,1\}^k \times \mathbf{Z}_n \times \mathbf{Z}_n$ satisfying $c_1 \oplus c_2 = \mathcal{H}(g_1||g_2||g_3||y_1||y_2||y_3||g_1^{s_1} y_1^{c_1}||g_3^{s_1} y_3^{c_1}||g_2^{s_2} y_2^{c_2}||g_3^{s_2} y_3^{c_2}||m)$ is a signature on a message $m \in \{0,1\}^*$ with respect to $y_1,\ y_2$ and z, denoted

$$SPK[(\alpha, \beta) : (y_1 = g_1^\alpha \wedge y_3 = g_3^\alpha) \vee (y_2 = g_2^\beta \wedge y_3 = g_3^\beta)](m).$$

We assume that the signer knows $x \in \mathbf{Z}_n$ such that $y_1 = g_1^x$ and $y_3 = g_3^x$ holds. Then a signature $(c_1, c_2, s_1, s_2) = SPK[(\alpha, \beta) : (y_1 = g_1^\alpha \wedge y_3 = g_3^\alpha) \vee (y_2 = g_2^\beta \wedge y_3 = g_3^\beta)](m)$ on a message $m \in \{0,1\}^*$ can be computed as follows:

- choose $r_1 \in_R \mathbf{Z}_n,\ r_2 \in_R \mathbf{Z}_n$ and $c_2 \in \{0,1\}^k$;
- compute $t_1 := g_1^{r_1}, t_2 := g_3^{r_1}, t_3 := g_2^{r_2} y_2^{c_2}, t_4 := g_3^{r_2} y_3^{c_2}$;
- $c_1 := c_2 \oplus \mathcal{H}(g_1||g_2||g_3||y_1||y_2||y_3||t_1||t_2||t_3||t_4||m)$; and
- $s_1 := r_1 - c_1 x$ and $s_2 := r_2$.

In the case of signer's private key $x \in \mathbf{Z}_n$ with $y_2 = g_2^x$, the SPK is computed in the same way as the above. Then a set of (c_1, c_2, s_1, s_2) is verified by

$$c_1 \oplus c_2 \stackrel{?}{=} \mathcal{H}(g_1||g_2||g_3||y_1||y_2||y_3||g_1^{s_1} y_1^{c_1}||g_3^{s_1} y_3^{c_1}||g_2^{s_2} y_2^{c_2}||g_3^{s_2} y_3^{c_2}||m).$$

2.7 Group Signature

The concept of group signature was introduced by Chaum and van Heyst[10]. Group signature allows any member to sign on behalf of a group and keeps the member identity secret. The scheme[9] is the first efficient group signature schemes in that the size of both group's public key and of signatures are independent of the number of group members and that a group's public key remains unchanged if a new member is added to a group. Later, group signature schemes with improved performance and better flexibility are proposed in [2, 7, 8, 20]. An authority in a group signature scheme is usually divided into two parties, group manager (GM) and escrow manager (EM) by using an idea of identity escrow[20]. In such a scheme, we assume that these two authorities do not collude together.

2.7.1 Protocol

Setup: Let Y, x_i, x_G, x_E, m, and σ_i be the group public key, member M_i's private key, GM's private key, EM's private key, a message, and a signature of M_i.

Sign: For m, x_i, and Y, M_i generates a signature σ_i.

Verify: For a verification algorithm Verify, $\mathsf{Verify}(m, \sigma_i, Y) = 1$ if and only if σ_i was generated by M_i.

Tracing: For σ_i, m, x_E and Y, EA returns the identity ID_i of M_i.

2.7.2 Security requirements

Unforgeability of signatures: Only group members are able to sign messages, which can be traced by the EM.

Anonymity of signatures: It is infeasible to find out the member who signed a message without knowing EM's private key.

Unlinkability of signatures: It is infeasible to decide whether two signatures have been issued by the same member or not.

No framing: Nobody can impersonate non-involved members.

2.8 Hash Chain Technique

We use a hash chain technique introduced by Rivest and Shamir[40]. A hash chain is computed by the following rule:

$$\mathcal{H}^k(r) = \mathcal{H}(\mathcal{H}^{k-1}(r)),$$

where r is a random number and k is the number of hash computing. If r is not known, computing $\mathcal{H}^j(r)$ for $j < k$ is infeasible even though $\mathcal{H}^k(r)$ is known.

2.9 Verifiable ElGamal Encryption and Decryption

We can prove that $E_y(m) = (G = g^r, M = my^r)$ is an encryption of m without revealing r by showing

$$SPK[(\alpha) : G = g^\alpha \wedge M/m = y^\alpha](m),$$

and that $m = M/G^x$ is the decryption of $E_y(m) = (Gg^r, M = my^r)$ without revealing x by showing

$$SPK[(\alpha) : M/m = G^\alpha \wedge y = g^\alpha](m).$$

Chapter 3

Previous Electronic Auction Schemes

We summarize three kinds of electronic auctions. In an electronic auction, it is important to spoil the collusion of bidders, because Internet makes the formation of ring members much easier[25]. Therefore anonymity plays an important role in spoiling the collusion of bidders. It is also important to satisfy anonymity for an authority in order to protect the information of who wants a good and a bidder's history of bidding. Such information may be bought and sold through illegal channels. In an anonymous bidding anybody should be able to verify the validity of a winner, while in a secret bidding anybody should be able to verify the correctness of a winning bid.

3.1 English Auction Schemes

3.1.1 Background

An English auction is the most familiar type of auctions. In an English auction, each bidder offers the higher price one by one, and finally a bidder who offers the highest price gets a good. It has the following features:

1. A bidder easily knows the market price position and trend for a good through the auction (good point).
2. The competition principle well works, and thus a winning bid value reflects a market price (good point).
3. A bidder has the dominant strategy (see Section 2.1) for bidding, which places a little higher than a current bid value (good point).
4. Much time is required to decide a winner (bad point).
5. Much information of the market price is disclosed because all bid values are published. (bad point).
6. The auction has a feature of entertainment. Many participants can enjoy in the price-decision process (good point).

An English auction is used on the Internet as well as the real world. An electronic auction is used in several situations like Yahoo auction[49]. Yahoo auction adopts an English auction. First of all, the computational and communicational costs for one bidding should be efficient in an electronic English auction. Since a bidder repeatedly places a bid in real time, it is required to reduce the time in one bidding. Also, a winner should not be able to cancel her/his bidding. If a winner cancels that she/he did, the highest bid is insignificant.

3.1.2 Overview

Several studies on English auction[25, 26, 28, 31, 35, 37, 38, 46] have been reported. The timing when each bidder sends a bid in real-time electronic English auction is considered[38]. [25, 28] do not concern with the security aspect of public auctions but describe those different methods. [26] proposed an English auction scheme and solves the problem of [35] that public verifiability of a winner is not realized, applying hash chains technique (see Section 2.8). [46] also proposed an English auction scheme using hash chains technique as a bid, which is similar to multiple sealed-bid biddings in order to satisfy fairness. When a bidder participates in an auction, it has two advantages that a valid bidder can place a bid many times by using only one-time signature and that bidder fairness is satisfied for a non-trusted authority. However, in this scheme, the following two problems exist:

1. Anonymity of bidder is not satisfied for the AM after each bidding because the AM knows the bidder's identity.

2. The bidding points are set up discretely. For K bidding points, it is necessary for a bidder to compute hash functions K times. Apparently each bidder cannot place a bid as she/he likes. Many bidding points are desired because a bidder places a bid many times in an English auction.

The scheme[31] also realizes an English auction, which is described in the next section. It is similar to our English auction scheme, in that they use two authorities.

3.1.3 NT-scheme

This auction scheme[31] introduced by Nguyen and Traoré applies a group signature scheme (see Section 2.7) to an English auction. In an English auction, a group manager (GM) in a group signature scheme works as the AM and a group member corresponds to a bidder. When a bidder places a bid, she/he generates a group signature on a bid. The validity of signature can be verified easily by any participant using a group public key, but any participant does not know who places the bid. An escrow manager (EM) works to identify a winner at every auction. In this section, we summarize the NT-scheme and discuss some drawbacks. We illustrate the overview of the NT-scheme in Figure 3.1.

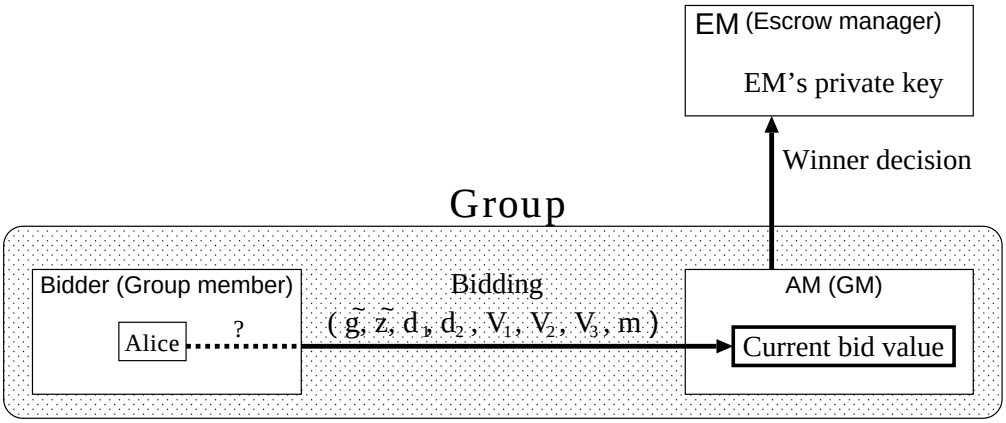


Figure 3.1: Overview (NT-scheme)

Protocol

This scheme introduces group signature scheme, and thus AM and EM do not collude together.

Initialization: The AM computes an RSA modulus n, where n is the product of two primes, an RSA key pair (e, d), a cyclic group $G = \langle g \rangle$ of order n over the finite field $\mathbf{Z}_p$ for a prime p, an element $a \in \mathbf{Z}_n^*$ that is of the order $\phi(n)/4$, and an upper bound λ on the length of the private keys: the EM chooses $h \in G$ with order n, computes ElGamal-encryption key pair $(\rho,\ Y_E(= h^\rho)) \in \mathbf{Z}_n \times G$, and sets a constant $b \neq 1$. The group public key is $\mathcal{Y} = (n, e, G, g, a, b, \lambda, h, Y_E)$. AM's private key is d and EM's private key is ρ.

Bidder registration: Alice randomly generates a private $x \in \{0, \cdots, 2^\lambda - 1\}$ and sends the value $y = a^x \pmod n$ and $z = g^y$ to the AM; the AM returns $v = (y + b)^d \pmod n$. Note that the AM cannot see the value of x.

Bidding: In order to put a bid m with her signature, she computes the following values $(\tilde{g}, \tilde{z}, d_1, d_2, V_1, V_2, V_3)$:

- $\tilde{g} = g^r$ and $\tilde{z} = \tilde{g}^y$ for $r \in_R \mathbf{Z}_n$;
- $d_1 = {Y_E}^u g^y$ and $d_2 = h^u$ for $u \in_R \mathbf{Z}_n$;
- $V_1 = SPK[(\gamma, \delta) : \tilde{z} = \tilde{g}^\gamma \wedge d_2 = h^\delta \wedge d_1 = {Y_E}^\delta g^\gamma](m)$;
- $V_2 = SPK[(\beta) : \tilde{z} = \tilde{g}^{a^\beta}](V_1)$;
- $V_3 := SPK[(\alpha) : \tilde{z}\tilde{g}^b = \tilde{g}^{\alpha^e}](V_2)$

Assume that computing the discrete logarithm, the double discrete logarithms and the e-th root of the discrete logarithm is infeasible. The concrete algorithm for these signatures is referred to [7, 9]. Alice's group signature consists of a set of $(d_1, d_2, V_1, V_2, V_3)$. If the signature (V_1, V_2, V_3) is valid, anyone confirms that (d_1, d_2) is an encryption of z by using ElGamal encryption function with EM's public key Y_E, and that Alice knows her private key x and her membership certificate v.

Winner decision: The EM restores (d_1, d_2) using his private key ρ and identifies a member Alice from z because he knows the correspondence of z to member's identity.

In this scheme, the signature V_3 is slightly modified using a verifiable group signature sharing scheme in order to satisfy anonymity of bidder.

Drawbacks

This scheme satisfies the basic seven properties except for efficiency of bidding. There exist some problems as follows.

Efficiency of bidding: In applying a group signature to an electronic auction, it is necessary to generate or verify a signature on each bid. A signature generation or verification corresponds to bidding or verification of bids respectively, both of which are required in each bidding. However the computational cost for both signature generation and verification is rather large. Therefore it is not realistic to apply directly a group signature to an electronic auction.

Revocation of Bidder: In an Electronic auction, a revocation of bidder is frequently conducted when a bidder wants to withdraw from an auction or the AM wants to revoke a certain bidder. So revocation-procedure should not be complicated. However, in the previous scheme, it is rather difficult to revoke a bidder because a membership certificate has been distributed to each bidder indicated in [3]. Even in the case of [4] or [21], although they realize a revocation of bidders, the computational cost depends on the number of revoked numbers or each bidder must renew her/his key in each revocation of member, respectively.

3.2 A First-price SB Auction Schemes

3.2.1 Background

In an English auction, the competition principle well works, but much time is required in order to decide a winner. In the SB auction, each bidder secretly submits a bid to the AM only once, and a bidder who offers the highest price gets a good. Compared with an English auction, a winner is decided more efficiently. So the SB auction decides the price more efficiently than an English auction. It has the following features:

1. Any bidder cannot know the market price position and trends. So a winning bid may be much higher than a market price (bad point).

2. The competition principle does not works well, and thus a winning bid price may be lower than the market price for a good (bad point).

3. A bidder does not have the dominant strategy for bidding. So many bidders may try to steal and estimate the other bid values (bad point).

4. It is efficient to decide a winner because each bidder places a bid only once (good point).

Figure 3.2: Secret computing (First-price)

5. Since the bid values except for a winning bid are not revealed, this auction protects losers' privacy (good point).

6. The auction does not have a feature of entertainment. A winning bid is decided at once (bad point).

Recently, an electronic first-price SB auction is introduced in negotiation trading of construction work in Japan. Since this auction sets plenty interval of bidding, each bidder can place a bid fairly. In a first-price SB auction, it is easy to realize fairness. This is why many electronic first-price SB auction schemes are investigated. In an electronic first-price SB auction scheme, it is important to conceal the loosing bids even after an acution because of keeping bidder's privacy. However, each bidder wants to check whether or not the published result of a winning bid is the highest of all bids. Therefore, it needs the secret computing with public verifiability shown in Figure 3.2, which outputs only the highest bid value. Any bidder can publicly verify that the winning bid is the highest bid in an auction.

3.2.2 Overview

Sealed-bid auctions are often investigated[5, 14, 16, 19, 23, 24, 29, 30, 34, 36, 42, 43, 47]. We note that all electronic auction aims at efficiency but not a feature of entertainment. For anonymity, a bid[14, 15, 19] or the opening function[42] is distributed among plural AMs by using the secret sharing technique[45]. In this technique, however, anonymity on the correspondence of a bidder to a bid should leak out by a dealer[14, 42] or a collusion of the AMs forming a quorum[15, 19]. Usually plural AMs require more communication cost[14, 15, 19] or more computation amount[42]. Although the schemes[16, 29] realize anonymity for the AM, all bids are opened after the bidding phase. These schemes do not satisfy secrecy of loosing bids at all. On the other hand, the schemes[24, 23, 43, 47] do not realize anonymity for the AM. The previous schemes[5, 30] use two kinds of auction managers (AM). However the scheme[5] does not realize anonymity for a single AM and discloses a order of all bids for the AM.

Bidding points are usually set up discretely in advance in order to realize secrecy of loosing bids [5, 15, 19, 23, 30, 42, 43, 47]. A one-way hash function instead of a public key cryptosystem is used by introducing the hash chain technique (see Section 2.8), which exceedingly decrease the computational complexity[23, 47]. However, unfortunately the size of representation of bids directly depends on the number of bidding points[19, 23, 43, 47]: for K bidding points, the size of the representation of bids is just K. Therefore the more bidding points are set up, the more communication or computation amount is

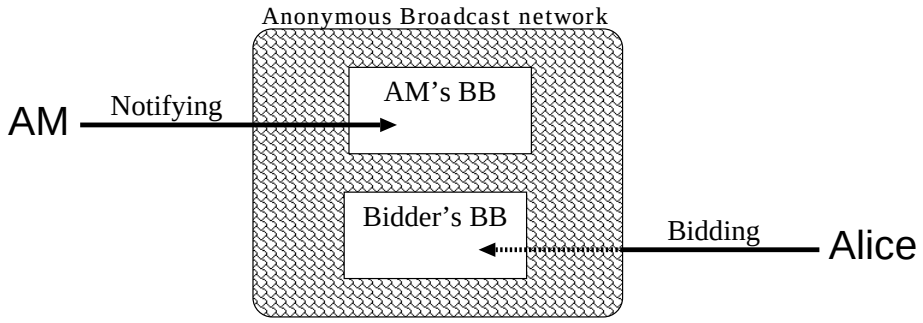


Figure 3.3: Overview (NFW-scheme)

required in the bidding or opening phase. Two previous schemes[5, 30] has a fairly efficient opening phase: for K bidding points, the size of the representation of bids is just $\log_2 K$.

On the other hand, a bid is efficiently represented as an encryption of a known message[42], which does not depend on the number of bidding points. Therefore it improves the representation of bids. However it costs much computation time in the opening phase: the decryption of ElGamal or RSA cryptosystems depends on $O(IK)$ until the winning bids are decided, where I and K are the number of bidders and the number of bidding points, respectively. Apparently it is not suited for handling many bidders and many bidding points.

We show two previous schemes: the NFW-scheme in that anonymity for a single AM is satisfied, the KMSH-scheme in that loosing bids is secret and the opening cost is efficient.

3.2.3 NFW-scheme

This auction scheme[29] introduced by Nakanishi, Fujiwara and Watanabe realizes a first-price SB auction. This scheme relies on anonymous broadcast network between the AM and $\mathcal{B}_i$, applies an undeniable signature scheme to bidding, and thus satisfies anonymity for a single AM. In this section, we summarize the NFW-scheme and discuss some drawbacks. We illustrate the overview of the NFW-scheme in Figure 3.3.

Protocol

Initialization: The AM constructs an anonymous broadcast network for an auction. There is some BBSs on network.

Registration: A verification key of a signature generated by each participant is published. The correspondence of the verification key to the owner is known to everyone on the network.

Auction preparation: The AM makes M_A which specifies the goods and period of auction and selects ID_A which identifies an auction. The AM computes his signature $Sig_{AM}(M_A||ID_A)$. Then the AM publishes $M_A||ID_A||Sig_{AM}(M_A||ID_A)$.

Bidding: Alice ($\mathcal{B}_i$) computes $\mathcal{H}(price_i||r_i)$ for her bid price $price_i$, using a secret random number r_i. $\mathcal{B}_i$ also computes $USig_i(ID_A||\mathcal{H}(price_i||r_i))$ as her undeniable signature.

Then $\mathcal{B}_i$ publishes

$$\mathcal{H}(price_i||r_i)||USig_i(ID_A||\mathcal{H}(price_i||r_i)).$$

The undeniable signature scheme prevents repudiation of a bid and pretence by other bidders. The AM makes M_{p1} that specifies the period in which the bidders must reveal the contents of their hash values. The AM publishes $M_{p1}||Sig_{AM}(M_{p1})$. During the period, $\mathcal{B}_i$ publishes

$$price_i||r_i||\mathcal{H}(price_i||r_i)||USig_i(ID_A||\mathcal{H}(price_i||r_i))$$

named the revealed bid. The AM checks whether each revealed bid is valid or not.

Opening winning bid and winner: The AM determines the highest bid $price_j$ of $\mathcal{B}_j$ among all revealed bids with correct hashed value. The AM makes M_{p2} that specifies the period in which the bidder offering $price_j$ must reveal her/his name. The AM publishes

$$price_j||M_{p2}||Sig_{AM}(price_j||M_{p2}).$$

During the period, $\mathcal{B}_j$ offering $price_j$ publishes her/his identifier, ID_j, with the non-interactive proof for the confirmation protocol of her/his undeniable signature in her bid and the non-interactive proofs for the disavowal protocols of the undeniable signatures in the other bids. The confirmation protocol ensures that she/he casts the bid with $price_j$, and the disavowal protocols ensure that the bid is her/his only one in the bidding phase.

Drawbacks

This scheme satisfies the basic seven properties. But there exist some problems as follows.

Secrecy of loosing bids: All bids are revealed after an auction is closed. So this scheme does not satisfies secrecy of loosing bids at all. In the SB auction, it is important to conceal the loosing bids as many as possible even after the auction in order to protect a bidder privacy.

Efficiency of opening: A winner must compute the undeniable signatures proportional to I, where I is the number of bidders. A user unlike the AM does not usually have a powerful computing machine. So the computational cost of a winner is rather large.

3.2.4 KMSH-scheme

This auction scheme[23] introduced by Kobayashi, Morita, Suzuki and Hakuta also realizes a first-price SB auction. This scheme realizes an efficient auction by introducing a hash chain technique (see Section 2.8). This scheme satisfies secrecy of loosing bids. In this section, we summarize the KMSH-scheme and discuss some drawbacks. We illustrate the overview of the KMSH-scheme in Figure 3.4.

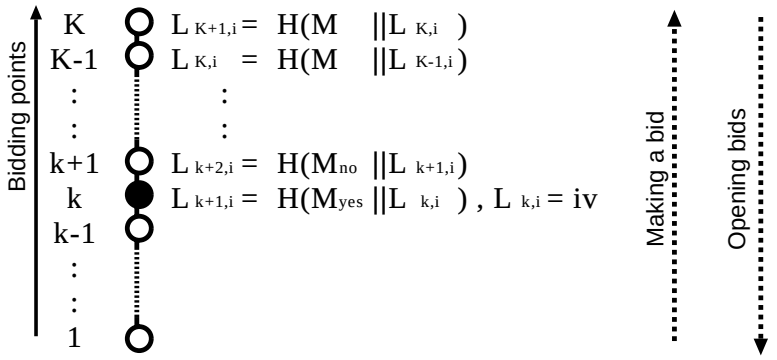


Figure 3.4: Overview (KMSH-scheme)

Protocol

Initialization: The AM sets the hash function $\mathcal{H}$.

Bidder registration: A bidder Alice ($\mathcal{B}_i$) genarates her private key x_i and her public key y_i, and sends y_i and ID_i to the AM. The AM registers ID_i and y_i together in his database. At the same time, the AM sends his signature $Sig_{AM}(y_i)$ to $\mathcal{B}_i$.

Auction preparation: The AM sets the bidding points $\{v_1, \ldots, v_K\}$ and publishes two kinds of messages M_{yes} and M_{no}.

Bidding: Let $\mathcal{B}_i$'s bid value and $\mathcal{B}_i$'s real ID be $v_k \in \{v_1, \ldots, v_K\}$ and ID_i, respectively. $\mathcal{B}_i$ computes the values of hash chain and her signature:

$$L_{k,i} = iv,\ L_{k+1,i} = \mathcal{H}(M_{yes}||L_{k,i}),\ L_{k+2,i} = \mathcal{H}(M_{no}||L_{k+1,i}), \cdots,$$
$$L_{K,i} = \mathcal{H}(M_{no}||L_{K-1,i}),\ L_{K+1,i} = \mathcal{H}(M_{no}||L_{K,i}).$$

$\mathcal{B}_i$ sends $\{L_{K+1,i}, Sig_i(L_{K+1,i}), y_i, Sig_{AM}(y_i)\}$ to the AM, and then these are published.

Opening winning bid and winner: The AM conducts the following steps.

Step 1: The AM lets t be K.

Step 2: The AM inquires of all bidders whether they placed a bid v_t.

Step 3: If no bidder declares, the AM sets t to $t-1$ and returns to Step 2. If the bidder $\mathcal{B}_j$ (Alice) declares that she places a bid v_t, all bidders $\mathcal{B}_i$ $(i = 1, \ldots, I)$ send $L_{t,i}$ to the AM and go to Step 4.

Step 4: The AM verifies the equality of

$$L_{n+1,j} \stackrel{?}{=} \mathcal{H}(M_{no}|| \cdots ||\mathcal{H}(M_{no}||\mathcal{H}(M_{yes}L_{k,j})) \cdots),$$

and

$$L_{n+1,i} \stackrel{?}{=} \mathcal{H}(M_{no}|| \cdots ||\mathcal{H}(M_{no}||\mathcal{H}(M_{no}L_{k,i})) \cdots).$$

Step 5: If all the results in Step 4 are valid, the AM declares that a winning bid price v_t and the winner is $\mathcal{B}_j$.

Drawbacks

This scheme satisfies the basic six properties except for anonymity and efficiency of bidding. There exist some problems as follows.

Anonymity: This scheme is not realized anonymity for the AM.

Efficiency of bidding: The computational and communicational costs for a bidding are of the order of $O(K)$.

Efficiency of opening: The computational and communicational costs for an opening phase are of the order of $O(K)$.

3.3 A Second-price SB Auction Schemes

3.3.1 Background

In a first-price SB auction, a bidder does not have the dominant strategy. So a winning bid may be much higher or much lower. By improving a first-price SB auction, W. Vickrey proposed a second-price SB auction and won the Nobel Economics Prize in 1961[48]. In this style of auction, a bidder who offers the highest price gets a good in the second highest price. This style of auction has the *incentive compatibility* (see Section 6.2), in which the dominant strategy for each bidder is to place a bid honestly her/his own true value[48]. So a winning bid reflects a market price better than a first-price SB auction. Therefore this style of auction solves the problems of both an English auction and a first-price SB auction. It has the following features:

1. A winning bid price reflects a market price as well as English auction because of incentive compatibility (good point);
2. A bidder has the dominant strategy for bidding (good point).
3. It is efficient to decide a winner because each bidder places a bid only once (good point).
4. Since the bid values except for a winning bid are not revealed, this auction protects losers' privacy (good point).
5. A second-price SB auction does not have entertainment. A winning bid is decided at once (bad point).

Since this auction sets plenty time of bidding like a first-price SB auction, each bidder can place a bid fairly. It is easy to realize fairness in this auction. However, because of incentive compatibility, any bidder does not want to disclose her/his bid value compaired with a first-price SB auction. That is why the secret computing shown in Figure 3.5 is more necessary for a second-price SB auction than a first-price one. If the highest bid value is not revealed in this auction, it is difficult to confirm whether or not a winning bid is the second highest bid. Therefore, in the secret computing of the second highest value, the auction should realize public verifiability of a winning bid . Also, it is important to conceal the loosing bids because of keeping bidder's privacy like a first-price SB auction.

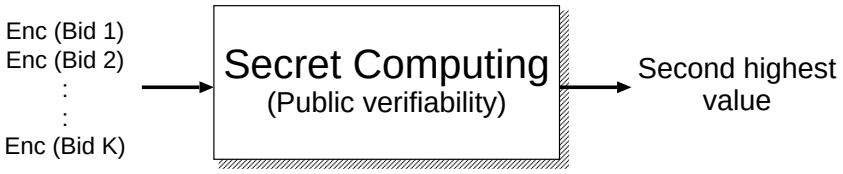


Figure 3.5: Secret computing (Second-price)

3.3.2 Overview

We overview several studies[1, 15, 18, 30, 33] as a second-price SB auction. These schemes set the bidding points discretely. [15] realize a second-price SB auction, in which the bidding points are represented by polynomials that are shared by plural AMs. In this scheme, each bidder must communicate with plural AMs to place a bid. [30] realizes some kinds of the SB auctions (i.e. a first-price SB auction, a second-price SB auction, the (M+1)st-price SB aution, etc.) using two auction managers AM1 and AM2, which applies the oblivious transfer. But this scheme does not satisfy public verifiability of both the winner and the winning bid. [18] realizes the (M+1)st-price SB auction using a verifiable secret sharing technique, where the bidding point is represented by the degree of a polynomial shared by the number of AMs m. In his scheme, there exist some drawbacks: (1) this scheme has a undesirable condition that m is larger than the number of bidding points, so it is difficult to set many bidding points; (2) anyone can anonymously disturb an auction by submitting an invalid bid. These problems are solved in our scheme. [1] proposed the (M+1)st-price SB auction using homomorphic encryption and mix and match technique[17]. This scheme realizes public verifiability of a winner and the winning bid using an auction manager and a trusted authority. However, However, each bidder must compute K+1 zero-knowledge proofs in bidding, where K is the number of bidding points.

3.3.3 NPS-scheme

This auction scheme[30] introduce by Naor, Pinkas and Sumner realizes a second-price SB auction using two kinds of auction managers, which applies the oblivious transfer. In their scheme, the bid representation is of $O(\log K)$ for the number of bidding points K. In this section, we summarize the NPS-scheme and discuss some drawbacks. We illustrate the overview of the NPS-scheme in Figure 3.6.

Protocol

This scheme has two kinds of auction managers AM1 and AM2.

Auction preparation: The AM1 generates programs for computing a winning bid and publishes a public key encryption E_1. Then the AM1 publishes $c = g^r (\mathrm{mod}\ p)$ (p is a prime, r is a random secret number, and g is a basepoint on which the DLP is hard), and keeps the two kinds of bidder $\mathcal{B}_i$'s values $m^0_{i,j}, m^1_{i,j}$ $(j = 1, \ldots, \lambda)$ secret.

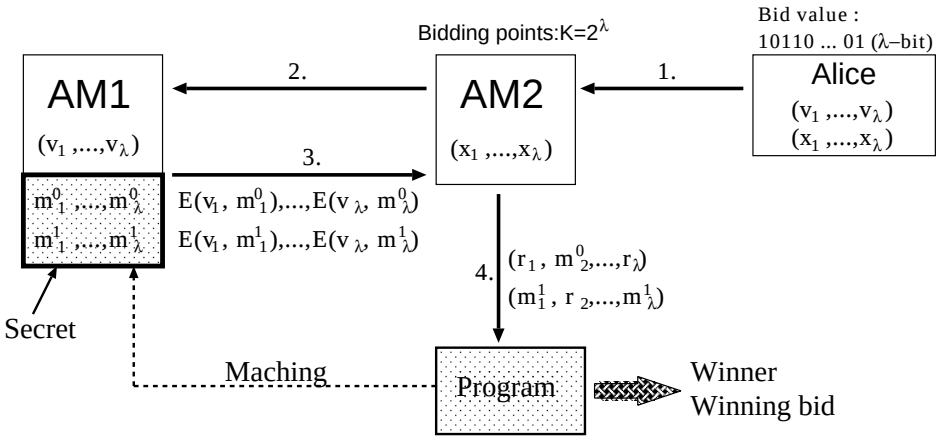


Figure 3.6: Overview (NPS-scheme)

Note that the values $m^0_{i,j}$ and $m^1_{i,j}$ mean the bit 0 and 1 for bid value, respectively. The AM2 sets $K = 2^\lambda$ bidding points.

Bidding: When $\mathcal{B}_i$ places a bid, each $\mathcal{B}_i$ follows a 1-out-of-2 proxy oblivious transfer protocol for each bit of her/his bid. The bid value is expressed by binary numbers. $\mathcal{B}_i$ selects her/his secret keys $\{x_{i,1}, \ldots, x_{i,\lambda}\}$, and sends both a set of $\{x_{i,1}, \ldots, x_{i,\lambda}\}$ to the AM2 and a set of $\{E_1(g^{\alpha_{i,1}}), \ldots, E_1(g^{\alpha_{i,\lambda}})\}$ to the AM1, where $\alpha_{i,j}$ is either $x_{i,j}$ or $r - x_{i,j}$. If $\alpha_{i,j} = x_{i,j}$ holds, the j-th bit of $\mathcal{B}_i$'s bid is 0. If $\alpha_{i,j} = r - x_{i,j}$ holds, the j-th bit of $\mathcal{B}_i$'s bid is 1.

Opening winning bid and winner: The AM2 forwards $\{E_1(g^{\alpha_{i,j}})\}$ to the AM1, and the AM1 decrypts them to $\{g^{\alpha_{i,j}}\}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, \lambda$. Note that the AM1 cannot know the value of $\alpha_{i,j}$. The AM1 sends $(g^{s_j},\ g^{\alpha_{i,j}s_j} \oplus m^0_{i,j},\ (c/g^{\alpha_{i,j}})^{s_j} \oplus m^1_{i,j})$ to the AM2 (s_j is a random number) for $i = 1, \ldots, n$ and $j = 1, \ldots, \lambda$. Although the AM2 attempts to restores both $m^0_{i,j}$ and $m^1_{i,j}$ using $x_{i,j}$ $(j = 1, \ldots, \lambda)$ for $\mathcal{B}_i$, either $m^0_{i,j}$ or $m^1_{i,j}$ is valid. Note that the AM2 cannot know which value is rightfully decrypted. Then the AM2 inputs the decrypted values $m^0_{i,j}$ or $m^1_{i,j}$ $(i = 1, \ldots, n$ and $j = 1, \ldots, \lambda)$ to a program , which is made by the AM1 and outputs both a winner and a winning bid (the second highest bid).

In this scheme, there is no single entity who knows the second highest bid value, a bidder $\mathcal{B}_{sec}$, and loosing bid values.

Drawbacks

This scheme satisfies the basic seven properties except for public verifiability. There exist some problems as follows.

Public verifiability: As mentioned in the opening phase, the AM2 uses a program that the AM1 made. It is difficult to verify the outputs of program because he does not know which value of $\{m^0_{i,j}, m^1_{i,j}\}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, \lambda$ is used in a

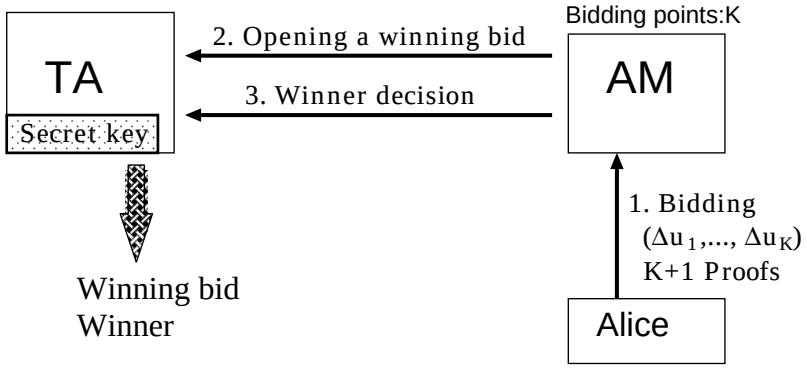


Figure 3.7: Overview (AS-scheme)

program. Nobody can verify whether the AM1 has made a faulty program or not. In fact, the following injustice could be done by the AM1.

- The program can output the winning bid higher than the second highest bid value because a program knows the highest bid value. It can output the false winning bid. Nobody can tell whether the winning bid is false or not.
- The AM1 colludes with a bidder $\mathcal{B}_i$, and the AM1 makes a faulty program that $\mathcal{B}_i$ always becomes a winner. A program always makes $\mathcal{B}_i$ a winner because $\mathcal{B}_i$'s bid is not opened even if $\mathcal{B}_i$ is not a winner. Nobody can tell whether the winner is false or not.

Although this scheme may introduce the cut-and-choose technique in order to satisfy verifiability of the output, its cost is much required in that π times execution of the protocol is needed where π is the security parameter of cut-and-choose ($k \simeq 64$). This execution is not practical because all bidders need to check whether $\pi/2$ times execution is valid or not. The valid probability of the protocol after $\pi/2$ times execution is $(1/2)^{\pi/2}$ in average.

3.3.4 AS-scheme

This auction scheme[1] introduced by Abe and Suzuki realizes the (M+1)st-price SB auction using homomorphic encryption and mix and match technique[17]. This scheme can apply to the second-price SB auction by setting $M = 1$. We illustrate the overview of the AS-scheme in Figure 3.7.

Protocol

There are bidders $\mathcal{B}_1, \ldots, \mathcal{B}_I$, the auction manager AM, and the trusted authority TA.

Initialization: The TA generates a secret key and a public key of ElGamal cryptosystem that each bidder uses in the bidding phase and publishes a generator $z \in \mathbf{Z}_p$ of the cyclic group used for the encryption.

Auction preparation: The AM sets the bidding points $\{1, \ldots, K\}$ for the good of auction and publishes the bidding points.

Bidding: A bidder Alice chooses her bidding point $k_i \in \{1, \ldots, K\}$, and then computes the corresponding bid vector:

$$\Delta v_{i,k} = \begin{cases} E(z) & \text{if } k = k_i \\ E(1) & \text{if } k \neq k_i \end{cases} \qquad (1 \leq k \leq K).$$

which conceals the bid value by ElGamal encryption E. Furthermore, she must construct the proofs of both $\prod_{k=1}^{K} v_{i,k} = E(z)$ and $\Delta v_{i,k} = \{E(1), E(z)\}$ $(k = 1, \ldots, K)$. When a bidder $\mathcal{B}_i$ places a bid, she sends her bid vector and the proofs.

Opening a winning bid: The AM computes and publishes the following values:

$$v_{i,k} = \Delta v_{i,k},\ v_{i,k-1} = \Delta v_{i,k-1} v_{i,k},\ \cdots,\ v_{i,1} = \Delta v_{i,1} v_{i,2} \qquad (i = 1, \ldots, I),$$

and

$$V_k = v_{1,k} \cdots v_{I,k} \qquad (k = 1, \ldots, K).$$

By using the following homomorphic property for each bidding point k,

$$V_k = \overbrace{E(z) \cdots E(z)}^{b} \overbrace{E(1) \cdots E(1)}^{I-b} = E(z^b).$$

Suppose that I is the number of bidders and b is the bidding number in the bidding point k. The TA can publicly show whether $D^*(E(z^\lambda)) \in \{1, z, z^2, \ldots, z^I\}$ or not by using the mix and match technique, where D^* is a verifiable ElGamal decryption. Note that only the TA knows the value $D^*(E(z^\lambda))$. If $D^*(E(z^\lambda))$ is z^b, b bidders place a bid in the bidding point k. The AM finds the highest bidding point k_{win} (a winning bid value) so that $D^*(E(z^\lambda))$ might be z^{M+1}, where M is the number of winners. The AM publishes the winning bid value.

Winner decision: The AM sends $v_{i,k_{win}+1}$ $(i = 1, \ldots, I)$ to the TA, and then the TA decrypts $v_{i,k_{win}+1}$ $(i = 1, \ldots, I)$ and finds M winning bidders with $D^*(v_{i,k_{win}+1}) = z$. Finally, the AM publishes the winners.

The TA can know any bidder's bid value by decrypting the bid vector. In order to conceal the bid values for the TA, this scheme may share the secret key among plural authorities by using a secret sharing technique.

Drawbacks

Since a bidder must send either E(1) or E(r) as the element of bid vector, each bidder must compute K+1 zero-knowledge proofs that each element in bid vector is whether E(1) or E(r). So the computational cost for a bidder gets rather large.

Chapter 4

Scheme I (English auction scheme)

4.1 Motivation

In an English auction, it is required to reduce the time in one bidding because a bidder repeatedly places a bid in real time. Therefore, it is important that the scheme must reduce the computational and communicational costs for one bidding. In our scheme, the computational cost of both bidding and verifying each bid is fairly reduced by introducing two kinds of BBSs (see Section 2.2).

In the case of first-price SB auction, any canceled bid does not affect the valid bidders. However, in the case of English auction, any bid does not allow to be canceled. If a bid can be canceled in an English auction, the highest bid may be insignificant. It is also important to satisfy anonymity for authorities in order to protect the information of who wants a good and a bidder's history of bidding. Therefore, in an electronic English auction, it is important to satisfy the following two properties, (a) Anonymity and (b) Non-cancelability. Although any bidder can participate anonymously, it is necessary to identify a winner after a bidding. This means that every bid placed in an English auction must be verified maintaining bid anonymity.

The NT-scheme[31] proposed an electronic English auction, which keeps a bidder privacy using a slightly modified group signature scheme[7, 8, 9]. So this protocol suffers from the following drawbacks of group signature schemes. The first problem, which is the most serious, is rather complicated signature generation and verification procedure. In [2, 7, 8, 9], a membership certificate is used to reduce the data size of public group key[6]: only a group member has the certificate issued by the GM. When each member generates a signature on this certificate and a bid, she/he is required the proof of the knowledge. However the proof of the knowledge needs enormous modular multiplication. In an English auction, signature generation or verification corresponds to bidding or verification of bids respectively, both of which are required in each bidding. In an electronic auction, reducing the computational amount of both signature generation and verification are much concerned compared with reducing the group public key size. Therefore we realize an electronic English auction with both fairly simple bidding and verifying procedures by introducing the BBS, which is usually used in putting each bid. The important feature of the BBS is that anybody can check the correctness of the board easily. In our protocol, the computational cost for both bidding and verifying a bid can be reduced.

The second problem is that it is difficult to revoke a bidder because a membership certificate is distributed to each bidder indicated in [3]. Revocation of bidder is necessary when a bidder wants to withdraw from an auction or an authority wants to revoke a certain bidder. Therefore an authority should be able to revoke a bidder easily. [4, 21] realize a group signature scheme with a member revocation, both of which do not have to change a public group key. However, these schemes are not so efficient if the member revocation happens frequently like an electronic auction. In our scheme, a revocation of bidder is done easily by using the BBS: just remove her/him on it.

Our scheme satisfies the basic seven properties (see Section 1.2) without using a group signature, and also satisfies the following four properties:

(h) **One-time registration:** Any bidder can participate in plural auctions by only one-time registration. Even if a bidder is identified as a winner, she/he can participate in the next auction without repeating registration, maintaining anonymity for authorities.

(i) **Simple revocation:** A bidder can withdraw from an auction efficiently.

(j) **Unlinkability among different actions:** Nobody can link the same bidder's bids among plural auctions.

(k) **Linkability in an auction:** Anybody can link which bids are placed by the same bidder and knows how many times a bidder places a bid in an auction.

(ℓ) **Two independent authority's powers:** There is no single authority who can break anonymity and secrecy of bids.

Since we also aim at the functions of a real English auction like Yahoo auction through the Internet, our scheme satisfies the features of Linkability in an auction, and Unlinkability among different auctions. Linkability is also important because the AM can discover the repeated invalid bidding by the same bidder without verifying her/his signature. Also, any bidder can take part in plural auctions as a valid bidder in one-time registration of public key. Since a revocation of bidder can be frequently conducted when a bidder wants to withdraw from an auction or the RM wants to revoke a certain bidder, it should be simple and easy. In our scheme, it is easy to revoke a bidder: the RM has only to delete a bidder from RM's BBS.

4.2 Preliminary

4.2.1 Authorities

The authorities of our scheme consist of the registration manager (RM) and the auction manager (AM), where each role of AM and RM is different from that of the NT-scheme. In our scheme, we assume that these two authorities RM and AM do not collude together. The role of each entity is as follows:

- **RM:**

- manages the participants of auctions.
- prepares for auctions.
- works like Identity Escrow Agency[20] and identifies a certain bidder at the request of the AM.

- **AM:**
  - prepares for auctions.
  - sponsors several auctions.
  - manages the current bid value.

GM's roles in the group signature are well divided into two parties RM and AM. Especially the functions of anonymity and Unlinkability are divided into both RM and AM, and are realized by using each BBS. That is, in our scheme, two kinds of BBSs works as member certificates and also for Unlinkability. Thus it realizes anonymity, Unlinkability and Traceability without using group signature scheme. Furthermore, these BBSs make member revocation simple.

In our scheme, there is no single trusted entity, see, any entity can break neither anonymity nor unlinkability by himself. A protocol with a trusted entity needs the multiple TTPs of the threshold structure. However, our scheme does not need such a threshold structure for auction managers.

4.2.2 Notations

Notations are defined as follows:

p, q	:	two primes which satisfy $q \mid p-1$;
g	:	$g \in \mathbf{Z}_p$ with order q;
x_i	:	$\mathcal{B}_i$'s private key of ($x_i \in_R \mathbf{Z}_q$);
y_i	:	$\mathcal{B}_i$'s public key of ($y_i = g^{x_i} \pmod p$);
r	:	RM's private random number ($r \in_R \mathbf{Z}_q$);
s	:	AM's private random number ($s \in_R \mathbf{Z}_q$);
T_i	:	an auction key for $\mathcal{B}_i$.

4.2.3 The BBS's role

Our scheme uses two kinds of BBSs for RM and AM in order to solve two problems of group signature. The BBS is a kind of public communication channel which can be read by anybody, but can be written only by RM or AM, and also plays a role of member certificate, and thus our scheme uses two kinds of certificates. Both RM and AM manage their BBSs safely.

- RM's BBS: $\{p, q, g\}$, a pair of the identities and public keys for bidders, and $\{y_i^r\}$ $(i = 1, \ldots, I)$.
- AM's BBS: g^{rs} and $\{y_i^{rs}\}$ $(i = 1, \ldots, I)$, and the current bid value.

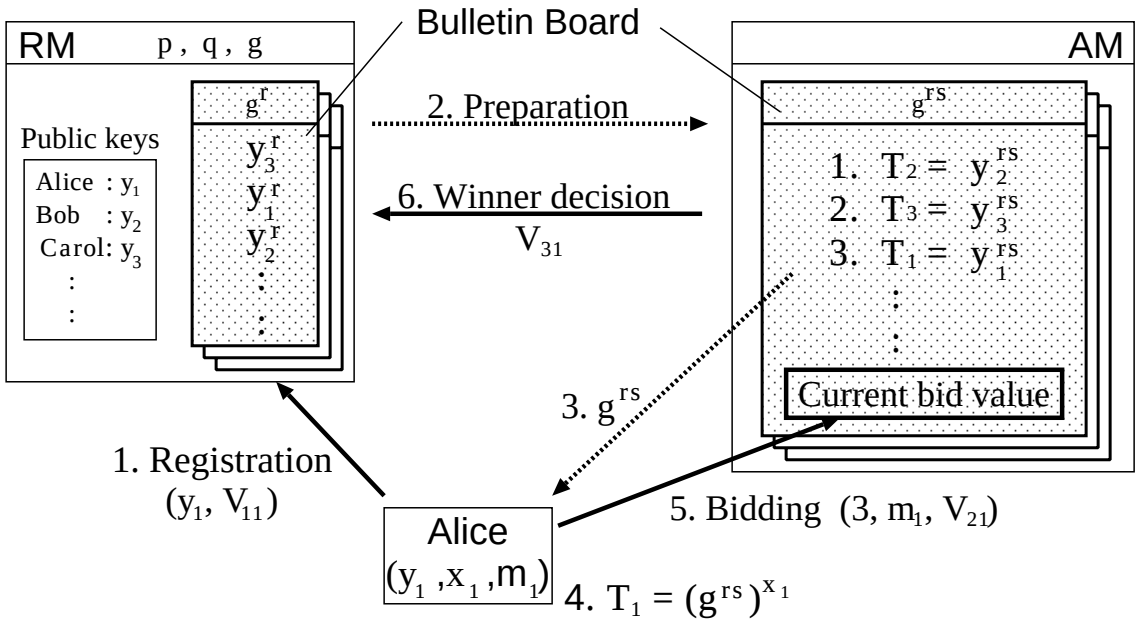


Figure 4.1: Overview (Scheme I)

4.3 Protocol

In this section, we describe an English auction protocol in detail. Secrecy of communication channel is not required because our scheme realizes a public auction. We illustrate the overview of the Scheme I in Figure 4.1.

[Initialization:]

The RM publishes two primes p, q and an element $g \in \mathbf{Z}_p$ with order q.

[Bidder registration:]

A bidder Alice $\mathcal{B}_i$ ($i \in \{1, \ldots, I\}$) registers her public key in the following steps:

Step 1: Alice chooses her private key x_i and computes her public key $y_i = g^{x_i} \pmod{p}$.

Step 2: She sends y_i to the RM, registers her identity and proves that she knows the discrete logarithm x_i of y_i to the base g by showing V_{1i} (see Section 2.6):

$$V_{1i} = SPK[(\alpha) : y_i = g^{\alpha}](m_R),$$

where m_R is a message published by the RM.

Step 3: When the RM accepts that Alice knows the discrete logarithm, he publishes y_i with her name.

[Auction preparation:]

When an auction starts, the RM computes $y_i^r \pmod p$ $(i = 1, \ldots, I)$ as the renewal public keys and publishes them with g^r on RM's BBS. Note that the RM shuffles $\{y_i^r\}$ of all bidders on his BBS and keeps her name secretly (Figure 4.1).

She can confirm whether there exists y_i^r on RM's board or not by checking $y_i^r \stackrel{?}{=} (g^r)^{x_i}$. Here y_i^r works also as a pseudonym during an auction. Note that the random number r is generated every auction, and so does each user's renewal public key y_i^r.

When a vendor requests the AM to hold an auction, the AM conducts the following procedure.

Step 1: The AM generates a random number $s \in_R \mathbf{Z}_q$ and computes $g^{rs} \pmod p$ by using g^r on RM's BBS.

Step 2: The AM computes the following auction key T_i for $\mathcal{B}_i$,

$$T_i = (y_i{}^r)^s \pmod p,$$

by using the private random number s and y_i^r on RM's BBS.

Step 3: The AM publishes the shuffled auction key $\{T_i\}$ of all bidders on his BBS with g^{rs}.

Note that the random number s is generated every auction, and so does each user's y_i^{rs}. Nobody except for the AM can know the correspondence of y_i^r to T_i because y_i^r is concealed by s. On the other hand, the AM cannot know the correspondence of y_i to T_i. Therefore neither AM nor RM can identify a bidder from the information on the BBSs. Furthermore, (j) Unlinkability among plural auctions is realized because both the random numbers r and s are changed at every auction.

Each bidder downloads g^{rs} on AM's BBS. Alice computes her auction key $T_i = (g^{rs})^{x_i} \pmod p$ by herself. Also, she can easily find her auction key T_i in $\{T_1, \cdots, T_I\}$ published on AM's BBS.

[Bidding:]

When she places a bid, she sends the following bid information (ID_{T_i}, m_i, V_{2i}) to the AM.

- the identity ID_{T_i} of auction key T_i
- a bid m_i $\quad (m_i = \text{auction identity}||\text{bid value})$
- $V_{2i} = SPK[(\alpha) : T_i = (g^{rs})^{\alpha}](m_i)$

Here V_{2i} implies that $\mathcal{B}_i$ knows the value of $\alpha = x_i$ if the signature of knowledge V_{2i} is valid. T_i on AM's BBS works like a certificate.

We assume that the AM checks the validity of the signature V_{2i} on each bid. Of course, anybody can check the validity. If the signature V_{2i} is invalid signature, the AM removes the bid with V_{2i}

Checking the validity of the signature of knowledge V_{2i}, anybody can confirm that $\mathcal{B}_i$ knows her/his private key. Furthermore anybody can accept that the signer is one of the valid bidders if the value $y_i{}^{rs}$ is published on AM's BBS.

[Winner decision:]

Let Alice's bid (ID_{T_j}, m_j, V_{2j}) be a winning bid. The AM must publicly prove that T_j corresponds to ${y_j}^r$ in order for the RM to identify Alice. So the AM generates the signature of knowledge V_{3j}:

$$V_{3j} = SPK[(\alpha) : T_j = ({y_j}^r)^\alpha)](m_R),$$

where m_R is a message published by the RM, and the AM publishes V_{3j} with $(T_j, {y_j}^r, m_j, V_{2j})$. Then anybody can confirm the winner by checking the validity of V_{3j} in the following reason.

Theorem 1 (Public verifiability of a winner) *If V_{3j} is a valid signature, then T_j for a winner $\mathcal{B}_j$ is generated by y_j^r .*

Proof. Let $\mathcal{B}_i$'s public key and $\mathcal{B}_j$'s public key be y_i and y_j $(y_j = y_i^z)$, respectively. We assume that nobody knows z. The AM can generate $V_{3j} = SPK[(\alpha) : T_j = ({y_j}^r)^\alpha)](m_R)$. Here suppose that the AM can generate $V_{3j} = SPK[(\alpha) : T_j = ({y_i}^r)^\alpha)](m_R)$ $(i \neq j)$. This means that the AM can solve the discrete logarithm of T_j to the base y_i^r, which is contradictory to the difficulty of DLP. Therefore the AM cannot generate a valid signature V_{3j} using ${y_i}^r$ $(y_i \neq y_j)$. ∎

When the RM received a valid signature V_{3j}, he can identify Alice as a winner for the first time. Note that the AM cannot identify a winner Alice in this winner decision.

[Winner announcement:]

The RM must publicly prove that y_j^r corresponds to y_j in order to identify a winner $\mathcal{B}_j$. So the RM generates the signature of knowledge V_{4j}:

$$V_{4j} = SPK[(\alpha) : y_j^r = (g^r)^\alpha)](m_A),$$

where m_A is a message published by the AM, and the RM publishes V_{4j} with y_j^r and y_j. Then anybody can confirm that a winner is Alice whose public key is y_j by checking the validity of V_{4j}. This is proved in the same way of Theorem 1.

Generally, there is a problem of bidder collusion to form a ring. However, in our scheme, even if a winner Alice offers her values of bid, any bidder cannot identify her at the next auction, because both RM and AM change the random number, r and s at every auction.

4.4 Consideration

4.4.1 Features

We discuss the following twelve properties in our English auction scheme.

(a) **Anonymity:** Nobody including both RM and AM can identify a bidder from her/his signature on a bid. More importantly any bidder can anonymously participate in another auction even if she/he has been identified once.

(b) **Non-cancelability:** The RM can open a signature on a bid with the help of the AM and can identify a winner. So a winner cannot deny that she/he has submitted the winning bid after the winner decision procedure.

(c) **Public verifiability:** Anybody can verify the signature V_{2i} on a bid. Furthermore anybody can confirm whether a bidder is valid or not by checking her/his auction key in AM's BBS. A winner $\mathcal{B}_j$ is publicly verified by checking both signatures V_{3j} and V_{4j}. RM and AM can show the correspondence of $\mathcal{B}_j$'s bidding information V_{2j} to $\mathcal{B}_j$'s public key y_j.

(d) **Unforgeability:** This will be discussed in Section 4.4.2.

(e) **Robustness:** The AM can easily reject a bid by verifying the signature V_{2i}. Of course, the AM can reject a bid which is lower than the current bid value.

(f) **Fairness:** Our scheme has fairness of bidder if it applies non-repudiation protocol to bidding (see Section 7.2). Otherwise the AM may decide on which bids to accept. However AM's misbehavior turn out by the BBS. A bidder can point out that the AM does not accept her/his bid.

(g) **Efficiency of bidding:** This will be discussed in Section 4.4.3.

(h) **One-time registration:** Any bidder can take part in plural auctions as a valid bidder in one-time registration of public key, maintaining anonymity for the RM, AM, and any bidder.

(i) **Simple revocation:** This will be discussed in Section 4.4.4.

(j) **Unlinkability among plural auctions:** Each auction key is different among plural auctions because the secret values r and s, which are different in every auction, is embedded in y_i^{rs} with a bid. So nobody can link two signatures among plural auctions.

(k) **Linkability in an auction:** A real auction has linkability in an auction. It is not so important to satisfy Unlinkability in an auction of an electronic English auction. An auction becomes active by a certain aggressive bidder who always places a higher bid. Anybody knows how many times a bidder places bids in an auction from the signature because a bidder uses the same y_i^{rs} in an auction.

(ℓ) **Two independent authority's powers:** In our scheme, two kinds of authorities are used, which are similar to the NT-scheme. Futhermore, there is no single authority who can break the properties (a) Anonymity and (j) Unlinkability among plural auctions.

4.4.2 Unforgeability

Here we discuss the security against framing attacks such that an entity impersonates another valid bidder.

Table 4.1: The cost for one bidding

	#Modular multiplication	Communication
[7]	13,000	1000 byte
Our scheme	240	40 byte

Theorem 2 (Unforgeability) *Both RM and AM cannot impersonate a valid bidder.*

Proof. Suppose that they can generates the signature of knowledge V_{2i} to impersonate a bidder $\mathcal{B}_i$. This means that they know the discrete logarithm of y_i^{rs} to the base g^{rs}, see, the value x_i. This is contradictory to the difficulty of DLP. Therefore they cannot impersonate a valid bidder. ∎

Even if both RM and AM are colluded, they cannot impersonate a bidder. Of course, other bidders and outsiders cannot also impersonate another valid bidder by Theorem 2.

4.4.3 Performance

In an English auction, it is required to reduce the time in one bidding because a bidder repeatedly places a bid in real time. Therefore, the computational and communicational costs for one bidding are the most important, compared with the other costs (e.g. the preparation of auction). We estimate the computational and communicational costs for one bidding. We use the definition field of DLP with 1200-bit, and the basepoint with 160-bit order. We assume that [7] uses the same field and the basepoint with about 1200-bit order because it is a RSA-based scheme. This order of basepoint is secret.

Table 4.1 compares our scheme with the scheme using the efficient group signature scheme[7] from the viewpoints of computational and communicational costs for one bidding by a bidder. Note that English auction scheme applying [7] is much more efficient than the NT-scheme. From Table 4.1, we see that both the computational and communicational costs for one bidding are fairly reduced. As for efficiency of [7], the signature generation needs 13,000 modular multiplications modulo a 1200-bit modulus in average, and the signature is about 1KBytes long. On the other hand, in our scheme, the signature generation corresponds to computing the proof of knowledge V_{2i}, and the signature corresponds to V_{2i}. Our signature generation needs 240 modular multiplications modulo a 1200-bit modulus because V_{2i} is the original Schnorr signature, and the signature is about 40 Bytes long (160-bit$\times$2) for V_{2i}.

Our scheme introduces two kinds of BBSs, which play the role of membership certificates. The AM has only to check whether the signature V_{2i} is valid or not and whether there exists an auction key is in his BBS or not when a bidder places a bid. In this way the computational and communicational costs for one bidding are reduced.

As for the costs of an auction preparation, a bidder needs to download her/his auction key, and both RM and AM need the computational cost of $O(I)$ to renew each bidder's key.

4.4.4 Simple revocation

In an electronic auction, a revocation of bidder can be frequently conducted when a bidder wants to withdraw from an auction or the RM wants to revoke a certain bidder. Therefore it should be simple and easy. Furthermore the bidding history should be kept secret if a bidder is revoked. In the previous schemes including[4, 21], it is not efficient to revoke a bidder if a revocation of bidder frequently happens. In our protocol, it is efficient to revoke a bidder: the RM has only to delete a bidder from RM's BBS.

4.5 Summary

We have proposed an electronic English auction which realize both anonymity of bidders and Traceability, maintaining efficiency of bidding. Main idea of our protocol is that we make use of not group signature but two BBSs, which has the feature of public and easy verifiability, and that we well separate the role of biddings into two entities, RM and AM, which also play an important role in efficiency of bidding. Since we also aim at the functions of a real English auction like Yahoo auction through the internet, our protocol satisfies the features of linkability in an auction, and unlikability among different auctions. However, in some cases where these features are not required, we might need a slight modification in two entities.

We expect that the bidding will be widely conducted by using a limited CPU power terminal such as a portable telephone in the future. Then, our efficient English auction will be more and more required.

Chapter 5

Scheme II (First-price SB auction scheme)

5.1 Motivation

In an English auction, it is easy to satisfy a property of public verifiability because since all bids value are published. However, in the SB auction, it is difficult to realize public verifiability because a bid is secretly submitted. Our first-price SB auction scheme should satisfy Public verifiability. It is also important to satisfy anonymity for an authority in order to protect the information of who wants a good and a bidder's history of bidding. In this scheme, anonymity is realized for a single AM without directly revealing whole distribution of bids. We use the discrete bidding points in order to realize anonymity for a single AM like the schemes[16, 29] and not to reveal loosing bids directly.

Up to the present, most first-price SB auction schemes aim at realizing the SB auction faithfully, whose concern is secrecy of loosing bids.

(m) **Secrecy of loosing bids:** The scheme should conceal all bids except for a winner. This property is desired in order to keep loser's privacy for the AM(s).

Apparently secrecy of loosing bids is not required in an English auction because all loosing bids are revealed. Therefore the necessity of secrecy of loosing bids depends on targeting what electronic auction. As we will describe below, we aim at the SB auction with a feature of English auction. So our scheme reveals only part of distribution of bids but not reveal loosing bids directly. Entertainment seen in a real English auction has not been discussed before. The SB auction would not have a feature of entertainment, see, all participants cannot enjoy the price-decision process. In real (i.e. non-electronic) auction, both efficiency and entertainment are desired. In our scheme, we introduce a new idea of entertainment to the opening phase by decreasing winner candidates little by little. Our price-decision process looks like a winner-decision process in lottery tickets. Note that the computational and round complexity for a bidder in the opening phase is negligible low in the average.

Our scheme satisfies the basic seven properties (see Section 1.2), and also satisfies the following two properties:

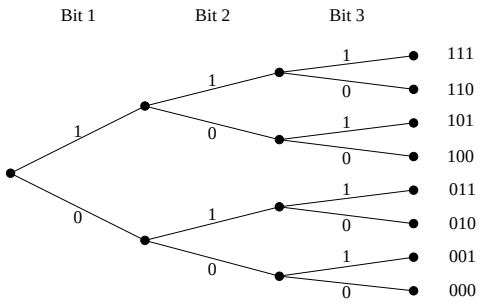


Figure 5.1: Example of bidding points

(n) **Entertainment:** Entertainment means that many bidders can enjoy the opening phase by decreasing winner candidates little by little.

(o) **Efficiency of opening:** the computational and communicational costs in opening the bids is practical.

In this scheme, the computational cost and round complexity in the opening phase depends on mainly (probabilistically) λ, but not directly on the number of bidders. Our scheme can well handle both tie bids and many bidders, and also represents a bid with the size λ for 2^λ bidding points.

5.2 Preliminary

5.2.1 Notations

Notations are defined as follows:

K	:	the number of the discrete bidding prices (bidding points)
λ	:	a number of bits ($K = 2^\lambda$);
$r_i, \tilde{r}_i, R_i$	:	a random number for $\mathcal{B}_i$;
x_i	:	$\mathcal{B}_i$'s private key;
y_i	:	$\mathcal{B}_i$'s public key;
x_A	:	AM's private key;
y_A	:	AM's public key;
$Enc(K, D)$	:	a public key encryption and decryption, which are a probabilistic
$Dec(K, D)$		encryption like ElGamal-encryption in Section 2.3
		$(K : key,\ D : data)$;
$\mathbf{M}_i$	:	$\mathcal{B}_i$'s bid vector;
$f()$	:	a one-way function (e.g. DLP, a hash function).

5.2.2 Bidding points

The bidding points are set up by the AM. There are $2^\lambda (= K)$ bidding points for λ bits. For example, eight bidding points are given by three bits in Figure 5.1. Note that a bid is represented by a bid vector $\mathbf{M}_i$, whose size depends on only λ. As a result, it is possible

to set more bidding points. More bidding points can reduce the probability of bidder's tie of bid.

5.2.3 Bid vector

When $\mathcal{B}_i$ places a bid v_{b_i}(λ-bit) to the AM, $\mathcal{B}_i$ sends a bid vector $\mathbf{M}_i$. The format of $\mathbf{M}_i$ is defined as follows:

$$\begin{aligned}\mathbf{M}_i &= [\mathrm{bit}_1, \cdots, \mathrm{bit}_\lambda, \mathcal{B}_i\text{'s } ID, \mathbf{M}_i\text{'s } ID] \\ &= [M_{i,1}, \cdots, M_{i,\lambda}, M_{i,\lambda+1}, M_{i,\lambda+2}],\end{aligned}$$

$1 \leq t \leq \lambda$

$$M_{i,t} = \begin{cases} f^{\lambda-t+1}(r_i) \oplus f^{\lambda-t}(r_i) & (\text{if } \mathrm{bit}_t = 1) \\ f^{\lambda-t+1}(r_i) \oplus R_{i,\lambda-t} & (\text{otherwise}), \end{cases}$$

$t = \lambda + 1$

$$M_{i,\lambda+1} = r_i \oplus x_i,$$

$t = \lambda + 2$

$$M_{i,\lambda+2} = Enc(y_A, \tilde{r}_i),$$

where $\oplus$ means the bit-wise exclusive or. Note that a function f satisfies $f^\lambda(r) = f(f^{\lambda-1}(r))$. Here we denote the t-th row of $\mathbf{M}_i$ by $M_{i,t}$ $(1 \leq t \leq \lambda + 2)$.

The bid vector $\mathbf{M}_i$ consists of the values expressing **0** or **1** in each bit. The $\mathcal{B}_i$'s ID and $\mathbf{M}_i$'s ID are embedded in the (λ+1)-th row, and the (λ+2)-th row, respectively. In a representation of a bid, a binary number **1** or **0** expresses whether a bid opens the next bit or not, respectively. The (λ+2)-th row $\mathbf{M}_i$'s ID is used for the purpose of correspondence of a bid vector $\mathbf{M}_i$ to the opening key, and does not reveal the correspondence of $\mathbf{M}_i$ to $\mathcal{B}_i$. Anonymity of $\mathcal{B}_i$ is revealed only by opening the (λ+1)-th row ID_i. ID_i can be opened only if $\mathcal{B}_i$ is a winner candidate. Therefore anonymity except for a winner is satisfied. $\mathbf{M}_i$ is opened from bit 1 to ID_i one by one. By checking ID_i for a winner candidate, we can confirm who places a highest bids.

5.3 Protocol

In this section, we describe a first-price SB auction protocol in detail. Our scheme relies on a kind of anonymous broadcast network used in the NFW-scheme. Our system can be implemented with the public key technology, cryptographic one-way functions and the BBS (see Section 2.2) like [43]. For simplicity, we assume the winners to be the one who places the highest bid among a set of bidding points. We illustrate the overview of the Scheme II in Figure 5.2.

[Initialization:]

The AM sets up a one-way function f and publishes f in AM's BBS. The AM sets up $K = 2^\lambda$ bidding points for a good.

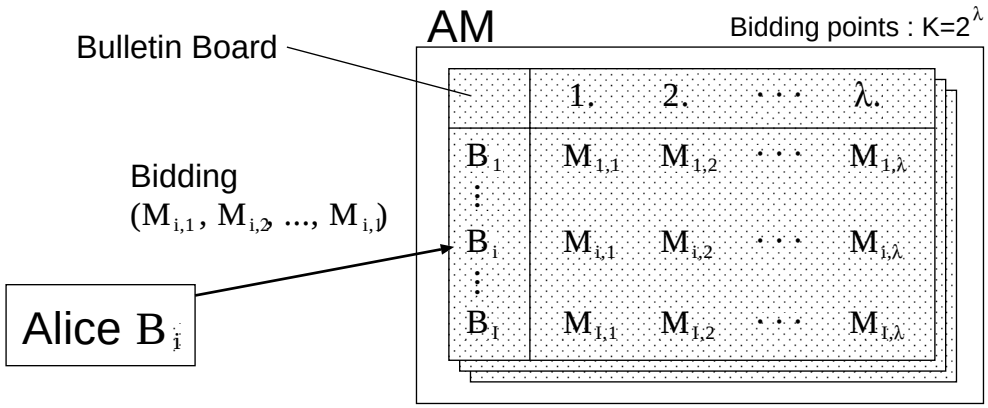


Figure 5.2: Overview (Scheme II)

[Bidder registration:]

Before starting an auction, bidders which want to buy goods execute the following procedure: first generate a pair of private key x_i and public key y_i, send y_i to the AM and get its certificate by the AM. The AM publishes all public keys y_i $(i = 1, \ldots, I)$ with the corresponding bidder's names.

[Bidding:]

We explain how $\mathcal{B}_i$ places a bid. For simplicity, $\mathcal{B}_i$ places a bid $v_{b_i} = (\mathbf{1} \cdots \mathbf{1} \overset{t}{\breve{\mathbf{0}}} \mathbf{1} \cdots \mathbf{1} \overset{\lambda-1}{\breve{\mathbf{0}}} \mathbf{1})$ that both the t-th and the $(\lambda-1)$-th bits are $\mathbf{0}$. Then bid vector $\mathbf{M}_i$ is as follows:

$$\begin{aligned}
\mathbf{M}_i &= [M_{i,1}, \cdots, M_{i,t}, M_{i,t+1}, \cdots, \ M_{i,\lambda-1}, M_{i,\lambda}, M_{i,\lambda+1}, M_{i,\lambda+2}] \\
&= \Big[f^{\lambda}(r_i) \oplus f^{\lambda-1}(r_i), \ \cdots, \ f^{\lambda-t+1}(r_i) \oplus R_{j,\lambda-t}, \ f^{\lambda-t}(r_i) \oplus f^{\lambda-t-1}(r_i), \ \cdots, \\
&\quad f^2(r_i) \oplus R_{i,1}, \ f(r_i) \oplus r_i, \ r_i \oplus x_i, \ Enc(y_A, \tilde{r_i})\Big],
\end{aligned}$$

where $R_{i,\lambda-t}$ is a random number $(R_{i,\lambda-t} \neq f^{\lambda-t}(r_i))$ and x_i is $\mathcal{B}_i$'s private key.

Step 1: $\mathcal{B}_i$ generates random numbers $R_{i,\lambda-t}, R_{i,1}, r_i$ and $\tilde{r_i}$, and computes $f(r_i), \cdots, f^{\lambda}(r_i)$ by using a one-way function f and r_i.

Step 2: $\mathcal{B}_i$ encrypts $\tilde{r_i}$ to $Enc(y_A, \tilde{r_i})$ by using AM's public key y_A.

Step 3: $\mathcal{B}_i$ constructs a bid vector $\mathbf{M}_i$ corresponding to v_{b_i}. $\mathcal{B}_i$ has to keep $\{f(r_i), \cdots, f^{\lambda}(r_i)\}$ secret, but posses only $\{f^{\lambda}(r_i), f^{\lambda-t}(r_i), f(r_i)\}$ as opening keys.

Step 4: $\mathcal{B}_i$ sends $\mathbf{M}_i$ and $Enc(y_A, \tilde{r_i})$ to the AM, where $\mathbf{M}_i$ does not need to be encrypted, because $\mathcal{B}_i$ keeps the opening key $f^{\lambda}(r_i)$ secret to conceal the value of v_{b_i}.

Step 5: The AM decrypts $\tilde{r_i}$ from $Enc(y_A, \tilde{r_i})$ by using his private key x_A, and keep $\tilde{r_i}$ secretly for the purpose of correspondence of $\mathbf{M}_i$ to the opening key. The AM publishes all bid vectors $\mathbf{M}_i$ $(i = 1, \ldots, I)$ in his BBS.

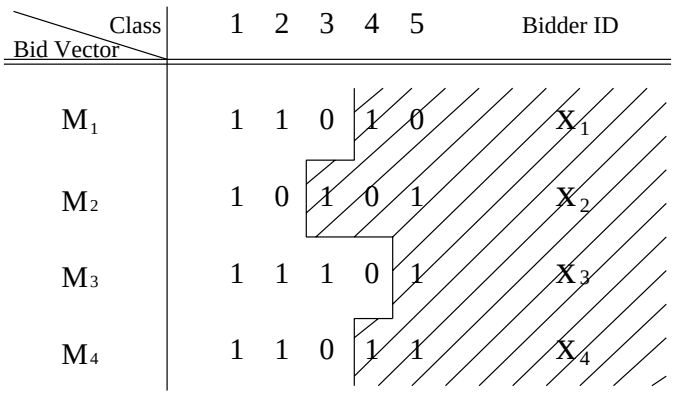


Figure 5.3: Opening example

Anonymity of the correspondence of a bidder to a bid vector is satisfied as long as opening keys are kept secret. Nobody gets any information about the correspondence of a bid vector to a public key.

[Opening a winning bid:]

This section presents the opening phase in our scheme. For simplicity, we assume that a bid v_{b_j} for $\mathcal{B}_j$ is the highest in this auction.

Step 1: $\mathcal{B}_i$ sends the first opening key $f^{\lambda}(r_i)$ with $Enc(y_A, \tilde{r}_i)$ to the AM. The AM corresponds $f^{\lambda}(r_i)$ to $\mathbf{M}_i$ by decrypting $Enc(y_A, \tilde{r}_i)$. Then the bid vector $\mathbf{M}_i$ is opened till the t-th row corresponding to "**0**". Everybody can confirm **0** of t-th row in $\mathbf{M}_i$ by checking $f^{\lambda-t+1}(r_i) \neq f(R_{j,\lambda-t})$. As a result, the only values $\{f^{\lambda}(r_i), f^{\lambda-1}(r_i), \cdots, f^{\lambda-t+1}(r_i)\}$ are opened. Note that the value $f^{\lambda-t}(r_i)$ is not opened.

Step 2: Only bidders $\mathcal{B}_i$ whose bid vectors are opened to the higher bit send the next opening key as winner candidates (e.g. $\mathbf{M}_3$ in Figure 5.3). $\mathcal{B}_i$, a winner candidate, sends the second opening key $f^{\lambda-t}(r_i)$ with $Enc(y_A, \tilde{r}_i)$ to the AM. In the same way as **Step 1**, this procedure continues till the last row. Note that $\mathcal{B}_i$'s private key is not opened as long as $\mathcal{B}_i$ keeps the final opening key r_i secret.

[Winner decision:]

Everybody can confirm that $\mathcal{B}_j$ is a winner of bid vector $\mathbf{M}_j$ by checking a pair of public key y_j and the private key x_j, which is revealed in the last row. Of course, after this auction a winner $\mathcal{B}_j$ has to get another certificate of y'_j by changing x_i into x'_j.

Schemes based on a practical one-way function

We will present two examples of one-way function f, one is based on DLP[13] and the other is based on a hash function.

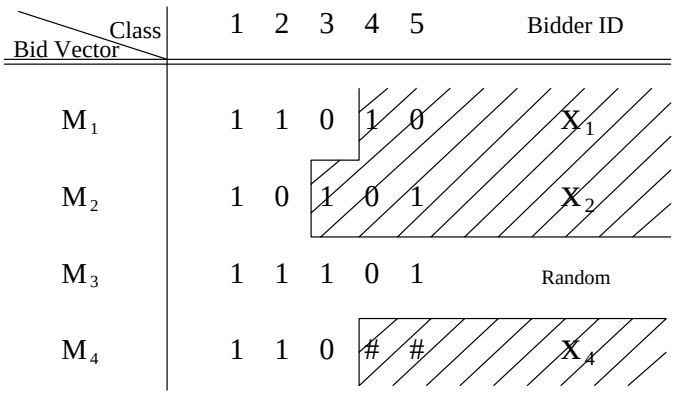


Figure 5.4: Examples of invalid bid

DLP: The AM selects a large prime p and $g \in Z_p^*$ with prime order q. Then a one-way function f is set to $f(r) = g^r \pmod{p}$. In this case, $f^2(r) = g^{g^r}$.

One-way hash function ($\mathcal{H}$): A one-way function f is set to $f(r) = \mathcal{H}(r)$ in the same way as hash chain technique (see Section 2.8). In this case, $f^2(r) = \mathcal{H}(\mathcal{H}(r))$.

5.4 Security

This section discusses security of our protocol.

5.4.1 Invalid bid vector

We investigate that any invalid bid does not have an influence on the auction proceedings. Figure 5.4 shows two types of invalid bid vector:

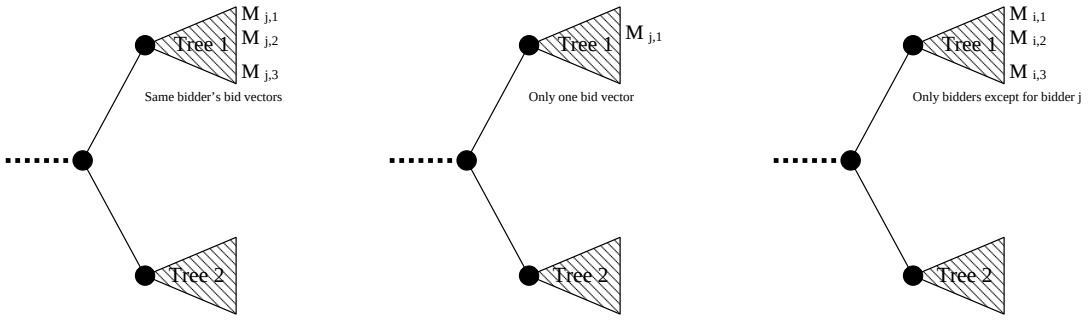
1. a bidder $\mathcal{B}_i$ does not embed her/his private key into $\mathcal{B}_i$'s ID bit in a bid vector (Figure 5.4-$\mathbf{M}_3$).

2. a bidder does not embed the proper opening key into a bid vector (Figure 5.4-$\mathbf{M}_4$).

First we discuss the case 1. Unless $\mathcal{B}_3$ is a winner candidate, there is no problem: $\mathbf{M}_3$ is simply ignored. If $\mathcal{B}_3$ is a winner candidate like Figure 5.4, nobody can identify $\mathcal{B}_3$ because $\mathcal{B}_3$'s private key is not embedded in $\mathbf{M}_3$. In such a case, $\mathbf{M}_3$ is simply removed from this auction as an invalid bid. In our protocol, a bid vector is opened from the highest bid. Therefore the auction proceedings may just continue except for an invalid bid vector.

Next we discuss the case 2. Both $\mathcal{B}_1$ and $\mathcal{B}_4$ are winner candidates except for $\mathcal{B}_3$. However, nobody can open the bit 4 of $\mathbf{M}_4$ because $\mathbf{M}_4$ is not embedded into the proper opening key in the 4-th bit. In such a case, $\mathbf{M}_4$ is also ignored. Therefore $\mathbf{M}_1$ is an only winner candidate. The opening phase continues except for $\mathbf{M}_3$ and $\mathbf{M}_4$.

In our scheme, we cannot identify the invalid bidders in the same way as some works[15, 19, 23, 42, 43, 47]. However our scheme has a feature that each bid vector of bidders is



(a) : Case 1 (b) : Case 2 (c) : Case 3

Figure 5.5: Bid manipulation

independently opened. Therefore even if an invalid bidder places a bid vector, the auction proceedings will be unaffected: all invalid bids are simply ignored. So our scheme satisfies disturbing resistance, i.e. (e) Robustness.

5.4.2 Bid manipulations

We investigate the multiple bidding by a bidder $\mathcal{B}_j$, who wants to get goods in the lowest price available. For simplicity, let $\{M_{i,1}, M_{i,2}, M_{i,3}\}$ be valid bid vectors. There are three cases in bid manipulations seen in Figure 5.5, which expresses a part of binary tree in bids (See Figure 5.1):

Case 1 (Figure 5.5-(a)): there are only $\mathcal{B}_j$'s bid vector $\{M_{j,1}, M_{j,2}$ and $M_{j,3}\}$ in higher trees.

Case 2 (Figure 5.5-(b)): there is only one of $\mathcal{B}_j$'s bid vector $M_{j,1}$ in higher trees.

Case 3 (Figure 5.5-(c)): there is no $\mathcal{B}_j$'s bid vector but there are other bidder's bid vector $\{M_{i,1}, M_{i,2}$ and $M_{i,3}\}$ in higher trees $(i \neq j)$.

In the case 1, $\mathcal{B}_j$ can get goods in the lowest bid of $M_{j,3}$ by canceling two bids of $M_{j,1}$ and $M_{j,2}$ presented in the NFW-scheme. But in both case 2 and case 3 it is impossible for $\mathcal{B}_j$ to control the winning bid. To sum up, a bidder can control the winning bid only in the case 1. However such bid manipulations have a little influence on the auction proceedings because $\mathcal{B}_j$ cannot necessarily get goods in the lower price than that of $\mathcal{B}_i (i \neq j)$. Furthermore even if $\mathcal{B}_j$ conducts the multiple bidding, this does not affect other bidders.

5.4.3 Group collusion

We can treat a group collusion likewise. This is not a serious problem as we have described in Section 5.4.2.

5.5 Consideration

5.5.1 Features

Our scheme satisfies the following properties:

(a) **Anonymity:** In our scheme, only a winner's private key is revealed, which identifies the corresponding bidder. On the other hand, other private keys are kept secret even after the opening phase. As a result, nobody (including the AM) can know the correspondence of a bidder to a bid except for a winner.

(b) **Non-cancelability:** A winner $\mathcal{B}_i$ cannot deny her/his bid because $\mathcal{B}_i$'s private key is revealed.

(c) **Public verifiability:** Since bid vectors are opened one by one from the higher bid, apparently a winning bid is the highest of all bids. Moreover the validity of a bid vector is easily checked by a one-way function and private key. A bidder $\mathcal{B}_i$ can easily notice $\mathcal{B}_i$'s falsified bid because all bid vectors are opened on the Internet.

(d) **Unforgeability:** Only $\mathcal{B}_i$ makes the valid bid vector because of knowing $\mathcal{B}_i$'s private key. Anybody can see $\mathcal{B}_i$'s private key in the last low of a bid vector $\mathbf{M}_i$ if $\mathcal{B}_i$ is a winner.

(e) **Robustness:** Our scheme has a feature that each bid is independently opened. Therefore if invalid bids are placed, the auction proceedings will be unaffected: invalid bids are simply ignored.

(f) **Fairness:** Any bidder can check whether her/his bid vector is published in AM's BBS or not for an bidding phase. So any bid is fairly dealt with.

(g) **Efficiency of bidding:** This will be discussed in Section 5.5.2.

(m) **Secrecy of loosing bids:** Before the opening, a bid cannot be revealed. In our scheme, each row of a bid vector consists of two random numbers $f(r_i) \oplus r_i$ and $r_i \oplus r'_i$ by using a one-way function f and a random number r_i and r'_i. As for the former, r_i is kept secret as long as $f(r_i)$ is not opened, whose secrecy depends on f. As for the latter, r'_i is chosen randomly, and r_i is kept secret as long as the next row is not opened. Therefore secrecy also depends on f. Secrecy on attacks of using all row data in a bid vector also depends on f. After the auction, our scheme does not satisfy complete secrecy of loosing bids, but conceals loosing bids as many as possible.

(n) **Entertainment:** English auction has a feature of entertainment that it does not only decide a winner but also pleases all participants until the winner is decided. In our scheme, we introduce a feature of entertainment to the opening phase by decreasing winner candidates one by one, which looks like a winner-decision process in lottery tickets. Since we aim at a feature of entertainment, our protocol reveals only part of distribution of bids. However our protocol does not reveal the whole

Table 5.1: The communicational costs

	A bidder ($\mathcal{B}$)			AM	
	Bidding	Opening	Winner	Opening	#AM
KMSH-scheme[23][2]	$O(K)$	–	$O(1)$	–	1
NFW-scheme[29]	$O(1)$	–	$O(I)$	–	1
NPS-scheme[30][1]	$O(\log K)$	–	–	$O(I \log K)$	2
Our scheme (Hash)[2]	$O(\log K)$	$O(1)$	–	–	1

distribution of bids though the schemes[14, 16, 24, 29] do, and what is still better, satisfies anonymity.

(o) **Efficiency of opening:** This will be discussed in Section 5.5.2.

5.5.2 Performance

In this section, we compare our scheme with three previous schemes, the KMSH-scheme, the NFW-scheme and the NPS-scheme, from the viewpoints of communicational and computational costs, which are shown in Table 5.1 and Table 5.2. Here let the number of bidding points and bidders be $K = 2^\lambda$ and I, respectively. We assume a one-way function f to be DLP (1024-bit) or a 160-bit output one-way hash function, whose output size is denoted by $|f|$.

First we examine the communicational cost in Table 5.1. As for the communicational cost in the bidding phase, the NFW-scheme is the most efficient, which is independent of K. However, it does not realize secrecy of loosing bids at all, see, all bidders must open their bid values after the bidding phase. Also, the communicational cost for a winner is of $O(I)$ based on a modular multiplication. Our scheme (Hash) is more efficient than the NPS-scheme which is based on 1024-bit modular multiplication. As for the communicational cost in the opening phase, the communication between $\mathcal{B}_i$ and the AM is required in our scheme because we aim at a feature of entertainment. But we will see in Table 5.1 that the communicational cost in the opening phase is negligible small. For simplicity, we assume that there are $I/2^t$ bidders in each branch of bit t on the average, and that each bidder sends an opening key in the probability $1/2$. Therefore the communicational cost for a bidder in the opening is on the average:

$$\frac{1}{n} \cdot |f| \sum_{t=0}^{\lambda} \frac{n}{2^t} = |f| \left(2 - \frac{1}{2^\lambda}\right) = |f| \left(2 - \frac{1}{K}\right) \simeq O(1).$$

The NPS99-scheme has the communicational cost of $O(I \log K)$ between two AMs, while the others including our scheme does not have such a communication because of a single AM.

Next we discuss the computational cost in Table 5.2. As for the bidding computation, our scheme (Hash) is more efficient than the NPS-scheme which is based on 1024-bit

[1] This scheme can also implement the first-price SB auction by changing the program.

Table 5.2: The computational cost

	A bidder ($\mathcal{B}$)		AM	
	Bidding	Winner	Opening	#AM
KMSH-scheme[23][2]	$O(K)$	–	$O(K)$	1
NFW-scheme[29]	$O(1)$	$O(I)$	$O(I)$	1
NPS-scheme[30][1]	$O(\log K)$	–	$O(I \log K)$	2
Our scheme (Hash)[2]	$O(\log K)$	–	$O(I)$	1

modular multiplication. In the NFW-scheme a winner's computational cost is of $O(I)$ based on 1024-bitmodular multiplication. On the other hand, our computational order of the opening for the AM is on the average:

$$O\left(\sum_{t=0}^{\lambda} \frac{I}{2^t}\right) = O\left(I(2 - \frac{1}{2^\lambda})\right) \simeq O(I), \qquad \left(0 \leq 2 - 1/2^\lambda \leq 2\right).$$

Even if the more number of K is set up, the computational cost for the AM depends on only I in our scheme.

5.6 Summary

We have proposed an anonymous first-price SB auction scheme with a single AM. Our scheme realizes anonymity for a single AM. As for efficiency of both bidding and opening, for K bidding points, the size of the representation of bids and the opening round are reduced to just $\log K$. Our scheme aims at (n) Entertainment, which is realized by English auction. Many bidders can enjoy the opening phase by decreasing winner candidates little by little. Furthermore, our scheme can be easily applied to a power auction, which decides the plural winners.

[2]The communicational and computational costs depends on 160-bit output hash computing, and thus it is much more efficient than the other schemes based on 1024-bit modular multiplication.

Chapter 6

Scheme III (Second-price SB auction scheme)

6.1 Motivation

A second-price SB auction is that a bidder who offers the highest bid price gets a good in the second highest price. If this auction scheme does not have to satisfy secrecy of the highest bid, we can easily realize it by using an adoption of first-price SB auction. In a second-price SB auction, since the highest bid is the winner's true value because of incentive compatibility (see Section 6.2), it is important to conceal the highest bid value for winner's privacy. It is easy to apply a second-price SB auction to a first-price SB auction. But a first-price SB auction cannot directly be applied to a second-price SB auction which keeps the highest bid secret. Our second-price SB auction scheme realizes secrecy of the highest bid with satisfying (c) Public verifiability. So our scheme satisfies the basic seven properties (see Section 1.2), and also satisfies the following four properties:

(ℓ) **Two independent authority's power:** There is no single authority who can break anonymity and secrecy of bids.

(m) **Secrecy of loosing bids:** The scheme conceals all bids except for a winning bid. This property is desired in order to keep loser's privacy for the AM(s).

(o) **Efficiency of opening:** The computational and communicational costs in opening phase are practical.

(p) **Secrecy of the highest bid:** The scheme does not disclose the information about the highest bid value except that it is placed higher than the second highest bid value. This property is desired for winner's privacy.

We use two authorities AM1 and AM2 in our scheme. Neither AM1 nor AM2 can manipulate the opening results (a winner and a winning bid) in our scheme unless both of the AMs collude. In order to satisfy the basic properties and the above properties, we introduce several techniques of the signature of knowledge, the discriminant function of the p_0-th root, verifiable decryption of ElGamal scheme, verifiable w-th power mix, and verifiable decryption mix.

6.2 Economic Viewpoints

A second-price SB auction has been proposed by W. Vickrey in 1961[48], who won the Nobel Economics Prize in 1996. A second-price SB auction is that each bidder secretly submits a bid to Auctioneer only once, and a bidder who offers the highest price gets a good in the second highest price. Here we explain why a second-price SB auction is so outstanding by the following example. Three bidders $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$ participate the car, BMW, auction and their *true values* for it, which means the maximum value that each bidder can spend, are as follows:

- $\mathcal{B}_1$'s true value : \$66,000;
- $\mathcal{B}_2$'s true value : \$64,400;
- $\mathcal{B}_3$'s true value : \$60,900.

If a bidder can buy BMW cheaper than her/his true value, she/he will make a profit. If she/he buys BMW higher than her/his true value, her/his purchase will end in failure. So the true value means the boundary between losses and gains for each bidder.

Suppose that they participate in a first-price SB auction under the above situation. Then each bidder will never place her/his true value because she/he wants to buy BMW as cheap as possible. In this case, it is often happened for each bidder to tap other bids in order to estimate exactly her/his bid since they can buy it as cheap as possible. If a winning bid is much higher than the second highest price, a winner may want to cancel it. Even if a winner bought a good, she/he will not agree with it.

However, suppose that they participate in a second-price SB auction. Then each bidder will place her/his true value because she/he cannot reduce her/his cost for BMW by her/his bid. Generally, it is said that a bidder has the dominant strategy (see Section 2.1) in a second-price SB auction. So it is useless for each bidder to estimate other bids. A winner's bid is decided by other bids. A winner's bid value is not a winning bid value but a datum line to decide a winner. So any bidder will place her/his true value in a second-price SB auction, which has the following property of incentive compatibility.

Incentive compatibility: Incentive compatibility means that the dominant strategy for each bidder is to place a bid honestly her/his own true value[48].

Each bidder can place a bid through mutual agreement. As a result, a bidder will not want to cancel her/his bid. Therefore a second-price SB auction is superior to a first-price SB auction from the view points of economics.

Next we compare a second-price SB auction with an English auction. A winning bid value in a second-price SB auction becomes the second highest true value (\$64,400) as mentioned above. On the other hand, in an English auction, each bidder places a bid many times until their true value. As a result, $\mathcal{B}_1$ gets BMW in \$64,400+Δ ($\Delta \simeq 0$) since $\mathcal{B}_2$ does not place a bid in more than \$64,400. Therefore a winning bid in a second-price SB auction is almost the same value as one in an English auction. This means that a second-price SB auction works the competition principle as well as an English auction.

6.2.1 Disadvantages

We wonder if a second-price sealed-bid auction is superior to English auction. Actually, however, an English auction is much more popular than a second-price sealed-bid auction. We think two reasons why a second-price sealed-bid auction is unpopular as follows:

1. A winning bid value is not winner's.

2. It is hard for each bidder to decide her/his true value in advance.

If the AM knows the highest bid value in the middle of auction, the AM may place a little lower bid than the highest bid as a valid bidder. In this case, a winning bid almost becomes winner's true value. Even a winner does not perceive such AM's handling. As long as the AM knows the highest bid value in the middle of auction, the bidder will not want to participate in the second-price sealed-bid auction. Such AM's handling cannot be happen in English auction. This is why secrecy of the highest bid is necessary for an authority in the second-price sealed-bid auction.

In the case 2, a bidder must decide her/his true value for the dominant strategy in advance. However, the bidder $\mathcal{B}_{sec}$ may change her/his true value in the middle of the auction. The true value depends on bidder's mood whether the bidder wants to buy the good. After an auction, $\mathcal{B}_{sec}$'s true value may be higher than the winner's bid value. Then $\mathcal{B}_{sec}$ may regret her/his bid. In an English auction, a bidder can raise her/his true value in the middle of auction.

6.3 Main Goals

Our main goals are to realize the following three requirements in an electronic second-price SB auction, where $\mathcal{B}_{sec}$ is a bidder who places the second highest bid:

1. The highest bid value are not disclosed for any entity;

2. Anonymity of $\mathcal{B}_{sec}$ is satisfied for any entity;

3. Anyone can publicly verify the auction process and results.

The first goal is desired even after winner's decision in order to satisfy a privacy of winner. Our scheme does not disclose the highest bid value as well as the partial range that the highest bid is placed for any entity including both auction managers (AM1 and AM2). The second goal is important because $\mathcal{B}_{sec}$'s bid is revealed as a winning bid. Our scheme realizes anonymity of $\mathcal{B}_{sec}$ without an anonymous channel. The correspondence of each bid to each bidder is also kept secret unless both AM1 and AM2 collude. The third goal ((c) Public verifiability) is important because our scheme secretly computes the auction results.

Furthermore, in our scheme, each bidder does not have to compute the zero-knowledge proofs unlike [1]. To reduce the computational cost of bidder is one of our goals.

Figure 6.1: Verifiable w-th power mix

6.4 Preliminary

6.4.1 Authorities

Our scheme uses two kinds of auction managers (AM1 and AM2) in order to eliminate a strong single authority. The role of each auction managers is as follows:

- **AM1:**
  - treats the bidder registration;
  - publicly computes the winning bid, decides a winner, and show the validity of the results;
  - manages AM1's BBS (see Section 2.2) which publishes a list of public keys and shows the validity of the results.
- **AM2:**
  - manages the bidding phase;
  - verifies a bid information;
  - publicly multiplies each element in all bid vectors;
  - manages AM2's BBS which publishes the computing process of bids.

6.4.2 Notations

Notations are defined as follows:

$\mathcal{B}_{sec}$	:	a bidder who places the second highest bid;
$\mathbf{V}_i$	:	a bid vector of bidder i;
p_0, p_1	:	small primes but greater in bit size than number of bidders, I (e.g.100bit);
p, q, p', q'	:	large primes ($p = 2p_0p' + 1, q = 2p_1q' + 1$) which are secret except for the AM1;
n	:	$n = pq$;
g	:	$g \in_R \mathbf{Z}_n$ whose order is $\mathrm{ord}(g) = 2p_0p'p_1q'$ and has neither p_0-th nor p_1-th root;
K	:	the number of the discrete bidding prices (bidding points)
k	:	the index of bidding points ($k = 1, \ldots, K$);

$t_{i,k}^{(0)},\ t_{i,k}^{(1)}$	:	$\mathcal{B}_i$'s secret random numbers generated by the AM1;
x_i	:	$\mathcal{B}_i$'s private key;
y_i	:	$\mathcal{B}_i$'s public key ($y_i = g^{x_i} \mod n$);
s, w	:	AM2's private keys (w is relatively prime to p_0 : $\gcd(w, p_0) = 1$);
Y	:	AM2's public key ($Y = g^s \mod n$) that has neither p_0-th nor p_1-th root;
$sig_{key}()$	:	a signature by key;
$E_y()$	:	ElGamal encryption with public key g and $y = g^x$ such as $E_y(m) = (G = g^r, M = my^r)$;
$D^*()$	:	the verifiable ElGamal decryption (see Section 2.9),
$\mathcal{M}()$	:	the discriminant function of the p_0-th root, where $\mathcal{M}(y)$ is 1 or 0 whether y has the p_0-th root in $\mathbf{Z}_n$ or not, which can be computed only by the AM1 (see Section 6.4.3).

The ElGamal public-key cryptosystem over $\mathbf{Z}_n$ is as secure as the Diffie-Hellman scheme described in [27].

6.4.3 The verifiable p_0-th root

Lemma 1 *For $n = pq$ ($p = 2p'p_0 + 1, q = 2q' + 1, p', q', p_0$: different primes > 2), $z \in \mathbf{Z}_n$ has the p_0-th root if and only if $z^{2p'q'} = 1 \pmod n$.*

Proof. If z has the p_0-th root, there exists x such that $z = x^{p_0}$. Therefore, $z^{2p'q'} = x^{2p'p_0q'} = 1 \pmod n$. Conversely, we can set $z = x^r$ ($r \in \mathbf{Z}_n$) that order of x is $2p'p_0q'$. If $z^{2p'q'} = 1 \pmod n$, then $z^{2p'q'} = x^{2p'q'r} = 1 \pmod n$. So $r = r'p_0$ is necessary ($\exists r' \in \mathbf{Z}_n$). Therefore, $z = x^r = x^{r'p_0} \pmod n$, see, z has the p_0-th root. ∎

$M(z)$ can be computed by only the knowledge of p' and q'. Therefore an authority who knows order of g can publicly prove that z has the p_0-th root by showing

$$SPK[(\alpha) : z^\alpha = 1 \wedge (g^{p_0})^\alpha = 1 \wedge g^\alpha = r](m),$$

for a random number $r \neq 1$. Also, such an authority can publicly prove that z does not have the p_0-th root by showing

$$SPK[(\alpha) : z^\alpha = r \wedge (g^{p_0})^\alpha = 1](m),$$

for random numbers $r \neq 1$. The above two SPKs mean that α is $2p'q'$. Checking whether z has the p_0-th root or not satisfies public verifiability.

6.4.4 Verifiable w-th power mix

A pair of $(c, C = c^w)$ is published, where w is secret. Let (a, b) and (A, B) be input and output of a verifiable w-th power mix, respectively, where $A = a^w$ and $B = b^w$ ($A \neq B$) in Figure 6.1. We hide the correspondence of an input to the output, but can show the validity of secret mix by proving the equality of three discrete logarithms of A, B and C. The proof is given by the following SPK (see Section 2.6):

$$SPK[(\alpha) : (A = a^\alpha \wedge B = b^\alpha \wedge C = c^\alpha) \vee (A = b^\alpha \wedge B = a^\alpha \wedge C = c^\alpha)](m).$$

Figure 6.2: Verifiable decryption mix

6.4.5 Verifiable decryption mix

Let $(E_Y(a), E_Y(b))$ and (a, b) be input and output of the verifiable decryption mix in Figure 6.2, respectively, where $E_Y(a) = (G_a, M_a)$ and $E_Y(b) = (G_b, M_b)$. We hide the correspondence of an input to the output, but can show the validity of secret mix. The proof is given by showing

$$SPK[(\alpha) : (M_a/a = {G_a}^{\alpha} \wedge M_b/b = {G_b}^{\alpha} \wedge Y = g^{\alpha}) \vee (M_a/b = {G_a}^{\alpha} \wedge M_b/a = {G_b}^{\alpha} \wedge Y = g^{\alpha})](m).$$

6.5 Protocol

In this section, we describe a second-price SB auction protocol in detail. We illustrate the overview of the Scheme III in Figure 6.3.

[Initialization:]

The AM1 selects $g, p_0, p_1, p', q', p, q$ and K, computes a product $n = pq$, and then publishes (g, p_0, p_1, n) but keeps (p', q', p, q) secret. The AM1 can show that g has neither the p_0-th nor p_1-th root. The AM2 computes $Y = g^s \pmod{n}$ and publishes Y. Note that s is AM2's secret and that both $\gcd(s, p_0) = 1$ and $\gcd(s, p_1) = 1$ hold. The AM1 checks that Y has neither the p_0-th nor p_1-th root and that order of Y is $2p_0p'p_1q'$.

[Bidder registration:]

When Alice ($\mathcal{B}_i$) participates an auction, she sends her public key y_i with the signature $sig_{x_i}(y_i)$ to the AM1 as a bidder registration. After the AM1 receives her values, he publishes her public key y_i.

[Auction preparation:]

The AM1 chooses her values $t_{i,1}^{(0)}, \ldots, t_{i,K}^{(0)}, t_{i,1}^{(1)}, \ldots t_{i,K}^{(1)} \in \mathbf{Z}_n$, all of which have the p_0-th root, and then secretly sends $\{t_{i,k}^{(0)} \cdot g^{p_0}\}$ and $\{t_{i,k}^{(1)} \cdot g^{p_1}\}$ to $\mathcal{B}_i$. The AM1 shuffles two values in every bidding point:

$$\left(\mathcal{H}(t_{i,1}^{(0)} \cdot g^{p_0}), \mathcal{H}(t_{i,1}^{(1)} \cdot g^{p_1})\right), \ \ldots, \ \left(\mathcal{H}(t_{i,K}^{(0)} \cdot g^{p_0}), \mathcal{H}(t_{i,K}^{(1)} \cdot g^{p_1})\right),$$

for $i = 1, \ldots, I$, and places them into AM1's public database. By checking AM1's public database, $\mathcal{B}_i$ can confirm whether her values $t_{i,1}^{(0)} \cdot g^{p_0}, \ \ldots, \ t_{i,K}^{(0)} \cdot g^{p_0}, \ t_{i,1}^{(1)} \cdot g^{p_1}, \ \ldots, \ t_{i,K}^{(1)} \cdot g^{p_1}$ are exactly registered. We assume that: nobody except the AM1 knows the correspondence

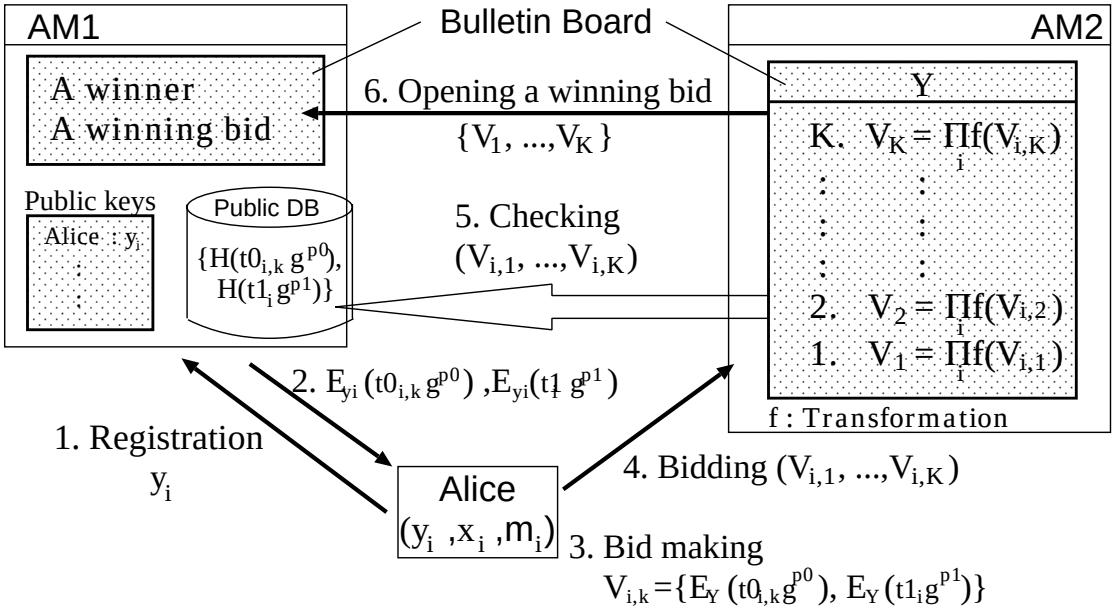


Figure 6.3: Overview (Scheme III)

of a bidder to her/his two values; anybody can refer to the data in his public database; but that only the AM1 can alter them.

[Bidding:]

When Alice places a bid at a bidding point $k_i \in \{1, \ldots, K\}$, she generates her bid vector $\mathbf{V}_i$ as follows:

$$\mathbf{V}_i = [E_Y(v_{i,K}), \ldots, E_Y(v_{i,1})],$$

where

$$v_{i,k} = \begin{cases} t_{i,k}^{(1)} \cdot g^{p_1} \pmod{n} & (k = k_i), \\ t_{i,k}^{(0)} \cdot g^{p_0} \pmod{n} & (k \neq k_i). \end{cases}$$

She sends $\mathbf{V}_i$ to the AM2. Note that she also sends her reverse bid vector $\mathbf{V}'_i = \left[E_Y(v'_{i,K}), \ldots, E_Y(v'_{i,1})\right]$, see, if $v_{i,k} = t_{i,k}^{(0)} \cdot g^{p_0}$, then $v'_{i,k} = t_{i,k}^{(1)} \cdot g^{p_1}$.

[Checking a bid vector:]

The validity of $\mathbf{V}_i$ is checked as follows: (1) The AM2 decrypts $\{E(v_{i,k}), E(v'_{i,k})\}$ by using the verifiable decryption mix; (2) The AM2 computes both $\mathcal{H}(v_{i,k})$ and $\mathcal{H}(v'_{i,k})$ and checks whether or not both values exist in AM1's public database; (3) The AM2 computes

$$\Gamma 1_i = \frac{1}{g^{p_1}} D^* \left(\prod_{k=1}^{K} E_Y(v_{i,k}) \right) \quad \text{and} \quad \Gamma 2_i = \frac{1}{g^{Kp_1}} \prod_{k=1}^{K} v_{i,k} v'_{i,k} \qquad (i = 1, \ldots, I)$$

by using the verifiable decryption D^*; (4) The AM1 publicly shows that both $\Gamma 1_i$ and $\Gamma 2_i$ have the p_0-th root. Thanks to this confirmation, any malicious bid vector can be detected by the cooperation of AM1 and AM2. Note that the AM2 does not know whether $v_{i,k}$ and $v'_{i,k}$ have the p_0-th root or not.

[Opening a winning bid:]

First, a winning bid is decided, then a winner is decided by the cooperation of both AM1 and AM2.

Step 1 The AM2 publicly computes the following values for $\mathcal{B}_i$:

$$E_Y(z_{i,K}), E_Y(z_{i,K-1}), \ldots, E_Y(z_{i,1}) = E_Y(v_{i,K}), E_Y(v_{i,K}v_{i,K-1}), \ldots, E_Y(\prod_{k=1}^{K} v_{i,k}).$$

for $i = 1, \ldots, I$, and then puts them in AM2's BBS.

Step 2 The AM2 publicly computes the following two kinds of values by multiplying $E_Y(z_{i,k})$ of all bidders for a bidding point k,

$$\begin{aligned} E_Y(Z_k) &= \prod_{i=1}^{I} E_Y(z_{i,k}) = \left(g^R,\ \left(\prod_{i=1}^{I} z_{i,k}\right) \cdot Y^R\right) = (G_k, M_k), \\ E_Y(Z'_k) &= \left(g^R,\ \frac{1}{g^{p_1}}\left(\prod_{i=1}^{I} z_{i,k}\right) \cdot Y^R\right) = (G_k, M'_k) \qquad k \in \{1, \ldots, K\}, \end{aligned}$$

where R is the sum of all bidder's random numbers in ElGamal encryption.

Step 3 The AM2 mixes $(E_Y(Z_k), E_Y(Z'_k))$ into $((E_Y(Z_k))^w, (E_Y(Z'_k))^w)$ using w relatively prime to p_0 and the technique of a verifiable w-th power mix in Section 6.4.4, and then publishes the following values:

$$\begin{aligned} (E_Y(Z_k))^w = E_Y({Z_k}^w) &= ({G_k}^w, {M_k}^w), \\ (E_Y(Z'_k))^w = E_Y({Z'_k}^w) &= ({G_k}^w, {M'_k}^w). \end{aligned}$$

The AM1 can publicly show that w is relatively prime to p_0 by using the verifiable w-th power mix in 6.4.4.

Step 4 The AM2 decrypts $\mathcal{X}_k = {Z_k}^w$ and $\mathcal{Y}_k = {Z'_k}^w$ from $E_Y({Z_k}^w)$ and $E_Y({Z'_k}^w)$ using the technique of a verifiable decryption, and publishes $(\mathcal{X}_k, \mathcal{Y}_k)$.

Step 5 The AM1 computes $\mathcal{M}(\mathcal{X}_k)$ and $\mathcal{M}(\mathcal{Y}_k)$, and publishes a tuple of $(\mathcal{X}_k, \mathcal{Y}_k, \mathcal{M}(\mathcal{X}_k), \mathcal{M}(\mathcal{Y}_k))$. A winning bid value is given by the highest bidding point with both $\mathcal{M}(\mathcal{X}_k) = 0$ and $\mathcal{M}(\mathcal{Y}_k) = 0$.

Since the values $\{t_{i,k}^{(0)}, t_{i,k}^{(1)}\}$ have the p_0-th root, g has neither p_0-th nor p_1-th root, and $\gcd(w, p_0) = 1$ holds, the following three cases are occurred for the values of $\mathcal{M}(\mathcal{X}_k)$ and $\mathcal{M}(\mathcal{Y}_k)$ in Figure 6.4:

1. If no bidder places a bid equal to or higher than the bidding point k, then $(\mathcal{M}(\mathcal{X}_k), \mathcal{M}(\mathcal{Y}_k)) = (1, 0)$.
2. If only one bidder places a bid equal to or higher than the bidding point k, then $(\mathcal{M}(\mathcal{X}_k),\ \mathcal{M}(\mathcal{Y}_k)) = (0, 1)$.
3. If more than two bidders place a bid equal to or higher than the bidding point k, then $(\mathcal{M}(\mathcal{X}_k),\ \mathcal{M}(\mathcal{Y}_k)) = (0, 0)$.

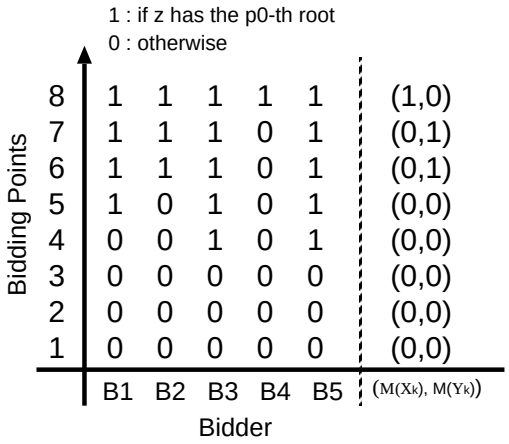


Figure 6.4: Opening Example

Note that we cannot distinguish between case 1 and case 2 because the AM2 uses the technique of a verifiable w-th power mix for $\mathcal{X}_k$ and $\mathcal{Y}_k$.

Public verifiability of a winning bid: The AM1 may rig a winning bid because only the AM1 computes $\mathcal{M}(\mathcal{X}_k)$ and $\mathcal{M}(\mathcal{Y}_k)$. In order to avoid rigging, the AM1 shows the following SPK:

$$SPK[(\alpha) : \mathcal{X}_k^{\alpha} = r_1 \wedge \mathcal{Y}_k^{\alpha} = r_2 \wedge \mathcal{X}_{k+1}^{\alpha} = r_3 \wedge \mathcal{Y}_{k+1}^{\alpha} = 1](m)$$

for given random numbers $r_1,\ r_2$ and r_3 $(r_1, r_2, r_3 \neq 1)$. This SPK means that only $\mathcal{Y}_{k+1}$ has the p_0-th root.

Furthermore, the cost of opening bids is $O(\log K)$ by adopting the technique introduced in [11, 18]: (1) For a set of bidding points $\{1, \ldots, K\}$, set $k_1 = 1, k_2 = K$ and $k' = \lfloor \frac{k_1+k_2}{2} \rfloor$; (2) If $k' = k_1$ or $k' = k_2$, then output k_2 as the second highest bid value; (3) If $\mathcal{M}(\mathcal{X}_{k'}) = 0$ and $\mathcal{M}(\mathcal{Y}_{k'}) = 0$, then set $k_1 = k'$ and $k' = \lfloor \frac{k_2+k'}{2} \rfloor$, and go to (2). Otherwise set $k_2 = k'$ and $k' = \lfloor \frac{k_1+k'}{2} \rfloor$, and go to (2).

[Winner decision:]

After a winning bid value k (the second highest bid) is decided, the AM2 decrypts all the values $v_{i,k+1}$ $(i = 1, \ldots, I)$ using the technique of a verifiable decryption. Anyone can confirm whether or not these values $v_{i,k+1}$ $(i = 1, \ldots, I)$ exist in AM1's BBS.

Public verifiability of a winner: In order to decide a winner $\mathcal{B}_j$, the AM1 shows the following SPK:

$$SPK[(\alpha) : (g^{p_0})^{\alpha} = 1 \wedge (v_{j,k+1})^{\alpha} = r_1](m)$$

for given random number r_1 $(r_1 \neq 1)$. This SPK means that $v_{j,k+1}$ does not have the p_0-th root. A winner $\mathcal{B}_j$'s bid is never revealed. If no bidder places a bidding point $k+1$, more than two winners place a bid at the bidding point k. This means that a winning bid is also k. The AM1 shows the following SPK:

$$SPK[(\alpha) : g^{\alpha} = r_2 \wedge (v_{1,k+1})^{\alpha} = 1 \wedge \cdots \wedge (v_{I,k+1})^{\alpha} = 1](m)$$

for given random number r_2 ($r_2 \neq 1$). This SPK means that all values $v_{i,k+1}$ ($i = 1, \ldots, I$) have the p_0-th root. Note that g does not have the p_0-th root.

6.6 Consideration

6.6.1 Properties

We discuss the following properties in our protocol.

(a) **Anonymity:** Unless both of the AMs collude, nobody can identify the bidder $\mathcal{B}_{sec}$ even if an anonymous channel is not used. Since all bid vectors are multiplied together before the opening phase, the bidder $\mathcal{B}_{sec}$ is never disclosed. If all bid values are disclosed in the bidding phase, the bidder $\mathcal{B}_{sec}$ is easily decided. Each bid value is protected by both hardness of the discriminant of the p_0-th root and the ElGamal encryption. So the identity of $\mathcal{B}_{sec}$ can be protected without using an anonymous channel.

(b) **Non-cancelability:** A winner cannot deny that she/he has submitted the highest bid after the winner decision procedure as long as both (c) and (e) are satisfied. Since the AM1 publicly shows the SPK(s) for the winner decision, a winner is certainly identified.

(c) **Public verifiability:** Anyone can publicly verify the correctness of an auction. An auction uses some tools based on the proof of knowledge in order to satisfy public verifiability. As long as the proofs of knowledges are secure, an auction process can be collect. As a result, both a winning bid and a winner become valid.

(d) **Unforgeability:** Nobody can impersonate a valid bidder $\mathcal{B}_i$ unless she/he knows x_i as well as the values $t_{i,1}^{(0)}, \ldots, t_{i,K}^{(0)}$ and $t_{i,1}^{(1)}, \ldots, t_{i,K}^{(1)}$.

(e) **Robustness:** Any malicious bid vector can be detected by AM1 and AM2. Unless a bidder uses the valid $v_{i,k}$ and $v'_{i,k}$, anybody notices that $H(v_{i,k})$ or $H(v'_{i,k})$ does not exist in AM1's database. Also, unless a bidder generates the valid V_i, the AM1 notices that $\Gamma 1_i$ and $\Gamma 2_i$ do not have the p_0-th root after the AM2 computes them. So no bidder can disturb the auction system by the malicious bid.

(f) **Fairness:** Any bidder can check whether her/his bid vector exists in AM2's BBS or not for an bidding phase. So any bid is fairly dealt with.

(g) **Efficiency of bidding:** This will be discussed in Section 6.6.2.

(ℓ) **Two independent AM's powers:** Our scheme is based on both RSA and ElGamal cryptosystems. Only the AM1 knows the prime factors of n, while only the AM2 knows the secret key of ElGamal encryption. Thanks to separation of two kinds of the cryptosystems, neither AM1 nor AM2 knows the highest bid value, a bidder $\mathcal{B}_{sec}$, and loosing bid values.

Table 6.1: The communicational costs

	A bidder ($\mathcal{B}$)		AM		
	Preparation	Bidding	Preparation	Opening × Round	#AM
NPS	$O(\log K)$	$O(\log K)$	$O(I \log K)$	$O(I) \times 2$	2
AS	–	$O(K)$	–	$O(1) \times \lceil \log K \rceil$	2
Ours	–	$O(K)$	$O(IK)$	$O(1) \times \lceil \log K \rceil$	2

(m) **Secrecy of loosing bids:** Our scheme keeps loosing bids secret unless both of AMs collude. This feature can be discussed similar to (p).

(o) **Efficiency of opening:** This will be discussed in Section 6.6.2.

(p) **Secrecy of the highest bid:** Our scheme keeps the highest bid secret unless both the AMs collude. Nobody can know the information about the highest bid except that it is placed higher than the second highest bid value. Each element $v_{i,k}$ ($z_{i,k}$) has information about whether it has the p_0-th root or not. So only AM1 who knows the products of n realizes the bid values from the values $v_{i,k}$ ($z_{i,k}$). However, such a bid value is encrypted by ElGamal encryption of AM2, and the values $v_{i,k}$ ($z_{i,k}$) themselves are never revealed in the auction procedure. Therefore, AM1 cannot know bid values as long as the ElGamal encryption is secure. Also, AM2 cannot realize bid values because she/he does not know the products of n, even if AM2 knows the values $v_{i,k}$ ($z_{i,k}$). By applying the verifiable w-th power mix to step 3 of the opening phase, the highest bid value can be hidden. Since the AM1 can publicly show that w is relatively prime to p_0, the highest bid value remains correct.

Our scheme does not have such a single entity, and it is based on both RSA and ElGamal cryptosystems. Only the AM1 knows the prime factors of n, while only the AM2 knows the secret key of ElGamal encryption. Thanks to the separation of two kinds of cryptosystems, neither AM1 nor AM2 knows the highest bid value, a bidder $\mathcal{B}_{sec}$, and loosing bid values.

6.6.2 Performance

We compare our scheme with the previous two schemes from the viewpoints of the communicational and computational costs in Table 6.1, 6.2 and 6.3. Here let the number of bidding points and bidders be K and I, respectively.

Table 6.1 shows the communicational amount of bidding and between the AMs. In the NPS-scheme, the bidding cost is of $O(\log K)$ for a bidder because each bidder encrypts each bit of binary representation of her/his bid. A bidder and the AM need the additional costs of $O(\log K)$ and $O(I \log K)$ in average, respectively, for the sake of public verifiability. It needs to introduce the cut-and-choose technique in order to satisfy public verifiability. If π-time auction is required, it costs $O(\pi I \log K)$ as the additional cost, where π is the secure parameter of cut-and-choose. So the additional cost in an auction is of $O(I \log K)$ in average. In both the SA-scheme and our scheme, only $\lceil \log K \rceil$ rounds

Table 6.2: The computational costs ($\mathcal{B}$)

	#Enc	#Proof	Preparation
NPS	$4\lceil \log K \rceil$	–	$4\lceil \log K \rceil$ Encryptions
AS	K	$K+1$	–
Ours	$2K$	–	–

Table 6.3: The computational costs (AM)

	#Enc	#Proof	#Multiplication	Bid check	#Dec
NPS	$2I\lceil \log K \rceil$	–	–	$O(I \log K)$	$4I\lceil \log K \rceil$
AS	–	–	$IK + I\lceil \log K \rceil$	$O(IK)$	$2\lceil \log K \rceil + I$
Ours	IK	$I(K+1)$	$2(IK + I\lceil \log K \rceil)$	$O(I)$	$2\lceil \log K \rceil + 2I(K+1)$

of communication are required in the opening phase because of binary search. In the auction preparation of our scheme, the AM1 must send K ElGamal encryption data to each bidder.

Table 6.2 shows the computational complexity of a bidder. In the NPS-scheme, each bidder needs $4\lceil \log K \rceil$ ElGamal encryptions in the bidding phase. Furthermore, in order to realize public verifiability, each bidder needs the additional $4\lceil \log K \rceil$ ElGamal encryption in average. In the SA-scheme, each bidder requires the $K+1$ proofs to avoid the malicious bidding. In our scheme, each bidder does not need to make such proofs, but the AM2 generates $K+1$ proofs for I bidders.

Table 6.3 shows the computational complexity of the AM. In the NPS-scheme, when the AM1 sends all bidder's bid to the AM2 in return, the AM1 must encrypt them again. So the AM1 needs $2I\lceil \log K \rceil$ ElGamal encryptions. A program checks each bid secretly, and its cost is of $O(I \log K)$. Both AM1 and AM2 need $2I\lceil \log K \rceil$ ElGamal decryptions, respectively. In the SA-scheme, the AM needs the bid checking of the cost $O(IK)$ in order to verify the proofs. In our scheme, the AM2 needs the bid checking of the cost only $O(I)$ because it uses the sum of all bid vectors. The AM1 needs IK ElGamal encryptions for an auction preparation. As for the number of decryption, our scheme requires $2IK$ times in generating proofs, I times in the bid checking, $2\lceil \log K \rceil$ times in the opening phase, and I times in the winner decision phase.

6.7 Summary

We have proposed an electronic second-price sealed-bid auction which mainly satisfies (a) Secrecy of the highest bid, (b) Anonymity of the second-price bid, (c) Public verifiability, and (g) Two independent AM's powers. In our scheme, there is no single entity who knows the highest bid value, a bidder $\mathcal{B}_{sec}$, and loosing bid values. Also, each bidder does not have to compute the zero-knowledge proofs, but the AM computes such proofs. So

the computational cost of bidder is lower.

Chapter 7

Discussion

We discuss three kinds of proposed schemes from the viewpoints of several features, bidder privacy and correctness of a winning bid.

7.1 Comparison of Proposed Schemes

We compare the features of our schemes in Table 7.1. Here let the number of bidding points and bidders be K and I, respectively.

First, all of our proposed schemes realize public verifiability of a winner and a winning bid. In Scheme I, we do not consider public verifiability of a winning bid because it publishes all bid values. All of our schemes do not have a single authority who can break anonymity and secrecy of bids. If such an authority exists, he may leak the information who wants to buy a good or how much is the good for each bidder.

As for the cost of bidding, in an English auction, efficiency of bidding is more important than that of auction preparation and winner decision. Scheme I is the most efficient, which has order of $O(1)$. Furthermore, it realizes simple revocation: a bidder can withdraw from an auction efficiently in one-time registration. In Scheme II, there is only a single AM who cannot break anonymity of bidder. Furthermore, it has a feature of entertainment: many participants enjoy the opening phase. Scheme III satisfies secrecy of the highest bid, which is hard to realize than secrecy of loosing bids. This is why the opening cost in Scheme III is relatively large.

Table 7.1: Comparison of proposed schemes

	Scheme I	Scheme II	Scheme III
Public verifiability	Winner	Winner Wining bid	Winner Wining bid
Bidding cost	$O(1)$	$O(\log K)$	$O(K)$
Opening cost	–	$O(I)$	$O(I \log K)$
#AM	2	1	2
Remarkable features	Simple revocation	Entertainment	Secrecy of highest bid

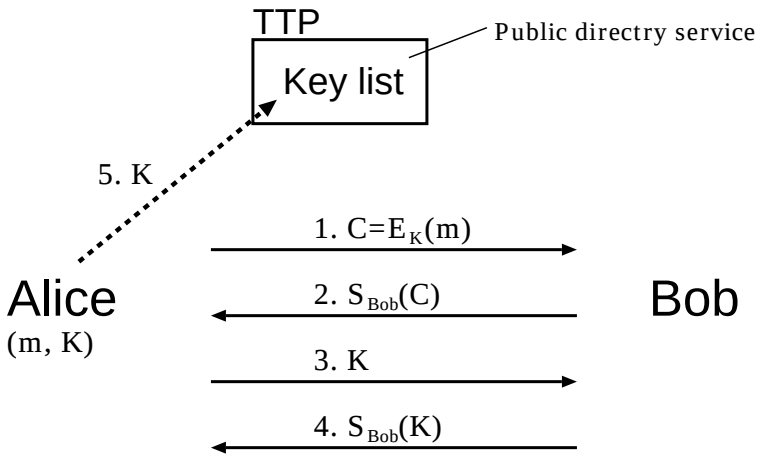


Figure 7.1: Non-repudiation protocol

7.2 Fairness

Fairness of bidder in an electronic auction means that any bid is fairly accepted by the AM. Note that we do not consider unfairness by network collision here because it can impartially happen to any bidder. There are two unfairness acts by the AM:

1. The AM repudiates any bidding by a certain bidder.
2. The AM repudiates any higher bid than a certain value.

In order to avoid case 1, a bidder has only to place a bid anonymously. Our three kinds of schemes can avoid the unfairness of case 1 because the bidding is done anonymously. Especially, in our schemes, there is no single entity who can break anonymity. Therefore the AM cannot repudiate the bidding by a certain bidder.

In order to avoid the unfairness of case 2, a bidder has to conceal a bid value for the AM. In the SB auction, the AM cannot do unfairness act of the case 2. Also, in our SB auction schemes, the AM cannot repudiate the higher bids than a certain value. However, since each bid value is public in English auction, the AM may make up the false network trouble to repudiate the higher bids in such an auction scheme. To avoid case 1 in our proposed English auction scheme (Scheme I), we may use *non-repudiation protocol*[22, 50, 51].

Non-repudiation protocol:

The non-repudiation protocol is that Alice sends a message to Bob and then Bob cannot repudiate a receipt of the message from Alice. We summarize the basic procedure (Figure 7.1).

1. Alice encrypts a message m into C and sends it to Bob.
2. He sends his signature $S_{Bob}(C)$ back to her after receiving C.
3. She sends the decryption key K of C to him after receiving $S_{Bob}(C)$.

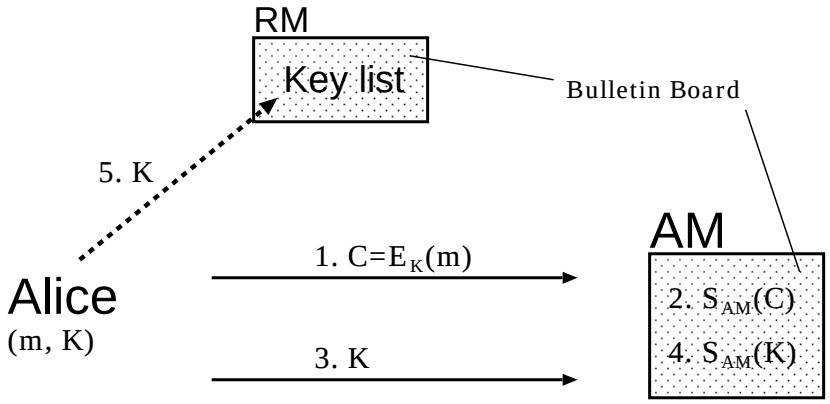


Figure 7.2: Bidding procedure with non-repudiation

Note that if Bob repudiates K after the deadline, she deposits K in the TTP (Alice cannot know whether Bob repudiates K or the network between Alice and Bob is broken down). The TTP publishes K using public directory service as soon as the TTP receives it. Bob cannot deny receiving a message m if the network between Bob and the TTP is not permanently broken down.

7.2.1 Bidding procedure with non-repudiation

We can apply the non-repudiation protocol to the bidding phase in Scheme I. Fairness of bidder is realized by introducing an idea of non-repudiation protocol as above. Alice and Bob correspond to a bidder and the AM, respectively (Figure 7.2). The RM also plays a role of the TTP. In our protocol both RM and AM use the BBSs. A bid m is placed as follows:

1. The AM cannot know each bid value because her bid information C is encrypted.
2. The AM publishes his signature $S_{AM}(C)$ in AM's BBS instead of returning it because the AM does not know who a bidder is.
3. Even if the AM repudiates a receipt of decryption key K from a bidder, the AM cannot deny getting bid information because the RM publishes K in RM's BBS.

7.3 Bidder Privacy

An electronic auction is not face-to-face auction. If the AM publishes all of bidder's identities and bid values after an auction, anybody will accept the auction results. This auction system satisfies public verifiability. However, in such an auction system, much information can be selected and gathered, and then their information may be bought and sold through illegal channels. A bidder does not want to participate such an auction. Therefore we need to show the correctness of auction results without their information secret.

As for strict privacy of bidder, it is also desired that loser's identities and loosing bid values are not revealed for the AM. The AM may sell their information to the black market. There should not exist such the AM who easily stores much information of who wants a good and a bidder's history of bidding. We need to realize public verifiability with keeping their information secret from the AM though realizing such public verifiability makes the auction system complicated. For the sake of bidder's privacy, such public verifiability is necessary for an electronic auction system even if it makes the system complicated. Our proposed schemes also keep their information secret from the AM as well as participants.

Scheme I separates anonymity into two managers by the shuffling of auction keys, two kinds of the BBSs, and the proof of knowledge. Unless two managers collude, anonymity of bidder is satisfied. Scheme II uses the anonymous broadcast network to protect anonymity for a single AM. There is a single AM who cannot break anonymity. Scheme III uses the discriminant function of the p_0-th root and verifiable w-th power mix to conceal both the highest bid value and the identity of $\mathcal{B}_{sec}$. Unless two AMs collude, both of their secret values are never disclosed.

In Scheme II and III, we set the bidding points, in which each bidder cannot place a bid as she/he likes. However, the setting is necessary for the sake of secret computing of a winning bid.

As for privacy of a winner, in a first-price SB auction, the correspondence of a winner to her/his bid is revealed for the participants. On the other hand, in a second-price SB auction, the correspondence of winner to her/his bid is not revealed for the participants because a winning bid is different from the bid that a winner placed. Therefore a second-price SB auction keeps privacy of a winner better than a first-price SB auction.

7.4 Correctness of Winning Bid

Since an English auction publishes all bid values, anybody can verify the correctness of a winning bid. Also, in the SB auction, any participant can check the correctness of a winning bid, which is the output of secret computing with public verifiability (see Figure 3.2, 3.5). However, if the scheme does not satisfy secrecy of the bid value for the AM in the middle of SB auction, the AM can know the highest bid value in an auction. It is valuable to get the highest bid value in the middle of the SB auction.

Here suppose that the AM knows the highest bid value in the middle of auction. Such the AM can place a little higher bid than the highest bid in the end of auction as a valid bidder. AM may divulge the highest value to the bidder who wants to get the good by all means. As a result, the bidder will place a little higher bid.

In the second-price SB auction, what made it even worse is that the highest bid value is valuable for a seller . If AM places a little lower bid than the highest bid as a valid bidder, the winning bid (the second highest bid) becomes higher. AM may also sell the information to a seller as well as a bidder (AM's illegal act). In this case, a seller benefits the max, and also even a winner does not notice that the second highest bid is manipulated because the winning bid is different from winner's. If the AM divulges the highest bid value to a seller, the seller can make a profit and may give a part of profit to the AM in return for AM's information. That is why it is important to distribute AM's power like

our Scheme III.

7.5 English auction vs. Second-price SB auction

From Section 6.2 we wonder if a second-price SB auction is superior to English auction. Actually, however, an English auction is much more popular than a second-price SB auction. We think two reasons why a second-price SB auction is unpopular as follows:

1. A winning bid value is not winner's.

2. It is hard for each bidder to decide her/his true value in advance.

If the AM knows the highest bid value in the middle of auction, the AM may place a little lower bid than the highest bid as a valid bidder. In this case, a winning bid almost becomes winner's true value. Even a winner does not parceive such AM's handling. As long as the AM knows the highest bid value in the middle of auction, the bidder will not want to participate in the second-price SB auction. Such AM's handling cannot be happen in English auction. This is why secrecy of the highest bid is necessary for an authority in the second-price SB auction. Our Scheme III, which distributes AM's power, may make contribution in order to spread the second-price SB auction.

In the case 2, a bidder must decide her/his true value for the dominant strategy in advance. However, the bidder $\mathcal{B}_{sec}$ may change her/his true value in the middle of the auction. The true value depends on bidder's mood whether the bidder wants to buy the good. After an auction, $\mathcal{B}_{sec}$'s true value may be higher than the winner's bid value. Then $\mathcal{B}_{sec}$ may regret her/his bid. In an English auction, a bidder can raise her/his true value in the middle of auction.

Chapter 8

Conclusion

8.1 Sumarry

In this thesis, we have explored three kinds of auction schemes from the viewpoints of bidder privacy, correctness of system and efficiency. As for bidding privacy, our proposed auction schemes satisfy anonymity for a single authority. Anonymity for a single authority is important to protect the information of who wants a good and a bidder's history of bidding. Our second-price SB auction scheme keeps the highest bid value secret from the AMs (Chapter 6). As for correctness of system in the SB auction, the auction system needs the secret computing in order to satisfy secrecy of bids, and thus it should satisfy public verifiability of a winning bid. In our SB auction schemes, any participant can publicly verify the auction results (Chapter 5, 6). As for efficiency, our auction schemes are reasonable compared with the previous schemes. In our English auction scheme, the computational and communicational costs for one bidding is more efficient (Chapter 4).

The following is a summary of research results for our auction schemes.

An English auction scheme (Scheme I): This scheme realizes an English auction without using a group signature, but it has the properties that the group signature scheme has. Since our scheme applies two kinds of BBSs well, the computational and communicational costs for one bidding are much reduced compared with the previous schemes[7, 31]. Furthermore in our scheme a bidder can easily revoked if necessary.

A first-price SB auction scheme (Scheme II): This scheme has only the single AM who cannot break anonymity of bidder. Also, in the same way of English auction, many participants can enjoy the opening phase by decreasing winner candidates little by little. Since our scheme uses hash chain technique in bid vector, public verifiability of a winning bid is satisfied.

A second-price SB auction scheme (Scheme III): Since this scheme needs to compute the second highest bid value with both the highest bid and loosing bids secret, it should publicly show the correctness of the auction results. Our scheme realizes secrecy of the highest bid with public verifiability by using techniques of the signature of knowledge, the discriminant function of the p_0-th root, verifiable decryption of ElGamal scheme, verifiable w-th power mix, and verifiable decryption mix.

8.2 Application to Electronic Auctions

We should change the auction type to suit the occasion. A business does not like an English auction as a trade system because it pubushes all bid values. A business wants to conceal its ceiling price on trading. Therefore the secret trade such as the SB auction is suitable for a business well. Although the SB auction scheme is not as efficient as English auction scheme, a business will prefer the SB auction with keeping bid values secret.

On the other hand, a personal buyer prefers an English auction because it has a feature of entertainment, in which many participants can enjoy an auction process. In an English auction scheme, the bidding is much more efficient than that in the SB auction schemes because the secret computing is not necessary. An English auction is suitable for a personal bidder because the computing power of personal bidder is lower than that of enterprise.

We should also consider such actual requirements realizing the electronic auction schemes. Auction types depend on requirements of participants.

8.3 Proxy Bidding

Recently, an electronic English auction like Yahoo auction[49] introduces an automatic agent system called "proxy bidding" mentioned in [18]. First, we explain the proxy bidding in detail, and then we describe the problem in it.

Suppose that the AM sets the bidding points $\{1, \ldots, K\}$. In a proxy bidding, a bidder $\mathcal{B}_i$ secretly sets the ceiling price $C_i \in \{1, \ldots, K\}$ which $\mathcal{B}_i$ can pay. The AM has to keep the value C_i secret from participants. If someone else $\mathcal{B}_j$ places the bid $k_j \in \{1, \ldots, K\}$ $(< C_i)$, the AM updates the current bid value into $k_j + 1$. Unless the current bid value $k_j + 1$ is lower than C_i in the end of auction, the bidder $\mathcal{B}_i$ becomes a winner in the winning bid value $k_j + 1$. $\mathcal{B}_i$'s ceiling price C_i should be kept secret even after an auction.

If the system applies such a proxy bidding to English auction, it is similar to the second-price SB auction because a winning bid value is decided by the second highest bid value. The ceiling price C_i means $\mathcal{B}_i$'s true value in the second-price SB auction. Once a bidder sets her/his ceiling price, she/he does not have to check the current bid value for the time being. This style of auction has a good point that $\mathcal{B}_i$ can change the value C_i in the middle of auction. The proxy bidding also has a feature of entertainment such as an English auction. That is why the proxy bidding becomes popular.

Actually, however, such a proxy bidding has the problem that AM knows bidder's ceiling price. A bidder wants to keep her/his ceiling price secret from the AM as well as participants. AM may sell the highest ceilling price C_{max} of all bidders' through illegal channels. If a seller places the bid $C_{max} - 1$ after he knows the value C_{max}, he benefits the max. A seller never become a winner as long as he places a little lower bid than C_{max}. We expect that such a problem will be solved in an electronic proxy bidding.

Bibliography

[1] M. Abe and K. Suzuki. "M+1-st Price Auction Using Homomorphic Encryption". In *Proceedings of the 5-th International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2002),* LNCS, Springer-Verlag, page to appear, 2002.

[2] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. "A Practical and Provably Secure Coalition-Registant Group Signature Scheme". In *Advances in Cryptology – CRYPTO 2000,* LNCS 1880, Springer-Verlag, pages 255–270, 2000.

[3] G. Ateniese and G. Tsudik. "Some Open Issues and New Directions in Group Signatures". In *Proceedings of the Third International Financial Cryptography Conference, (FC '99),* LNCS 1648, Springer-Verlag, pages 196–211, 1999.

[4] E. Bresson and J. Stern. "Efficient Revocation in Group Signatures". In *Proceedings of the 4-th International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2001),* LNCS 1992, Springer-Verlag, pages 190–206, 2001.

[5] C. Cachin. "Efficient Private Bidding and Auctions with an Oblivious Third Party". In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 120–127, 1999.

[6] J. Camenisch. "Efficient and Generalized group signatures". In *Advances in Cryptology – EUROCRYPT '97,* LNCS 1233, Springer-Verlag, pages 465–479, 1997.

[7] J. Camenisch and M. Michels. "A Group Signature Scheme with Improved Efficiency". In *Advances in Cryptology – ASIACRYPT '98,* LNCS 1514, Springer-Verlag, pages 160–174, 1998.

[8] J. Camenisch and M. Michels. "Separability and Efficiency for Generic Group Signature Schemes". In *Advances in Cryptology – CRYPTO '99,* LNCS 1666, Springer-Verlag, pages 106–121, 1999.

[9] J. Camenisch and M. Stadler. "Efficient Group Signature Schemes for Large Groups". In *Advances in Cryptology – CRYPTO '97,* LNCS 1294, Springer-Verlag, pages 410–424, 1997.

[10] D. Chaum and E. van Heyst. "Group signatures". In *Advances in Cryptology – EUROCRYPT '91,* LNCS 547, Springer-Verlag, pages 257–265, 1991.

[11] K. Chida, K. Kobayashi, and H. Morita. "Efficient Sealed-bid Auctions for Massive Numbers of Bidders with Lump Comparison". In *Proceedings of the 4th Information Security Conference (ISC 2001),* LNCS 2200, Springer-Verlag, pages 408–419, 2001.

[12] W. Diffie and M. Hellman. "New direction in cryptography". *IEEE Trans. on Information Theory*, pages 644–654, November 1976.

[13] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. on Information Theory*, Vol.31:pp.469–472, 1985.

[14] M. Franklin and M. Reiter. "The design and implementation of a secure auction service". *IEEE Trans. on Software Engineering*, Vol.22,No.5:pp.302–312, 1996.

[15] M. Harkavy, D. Tyger, and H. Kikuchi. "Electronic Auctions with Private Bids". In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, 1998.

[16] Y. Imamura, T. Matsumoto, and H. Imai. "Electronic Anonymous Bidding Schemes". In *Proceedings of Symposium on Cryptography and Information Security (SCIS '94)*, 1994.

[17] M. Jakobsson and A. Juels. "Mix and Match: Secure Function Evaluation via Ciphertexts". In *Advances in Cryptology – ASIACRYPT 2000,* LNCS 1976, Springer-Verlag, pages 162–177, 2000.

[18] H. Kikuchi. "(M+1)st-Price Auction Protocol". In *Proceedings of the 5th International Financial Cryptography (FC 2001),* LNCS, Springer-Verlag, page to appear, 2001.

[19] H. Kikuchi, M. Harkavy, and D. Tyger. "Multi-round anonymous auction protocols". In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62–69, 1998.

[20] J. Kilian and E. Petrank. "Identity Escrow". In *Advances in Cryptology – CRYPTO '98,* LNCS 1462, Springer-Verlag, pages 169–185, 1998.

[21] H. Kim, J. Lim, and D. Lee. "Efficient and Secure Member Deletion in Group Signature Schemes". In *Proceedings of the Third International Conference on Information Security and Cryptology (ICISC 2000),* LNCS 2015, Springer-Verlag, pages 150–161, 2000.

[22] K. Kim, S. Park, and J. Baek. "Improving fairness and privacy of ZhouGollmann 's fair non-repudiation protocol". In *Proceedings of 1999 ICPP Workshops on Security (IWSEC)*, pages 140–145, 1999.

[23] K. Kobayashi, H. Morita, K. Suzuki, and M. Hakuta. "Efficient Sealed-bid Auction by Using One-way Functions". *IEICE Trans. Fundamentals*, Vol.E84-A,No.1:pp.289–294, 2001.

[24] M. Kudo. "Secure electronic sealed-bid auction protocol with public key cryptography". *IEICE Trans. Fundamentals*, Vol.E81-A,No.1:pp.20–27, 1998.

[25] M. Kumar and S. Feldman. "Internet Auctions". In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, pages 49–60, 1998.

[26] B. Lee, K. Kim, and J. Ma. "Efficient Public Auction with One-time Registration and Public Verifiability". In *Progress in Cryptology – INDOCRYPT 2001,* LNCS 2247, Springer-Verlag, pages 162–174, 2001.

[27] M. Manbo and H. Shizuya. "A Note on the Complexity of Breaking Okamoto-Tanaka ID-Based Key Exchange Scheme". *IEICE Trans. Fundamentals*, Vol.E82-A,No.1:77–80, 1999.

[28] T. Mullen and M.Wellman. "The auction manager: Market middleware for large-scale electronic commerce". In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, pages 49–60, 1998.

[29] T. Nakanishi, T. Fujiwara, and H. Watanabe. "An Anonymous Bidding Protocol without Any Reliable Center". *Trans. IPS Japan*, Vol.41,No.8:pp.2161–2169, 2000.

[30] M. Naor, B. Pinkas, and R. Sumner. "Privacy Preserving Auctions and Mechanism Design". In *Proceedings of ACM Conference on Electronic Commerce*, pages 120–127, 1999.

[31] K. Nguyen and J. Traoré. "An Online Public Auction Protocol Protecting Bidder Privacy". In *Proceedings of the 5th Australasian Conference on Information and Privacy (ACISP 2000),* LNCS 1841, Springer-Verlag, pages 427–442, 2000.

[32] NIST. "Secure Hash Standard (SHS)". In *FIPS Publication 180-1*, April 1995.

[33] K. Omote and A. Miyaji. "A Second-price Sealed-bid Auction with the Discriminant Function of the p_0-th Root". In *Proceedings of the 6th International Financial Cryptography (FC 2002).*

[34] K. Omote and A. Miyaji. "An Anonymous Auction Protocol with a Single Non-trusted Center using Binary Trees". In *Proceedings of Information Security Workshop (ISW 2000),* LNCS 1975, Springer-Verlag, pages 108–120, 2000.

[35] K. Omote and A. Miyaji. "A Practical English Auction with One-time Registration". In *Proceedings of the 6th Australasian Conference on Information and Privacy (ACISP 2001),* LNCS 2119, Springer-Verlag, pages 221–234, 2001.

[36] K. Omote and A. Miyaji. "An Anonymous Sealed-bid Auction with a Feature of Entertainment". *Trans. IPS Japan*, Vol.42,No.8:pp.2049–2056, 2001.

[37] K. Omote and A. Miyaji. "A Practical English Auction with Simple Revocation". *IEICE Trans. Fundamentals*, Vol.E85-A,No.5:to appear, 2002.

[38] C-S. Peng, M. Pulido, J. Lin, and M. Blough. "The Design of an Internet-based Real Time Auction Systems". In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 70–78, 1998.

[39] R. Rivest. The md5 message-digest algorithm. In *RFC1321*, April 1992.

[40] R. Rivest and A. Shamir. "PayWord and MicroMint: Two Simple Micropayment Schemes". In *Proceedings of Security Protocols,* LNCS 1189, Springer-Verlag, pages 69–87, 1996.

[41] R. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM*, Vol.21,No.2:pp.120–126, 1978.

[42] K. Sako. "An Auction Protocol Which Hides Bids of Losers". In *Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000),* LNCS 1751, Springer-Verlag, pages 422–432, 2000.

[43] K. Sakurai and S. Miyazaki. "An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme". In *Proceedings of the 5th Australasian Conference on Information and Privacy (ACISP 2000),* LNCS 1841, Springer-Verlag, pages 385–399, 2000.

[44] C. Schnorr. "Efficient Signature Generation by Smart Cards". *Journal of Cryptology*, Vol.4,No.3:pp.161–174, 1991.

[45] A. Shamir. How to share a secret. *Communications of the ACM*, Vol.22,No.11:pp.612–613, 1979.

[46] Stuart G. Stubblebine and Paul F. Syverson. "Fair On-line Auctions Without Special Trusted Parties". In *Proceedings of the Third International Financial Cryptography (FC '99),* LNCS 1648, Springer-Verlag, pages 230–240, 1999.

[47] K. Suzuki, K. Kobayashi, and H. Morita. "Efficient Sealed-bid Auction Using Hash Chain". In *Proceedings of the Third International Conference on Information Security and Cryptology (ICISC 2000),* LNCS 2015, Springer-Verlag, pages 189–197, 2000.

[48] W. Vickrey. "Counter Speculation, Auctions, and Competitive Sealed Tenders". *Journal of Finance*, Vol.16:pp.8–37, 1961.

[49] Yahoo. "http://auctions.yahoo.com".

[50] J. Zhou and D. Gollmann. "A fair non-repudiation protocol". In *Proceedings of 1996 IEEE Symposium on Security and Privacy*, pages 55–61, 1996.

[51] J. Zhou and D. Gollmann. "An efficient non-repudiation protocol". In *Proceedings of the 10th Computer Security Foundations Workshop (PCSFW). IEEE Computer Society Press*, 1997.

Publications

[1] K. Omote and A. Miyaji. "An Anonymous Auction Protocol with a Single Non-trusted Center Using Binary Trees". In *Proceedings of the 2000 Symposium on Cryptography and Information Security*, **SCIS 2000–B48**, 2000.

[2] K. Omote and A. Miyaji. "A Practical Anonymous English Auction by Using Bulletin Boards". *IEICE Technical Report*, **ISEC 2000–85**, Nov. 2000.

[3] K. Omote and A. Miyaji. "An Anonymous Auction Protocol with a Single Non-trusted Center Using Binary Trees". In *Proceedings of Information Security Workshop*, **ISW 2000**, LNCS 1975, Springer-Verlag, pp.108–120, 2000.

[4] K. Omote and A. Miyaji. "A Practical English Auction with One-time Registration". *IEICE Technical Report*, **ISEC 2000–136**, Mar. 2001.

[5] K. Omote and A. Miyaji. "A Practical English Auction with One-time Registration". In *Proceedings of the 6th Australasian Conference on Information and Privacy*, **ACISP 2001**, LNCS 2119, Springer-Verlag, pp.221–234, 2001.

[6] K. Omote and A. Miyaji. "An Anonymous Sealed-bid Auction with a Feature of Entertainment". In *Trans. IPS Japan*, **Vol. 41**, **No. 8**, pp.2049–2056, 2001.

[7] K. Omote and A. Miyaji. "A Second-price Sealed-bid Auction Scheme with the Discriminant Function of the p-th Root". In *Proceedings of Computer Security Symposium 2001*, **CSS 2001**, pp.43–48, 2001.

[8] K. Omote and A. Miyaji. "An English Auction with Complete Unlinkability among Plural Auctions". *IEICE Technical Report*, **ISEC 2001–11**, Nov. 2001.

[9] K. Omote and A. Miyaji. "A Second-price Sealed-bid Auction Scheme with a feature of Public Verifiability". In *Proceedings of the 2002 Symposium on Cryptography and Information Security*, **SCIS 2002**, pp.855–860, 2002.

[10] K. Omote and A. Miyaji. "A Second-price Sealed-bid Auction with the Discriminant Function of the p_0-th Root". In *Proceedings of Financial Cryptography*, **FC 2002**, LNCS, Springer-Verlag, page to appear, 2002.

[11] K. Omote and A. Miyaji. "A Practical English Auction with Simple Revocation". In *IEICE Trans. Fundamentals*, **Vol. E85–A**, **No. 5**, page to appear, May 2002.