Improved Double Auction Protocol based on a Hybrid Trust Model

JungHoon Ha
School of Electrical Eng. & Computers Science, Kyungpook National Univ., Daegu, Korea
Email: short98@ee.knu.ac.kr

Jianying Zhou
Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore
Email: jyzhou@i2r.a-star.edu.sg

SangJae Moon
School of Electrical Eng. & Computers Science, Kyungpook National Univ., Daegu, Korea
Email: sjmoon@ee.knu.ac.kr

Abstract— **Recently, Wang *et al.* proposed a set of double auction protocols with full privacy protection based on distributed ElGamal encryption. Unfortunately, their protocols are expensive in computation, and are not robust in dealing with system malfunction or user misbehavior. In this paper, we propose a secure and practical double auction protocols based on a hybrid trust model, where computation load is distributed to buyers and sellers while a semi-trusted manager handles the registration phase. A prominent feature of the proposed protocol is its high robustness, achieved by using a publicly verifiable secret sharing scheme with threshold access structure.**

Index Terms—**Double auction, security, trust model**

I. INTRODUCTION

Currently, many auction services exist on the Internet that satisfies a variety of requirements. Auction protocols can be classified into two types, namely *one-sided auction protocols* in which a single seller (or buyer) accepts bids from multiple buyers (or sellers), and two-sided or *double auction protocols* in which multiple buyers and sellers are permitted to bid/ask[1] for designated goods [1]. For one-sided auctions, such as English auction, Vickrey auction and sealed-bid auction, there have been many papers in the literature considering various security properties [2,3]. However, not much research has been done regarding the security issues in double auctions.

Recently, Wang and Leung proposed a set of double auction protocols with full privacy protection [4], in which trust and computation are distributed among sellers and buyers themselves.

Although their protocols possess good security properties, they are expensive in computation and weak in robustness. Specifically, to identify the winning buyers

and sellers in an auction after the determination of the trading price, all participating buyers and sellers are required to perform a distributed ElGamal decryption.

The auction process fails even if only one seller or buyer does not contribute to the distributed decryption. This requirement is apparently too strong and therefore impractical - lost or failed buyers and sellers may refuse to corporate or drop out from the auction session early; even if all buyers and sellers are willing to perform the distributed decryption, they may be cut off from the auction session due to system or network malfunctions.

In this paper, we propose a secure, efficient and highly robust double auction protocols based on McAfee's and Yokoo's protocols. The high robustness of the protocols is realized by using a publicly verifiable secret sharing scheme with threshold access structure. In our protocols, the computation related to the determination of winning traders is distributed to all the buyers and sellers; however, a participation of a subset of buyers and sellers is sufficient for an auction session to be successfully completed. In addition, to meet most of the properties for a secure double auction, we employ a *semi-trusted* manager who is only trusted not to disclose the pseudonyms of participants until the announcement stage of winners.

The rest of this paper is structured as follows. Section 2 specifies the requirements for secure double auctions and introduces our assumptions. Section 3 reviews the necessary cryptographic primitives, and Section 4 presents our secure and practical double auction protocols. We analyze security and efficiency of our protocols in Section 5, and discuss the characteristics of TPD protocol in Section 6. Finally, Section 7 contains our conclusions.

II. REQUIREMNETS AND ASSUMPTIONS

A. Requirements for Secure Double Auction

Security requirements for secure double auctions are similar to these for one-sided auctions. The following

---

[1] We use the term bid for a buyer's declaration of value, and *ask* for a seller's declaration of value.

properties that are desirable in secure electronic auction systems have been identified in the literature [5].

- *Anonymity*: During the auction process, identities of participants remain confidential except winners identification or user misbehavior.
- *Impossibility of Impersonation*: No one can impersonate any other traders.
- *Robustness and Correctness*: Malicious behavior of any party should not collapse the system or lead to an incorrect result. That is, if some party acts honestly, the correct trading price and winners will be identified according to auction rules.
- *Non-repudiation*: All participants including the winning and lost buyers/sellers cannot deny that they have submitted bids/asks.
- *Public Verifiability*: Everybody can verify the validity of asks/bids and can confirm whether asks/bids are submitted from valid participants or not.

B. Assumptions and Model

In most of the previous secure auction protocols, trust models can be classified into three types. In the *threshold trust model*, there are m auctioneers, out of which a fraction are assumed to be trustworthy [6]. The *third-party trust model* assumes a third party who is not fully trusted but does not collude with other parties including auctioneers [7]. The *buyer/seller self-resolving model* distributes trust to all the buyers/sellers [8]. These models might be selected based on the security requirements and the application environments. However, any of these trust models alone cannot achieve most of the properties for secure double auction.

In our proposed double auction protocols, we employ a hybrid model with the relevant assumptions. First, we distribute both trust and computation for the determination of winners and trading price to buyers and sellers themselves. With a publicly verifiable secret sharing scheme based on a threshold access structure, the proposed auction protocols work well even if some buyers or sellers do not fully corporate in an auction process due to an unstable network or malicious behaviors, so that it can achieve flexibility and robustness. Second, we make use of a semi-trusted manager who is assumed not to release the pseudonyms of participants except at the winner announcement stage or because of user misbehavior. The manager may impersonate a valid trader and illegally attend an auction using an auction ticket of other participants. However, the manager's action can be monitored by buyers and sellers, thus his misbehavior can be detected.

III. CRYPTOGRAPHIC PRIMITIVES

A. Signature of Knowledge

We use the signature of knowledge introduced by B. Lee *et al.* [9] as anonymous signature, in which they extended the signature of knowledge discrete logarithm introduced by Camenisch and Stadler [10].

That is, it can be used as an anonymous signature if (y^r, g^r) are challenged for a secret random number $r \in Z_q$ instead of (y, g) of Camenisch and Stadler' scheme. The signer computes (c, s) satisfying $c = (m \| y^r \| g^r \| (g^r)^s \cdot (y^r)^c)$ for challenged (y^r, g^r). We denote this signature as

$$V = SK[x : y^r = (g^r)^x](m), \qquad (1)$$

where SK represents both the proof of knowledge of the private key x and a signature on message m. Readers are refereed to [9] for the technical details.

B. PVSS Scheme

The proposed protocols require a publicly verifiable secret sharing (PVSS) scheme rather than a verifiable secret sharing (VSS) scheme [11]. In a VSS scheme, the objective is to resist malicious players such as

- a dealer sending incorrect shares to some or all of the participants, and
- participants submitting incorrect shares during the reconstruction phase.

In a PVSS scheme, however, it is an explicit goal that not just the participants can verify their own shares, but that anybody can verify that the participants received correct shares [12]. To allow for public verifiability in double auction, we employ Schoenmakers' PVSS [13] which is much simpler than other schemes [12,14]. Readers are refereed to [13] for technical details.

C. McAfee's Protocol

The first of our proposed double auction protocols is based on McAfee's PMD protocol [15]. We first review PMD protocol. Let declared buyers' evaluations (*bids*) be $b_1, ..., b_m$ and declared sellers' evaluations (*asks*) be $s_1, ..., s_n$, where

$$b_{(1)} \geq b_{(2)} \geq \cdots \geq b_{(m)} \text{ and } s_{(1)} \leq s_{(2)} \leq \cdots \leq s_{(n)}.$$

Please note the different orderings for buyers' and sellers' evaluations. We use the notation i for the i-th highest evaluation value of buyers and the i-th lowest evaluation value of sellers. Choose k so that $b_{(k)} \geq s_{(k)}$ and $b_{(k+1)} < s_{(k+1)}$ hold. Since for (1) to k, the evaluation value of the buyers is larger than that of the sellers, at most k trades are possible. The candidate of a trading price p_t is defined as

$$p_t = \frac{1}{2}(b_{(k+1)} + s_{(k+1)}). \qquad (2)$$

The PMD protocol works as follows,

1. If $s_{(k)} \leq p_t \leq b_{(k)}$ holds, the buyers/sellers form (1) to (k) trade at price p_t.

2. If $p_t > b_{(k)}$ or $p_t < s_{(k)}$ holds, the buyers/sellers from (1) to $(k-1)$ trade. Each buyer pays $b_{(k)}$, and each seller gets $s_{(k)}$.

If the second condition holds, since the price for buyers $b_{(k)}$ is larger than the price for sellers $s_{(k)}$, the amount $(k-1) \cdot (b_{(k)} - s_{(k)})$ is left over. It is usually assumed that the auctioneer receives this amount. In our protocol, the manager receives this amount. This protocol is proven to be dominant-strategy incentive compatible if there is no false-name bid. Since our double auction protocol prevents malicious buyers and sellers from submitting false bids and asks by non-repudiation, and removes them before the determination of the trading price and winners, our protocol is obviously dominant-strategy incentive compatible.

D. Yokoo's Protocol

The second of our proposed double auction protocols is based on Yokoo's TPD protocol [16], which is a robust extension to the PMD protocol against false name bids. We review the TPD protocol in short.

First, the auctioneer determines a *threshold price r*. Auctioneer is a non-trading agent who does not desire to buy or sell the goods. He determines this threshold price without consulting the declared valuation of buyers and sellers. The declared buyers' valuations are $b_1, ..., b_m$ and declared sellers' valuations are $s_1, ..., s_n$, where

$$b_{(1)} \geq \cdots \geq b_{(i)} \geq r > b_{(i+1)} \geq \cdots \geq b_{(m)},$$
$$s_{(1)} \cdots \leq s_{(j)} \leq r < s_{(j+1)} \leq \cdots \leq s_{(n)}. \quad (3)$$

TPD protocol is defined as follows,

1. When $i = j$: the buyers and sellers from (1) to (i) trade at the price r.

2. When $i > j$: the buyers and sellers from (t) to (j) trade. Each buyer pays $b_{(j+1)}$ and each seller gets r. The auctioneer gets the amount of $j(b_{(j+1)} - r)$.

3. When $i < j$: the buyers and sellers from (1) to (i) trade. Each buyer pays r and each seller gets $s_{(i+1)}$. The auctioneer gets the amount of $i(r - s_{(i+1)})$.

IV. PROPOSED DOUBLE AUCTION PROTOCOL

The double auction process, to be presented below, consists of the following four phases: *system set-up*, *registration*, *bid/ask submission*, and *bid/ask opening*.

A. Notations

B_i is the identity of i-th buyer for $i = 0,1...,m-1$ and S_j is the identity of j-th sellers for $j = 0,1...,n-1$. T_{B_i}, T_{S_j} is auction ticket for B_i, S_j, respectively and $Cert_A$ represents the certificate of A issued by CA(Certification Authority). In addition, $Sig_A(m)$ means the digital signature of message m generated by entity A, and $H(m_1\|\cdots\|m_n)$ is one-way hash function with input strings $m_1,...,m_n$, where $(m_1\|\cdots\|m_n)$ represents concatenation of n binary strings.

B. System Set-up

The entities involved in the proposed double auction protocol include a manager M, m buyers B_i for $i \in Z_m$ and n sellers S_j for $j \in Z_n$. The role of each entity is as follows:

Manager M
- is in charge of the registration of buyers/sellers and provides each participant with an auction ticket as pseudonym.
- publishes the signature scheme, the public key for verification of signature and the certificates.
- announces the offer valuation range.
- releases G_q which has a group of prime order q.
- on behalf of participants, verifies the proofs of buyers and sellers in reconstruction step of bids/asks, and then determines the trading price and winners according to the auction rules.
- publishes the original identity of participants at the winner announcement step or because of user misbehavior.
- In case of determination of the trading price based on TPD protocol, he selects the threshold price r.

Buyer B_i
- registers with the manager and receives an auction ticket T_{B_i}.
- submits a bid in the submission phase, and in the ask opening phase, decrypts the encrypted shares that a seller S_j has submitted.

Seller S_j
- registers with the manager and receives an auction ticket T_{S_j}.
- submits an ask in the submission phase, and in the bid opening phase, decrypts the encrypted shares that a buyer B_i has submitted.

In the proposed protocols, 4 bulletin boards are used, i.e., a registration bulletin board, a submission bulletin board, an opening bulletin board, and a winner announcement bulletin board. A bulletin board is a public communication channel which can be read by anybody but only be written by the legitimate party in an authentic way [9].

C. Registraion Phase

All B_i and sellers S_j register with the manager M as follows:

1. Suppose that every buyer B_i has private key x_i and the corresponding public key $y_i = g^{x_i}$ certified by CA, where $x \in_R Z_q$, $i = 0,1,...,m-1$ and B_i is the

identity information of the buyer(e.g., ID card number).

2. B_i chooses a random number r_i and $k_i \in Z_q$, and keeps them confidential.

3. The buyer B_i computes $c_i = H(m_i \| y_i^{r_i} \| g^{r_i} \| g^{k_i})$ and $s_i = r_i^{-1} \cdot k_i - c_i \cdot x_i$, where *Buyer* indicates that he wants to buy goods and $m_i = (B_i \| Cert_{B_i} \| Buyer)$.

4. B_i sends $(m_i, c_i, s_i, y_i^{r_i}, g^{r_i})$ to M secretly.

5. M checks $c_i = H(m_i \| y_i^{r_i} \| g^{r_i} \| (g^{r_i})^{s_i} \cdot (y_i^{r_i})^{c_i})$.

6. After verifying the correctness of (c_i, s_i) and authenticating the buyer, the manager computes $h_i = H(y_i^{r_i})$ and $v_i = Sig_M(y_i^{r_i} \| h_i)$, generates an auction ticket $T_{B_i} = (y_i^{r_i} \| h_i \| v_i)$ and shuffles it on the registration bulletin board.

After the above registration, each buyer B_i can easily confirm whether his auction ticket is on that bulletin board or not. Because the auction ticket T_{B_i} can be recognized only by the buyer who knows the relevant y_i and r_i for T_{B_i}, it could be used as a pseudonym for anonymity.

Similarly, seller S_j registers with the manager M and obtains her auction ticket $T_{S_j} = (\tilde{y}_j^{\tilde{r}_j} \| \tilde{h}_j \| \tilde{v}_j)$ [2] from the registration bulletin board.

D. Bid/Ask-Submission Phase

Every buyer and seller first determines their own evaluation for an item traded by auction. Note that the proposed double auction protocol assumes w possible discrete bidding/asking price steps.

First consider the submission from a buyer B_i. Each buyer B_i chooses an evaluation $l_e \in L, e = 1, ..., w$ and selects a random polynomial $p_i(x)$ such that

$$p_i(x) = \prod_{k=0}^{t-1} \alpha_k x^k = \alpha_{t-1} x^{t-1} + \cdots + \alpha_0, \qquad (4)$$

where $\alpha_0 = l_e$ and $t \leq n$, n is the total number of sellers participating in the auction. The buyer B_i keeps this polynomial secret. Each buyer then computes shares $p_i(k+1)$ for $0 \leq k \leq n-1$ and encrypts them using the auction ticket of the seller, i.e., using the anonymous public key $\tilde{y}_j^{\tilde{r}_j}$ included in the auction ticket T_{S_j} on the registration bulletin board. Then, the buyer B_i signs the encrypted shares including the pseudonym of sellers as follows:

---

[2] To avoid the notation confusion between buyers and sellers, we just use the tilde symbol on some parameters related to sellers.

$$V_{B_i} = SK[x_i : y_i^{r_i} = (g^{r_i})^{x_i}](m_i), \qquad (5)$$

$$m_i = ((T_{S_0}, (\tilde{y}_0^{\tilde{r}_0})^{p_i(1)}) \| \cdots \| (T_{S_{n-1}}, (\tilde{y}_{n-1}^{\tilde{r}_{n-1}})^{p_i(n)})) \quad (6)$$

and sends the signed message [3] to the submission bulletin board.

In a similar way, each seller S_j chooses the polynomial, computes shares and signs the message including both the encrypted shares and the auction tickets of buyers. Table 1 indicates the information published on the submission bulletin board after the bid/ask submission phase is finished [4].

TABLE I.

SUBMISSION BULLETIN BOARD

Buyers		Sellers	
T_{B_1}	V_{B_1}	T_{S_1}	V_{S_1}
⋮	⋮	⋮	⋮
$T_{B_{m-1}}$	$V_{B_{m-1}}$	T_{S_n}	V_{S_n}
T_{B_m}	V_{B_m}	-	-

E. Bid/Ask-Opening Phase

The bid/ask opening phase consists of the following four steps: decryption of encrypted shares, reconstruction of bid/ask, determination of the trading price, and winner announcement.

Decryption of Encrypted Share. Each participant first verifies the correctness of auction tickets related to the entities that have sent the messages. To have a clear understanding, we consider a simple example. Assume some buyers B_0, B_1 and B_2 encrypted their shares $p_0(1), p_1(1)$ and $p_2(1)$ using an auction ticket T_{S_0} in the bid submission phase, and then they submitted the encrypted shares to the submission bulletin board. For decryption of encrypted shares, the seller S_0 first confirms whether her auction ticket exists in the messages that the buyers submitted to the submission bulletin board.

After checking the integrity of her own auction ticket, she verifies the correctness of the auction tickets T_{B_0}, T_{B_1} and T_{B_2} corresponding to the buyers B_0, B_1 and B_2, respectively. If the verification is correct, she decrypts the encrypted shares $(\tilde{y}_0^{\tilde{r}_0})^{p_0(1)}, (\tilde{y}_0^{\tilde{r}_0})^{p_1(1)}$ and $(\tilde{y}_0^{\tilde{r}_0})^{p_2(1)}$ using her secret keys $\tilde{x}_0$ and $\tilde{r}_0$ as follows:

---

[3] The buyer B_i should prove the correctness of the encrypted shares using the methods such as Chaum's proof of equality of discrete logarithm [11] or DLEQ protocol [13].

[4] We assume that the total number of buyers m is larger than the total number of sellers n.

$$((\tilde{y}_0^{\tilde{r}_0})^{p_0(1)})^{1/\tilde{x}_0 \cdot \tilde{r}_0} = ((g^{\tilde{x}_0 \cdot \tilde{r}_0})^{p_0(1)})^{1/\tilde{x}_0 \cdot \tilde{r}_0} = g^{p_0(1)}$$
$$((\tilde{y}_0^{\tilde{r}_0})^{p_1(1)})^{1/\tilde{x}_0 \cdot \tilde{r}_0} = ((g^{\tilde{x}_0 \cdot \tilde{r}_0})^{p_1(1)})^{1/\tilde{x}_0 \cdot \tilde{r}_0} = g^{p_1(1)} \qquad (7)$$
$$((\tilde{y}_0^{\tilde{r}_0})^{p_2(1)})^{1/\tilde{x}_0 \cdot \tilde{r}_0} = ((g^{\tilde{x}_0 \cdot \tilde{r}_0})^{p_2(1)})^{1/\tilde{x}_0 \cdot \tilde{r}_0} = g^{p_2(1)}$$

After decrypting the encrypted shares, the seller S_0 signs the decrypted shares and releases the signed messages [5] to the opening bulletin board as follows:

$$V_{S_0} = SK[\tilde{x}_0 : \tilde{y}_0^{\tilde{r}_0} = (g^{\tilde{r}_0})^{\tilde{x}_0}](\tilde{m}_0), \qquad (8)$$

$$\tilde{m}_0 = ((T_{B_0}, g^{p_0(1)}) \| (T_{B_1}, g^{p_1(1)}) \| (T_{B_2}, g^{p_2(1)})) \qquad (9)$$

Now, consider the decryption for the encrypted shares of sellers in a generalized case. Like the seller in the previous example, each buyer B_i verifies the messages and auction tickets of sellers and decrypts the shares encrypted by them. Then he signs the message $m_i = ((T_{S_0}, g^{\tilde{p}_0(i+1)}) \| \cdots \| (T_{S_{n-1}}, g^{\tilde{p}_{n-1}(i+1)}))$, where $i \in Z_m$, and publishes it on the opening bulletin board.

Reconstruction of Bid/Ask. To recover an evaluation of each participant, at least t correctly decrypted shares are needed. After verifying the messages and proofs of sellers submitted in the previous step, on behalf of participants, the manager M recovers the evaluation l_e of buyer B_i using Lagrange interpolation(Suppose that t sellers produce correct values for $g^{p_i(k)}$, for $k = 1,...,t$):
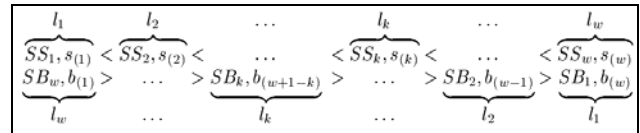
$$\prod_{k=1}^{t} (g^{p_i(k)})^{\lambda_k} = g^{\sum_{k=1}^{t} p_i(k)\lambda_k} = g^{p_i(0)}, \qquad (10)$$

where $\lambda_k = \prod_{j \neq k} \dfrac{j}{j-k}$ is a Lagrange coefficient and $p_i(0) = l_e$. Because the manager holds w discrete bidding/asking prices in the system set-up phase, he can pre-compute g^{l_e} for $e = 1,...,w$ so that he gets the evaluation l_e of the buyer from the above value $g^{p_i(0)}$. In the same way, the manager recovers the evaluation of each seller S_j.

Determination of the Trading Price. In this step, the trading price can be determined into two types according to McAfee's and Yokoo's protocol.

First, assume that the determination of the trading price is based on McAfee's PMD protocol. Let SB_f be the set of auction tickets corresponding to buyers who have bidden at the price l_f, $f = 1,...,w$. Also, SS_f indicates the set of auction tickets related to sellers who have asked at the price l_f . For the reverse ordering of McAfee's

---

protocol, let $s_{(i)}$ denote the representing ask of the set SS_f and $b_{(i)}$ denote the representing bid of the set SB_f, $i = 1,...,w$. We use the notation (i) for the i -th highest evaluation value of SB_f and the i -th lowest evaluation value of SS_f . At this time, the order statistics are as follows.

l_1	l_2	$\ldots$	l_k	$\ldots$	l_w
$\overbrace{SS_1, s_{(1)}}$ <	$\overbrace{SS_2, s_{(2)}}$ <	$\ldots$ <	$\overbrace{SS_k, s_{(k)}}$ <	$\ldots$ <	$\overbrace{SS_w, s_{(w)}}$
$\underbrace{SB_w, b_{(1)}}$ >	$\ldots$ >	$\underbrace{SB_k, b_{(w+1-k)}}$ >	$\ldots$ >	$\underbrace{SB_2, b_{(w-1)}}$ >	$\underbrace{SB_1, b_{(w)}}$
l_w	$\ldots$	l_k	$\ldots$	l_2	l_1

Note that $\sum_{f=1}^{w} |SB_f| = m$ (total number of buyers) and $\sum_{f=1}^{w} |SS_f| = n$ (total number of sellers), where $|SB_f|$ and $|SS_f|$ are size of sets SB_f and SS_f, respectively.

Now, the manager determines the trading price. That is, he first chooses a k such that $s_{(k)} \leq b_{(k)}$ and $s_{(k+1)} > b_{(k+1)}$, then defines the candidate of a trading price $p_t = \dfrac{1}{2}(b_{(k+1)} + s_{(k+1)})$. The protocol is defined as follows.

1. If $s_{(k)} \leq p_t \leq b_{(k)}$ holds, each buyer SB_f for $f = w-k+1,...,w$ and each seller SS_f for $f = 1,...,k$ trade at price p_t . In other words, those buyers whose bids are equal to or higher than $b_{(k)}$ trade with those sellers whose asks are equal to or lower than $s_{(k)}$.

2. If $p_t > b_{(k)}$ or $p_t < s_{(k)}$ holds, SB_f for $f = w-k,...,w$ and SS_f for $f = 1,...,k-1$ trade, which means those buyers whose bids are equal to or higher than $b_{(k-1)}$ trade with those sellers whose asks are equal to or lower than $s_{(k-1)}$. Each buyer pays $b_{(k)}$ and each seller gets $s_{(k)}$.

Second, suppose that the determination of the trading price is based on Yokoo's TPD protocol that is proven to be a *dominant-strategy incentive compatible* protocol even if participants might submit false-name bid. Like the first type based on McAfee's PMD protocol, let SB_f be the set of auction tickets corresponding to buyers who have bidden at the price l_f, $f = 1,...,w$. Also, SS_f indicates the set of auction tickets related to sellers who have asked at the price l_f . Since Yokoo's TPD protocol is based on the reverse ordering, let $s_{(i)}$ denote the representing ask of the set SS_f and $b_{(i)}$ denote the

---

[5] The signed message must include the proof that the decrypted shares are correctly computed, which is possible by a zero-knowledge such as *DLEQ* protocol [13] or Chaum's proof of equality of discrete logarithm [11].

representing bid of the set SB_f, $i = 1,...,w$. We use the notation (i) for the i-th highest evaluation value of SB_f and the i-th lowest evaluation value of SS_f. At this time, the order statistics are as follows.

$$
\begin{array}{ccccccc}
l_1 & \dots & l_k & & l_{k+1} & \dots & l_w \\
\overbrace{SS_1, s_{(1)}} < \dots < \overbrace{SS_k, s_{(k)}} & < r < & \overbrace{SS_{k+1}, s_{(k+1)}} < \dots < \overbrace{SS_w, s_{(w)}} \\
\underbrace{SB_w, b_{(1)}} > \dots > \underbrace{SB_j, b_{(j)}} & > r > & \underbrace{SB_{j+1}, b_{(j+1)}} > \dots > \underbrace{SB_1, b_{(w)}} \\
l_w & \dots & l_{w-j+1} & & l_{w-j} & \dots & l_1
\end{array}
$$

Note that the manager chooses the threshold price r before buyers/sellers attend an auction. Note that $\sum_{f=1}^{w} |SB_f| = m$ (total number of buyers) and $\sum_{f=1}^{w} |SS_f| = n$ (total number of sellers), where $|SB_f|$ and $|SS_f|$ are size of sets SB_f and SS_f, respectively. Now, according to TPD protocol, the trading price is determined as follows:

1. When $j = k$, SB_f for $f = w - j + 1, ..., w$ and SS_f for $f = 1, ..., j$ trade at the price r.

2. When $j > k$, SB_f for $f = w - k + 1, ..., w$ and SS_f for $f = 1, ..., k$ trade. The set of buyers, SB_f for $f = w - k + 1, ..., w$, pays $b_{(k+1)}$ and each seller SS_f for $f = 1, ..., k$ gets r. At this time, the auctioneer gets the number of $k(b_{(k+1)} - r)$.

3. When $j < k$, SB_f for $f = w - j + 1, ..., w$ and SS_f for $f = 1, ..., j$ trade. Each buyer SB_f for $f = w - j + 1, ..., w$, pays r and each seller gets $s_{(j+1)}$. At this time, the auctioneer gets the number of $j(r - s_{(j+1)})$.

Winner Announcement. After determining the winning sets, the manager releases the original identities of the winners on the winning announcement bulletin board. For public verification, he publishes the information $(c_i, s_i, m_i = (B_i \| Cert_{B_i} \| Buyer), y_i^{r_i}, g^{r_i}, T_{B_i})$ related to registration of winning buyers. Note that (c_i, s_i, m_i) are values used to authenticate an identity. Therefore, all entities including the lost participants or observers can identify the winning buyers. In the same way, the manager releases the registration information corresponding to the winning sellers, so that any entities can identify the winners.

V. ANALYSIS

In this section, we perform an informal analysis of our protocols with respect to security and efficiency.

A. Security

Anonymity. We have assumed the semi-trusted manager who does not open the real identity during the auction process except at the winner announcement step or because of user misbehavior, while he may try to illegally attend an auction by impersonating other participants. Thus, as long as the manager does not open the real identity, the anonymity is guaranteed by the following Lemma 1.

Lemma 1. *Nobody, except the manager, can associate an auction ticket T_{B_i}, T_{S_j} with the real identity B_i, S_j of buyer or seller, respectively.*

Proof: An auction ticket is in the form of $T = (y^r \| h \| v)$, where $h = H(y^r)$, $v = Sig_M (y^r \| h)$ and $y = g^x$, and it does not include the identity information. That is, to recover the original *ID*, one has to be able to at least find the parameter y from anonymous public key y^r. Since the manager does not release the public key y, the only way to break anonymity is to find the private key x from $g^{x \cdot r}$ and compute $y = g^x$, then finally compare it with some certificate lists [6]. However, this is to solve discrete logarithm problem, and it is also too difficult to determine a correct x because another random secret number r is used.

Impossibility of Impersonation. Since an anonymity service is provided in the proposed double auction protocol, an entity may try to illegally submit a faked bid or ask and impersonate a legal entity using the auction ticket of other participants. However, impersonation is technically impossible in our scheme, as shown in the following Theorem 1.

To induce Theorem 1, we first prove the following lemmas.

Lemma 2. *If solving the discrete logarithm problem is hard under a group for the given quintuplet (m, y^r, g^r, c, s), where x is the secret key and $y(= g^x)$ is the public key, finding random element k of the group satisfying both $c = H(m \| y^r \| g^r \| g^k)$ and $s = r^{-1} \cdot k - c \cdot x$ is equivalent to the difficulty of the discrete logarithm problem.*

Proof: It is straightforward to show the proof. Since we do not know the value of x and r from $(g^x)^r$ by the intractability of DLP under a group that solving DLP is hard in the polynomial time and k is also random elements, the only way to get k is to find the discrete

---

[6] We also consider the case that y and the corresponding certificate have been released in another auction, so that people have some lists related to them.

logarithm of $((g^r)^s) \cdot ((g^x)^r)^c)$ such that $g^k = ((g^r)^s) \cdot ((g^x)^r)^c)$. It leads to solve DLP again.

Lemma 3. An attacker who intercepts the valid signature information, (y^r, g^r), of another entity and then injects the faked bid or ask cannot generate a valid signature.

Proof: Suppose an attacker can generate a valid signature (c', s') to inject a faked bid or ask message m' using the intercepted valid value (y^r, g^r). The attacker then releases (m', c', s', y^r, g^r) on the submission bulletin board, so that he can impersonate an entity corresponding to the parameter y^r. To pass successful signature verification, the following equation should be satisfied:

$$c' = H(m' \| y^r \| g^r \| (g^r)^{s'} \cdot (y^r)^{c'}) \qquad (11)$$

That is, the attacker generates c' as follows:

$$c' = H(m' \| y^r \| g^r \| g^{k'}) \qquad (12)$$

From equations (9), (10) the following equations are induced:

$$g^{k'} = (g^r)^{s'} \cdot (y^r)^{c'} = g^{r \cdot s' + c \cdot x \cdot r} \qquad (13)$$

From equation (13), we know that the attacker needs to generate k' such that $k' = r \cdot s' + c' \cdot x \cdot r$. However, the only way to get both r and x is to find the discrete logarithm of g^r, and then to solve another discrete logarithm problem of $y^r = (g^x)^r = (g^r)^x$, respectively. Since this is contradictory to the intractability of DLP under a group, our assumption that an attacker can generate a valid signature using the parameters (y^r, g^r) of another entity is not valid.

Lemma 4. The manager also cannot impersonate a valid trader.

Proof: his can be proved straightforwardly by means of Lemmas 2 and 3, so we will omit the detailed proof. From Lemmas 2, 3 and 4, we can induce the following security theorem.

Theorem 1. In our proposed double auction protocols, nobody, not even manager, can forge the valid signature to submit a faked bid or ask, so that he cannot impersonate other entities.

Non-repudiation. Every trader, who has his unique key pair *i.e.*, private key x and the corresponding public key y certified by CA, signs all messages related to bid or ask information. Thus, we can also induce the following theorem by the foregoing sentence and Theorem 1.

Theorem 2. In the proposed schemes, every entity participating in auction process cannot deny that he has submitted ask or bid.

Robustness and Correctness. Even though some buyers and sellers cannot participate in or are dropped from an auction process due to an unstable network environment or their misbehavior, the proposed auction protocol still works well as long as at least t sellers and buyers among n sellers and m buyers are able to honestly attend an auction process. This robustness and correctness, **which is a major property being emphasized in our protocol**, is satisfied by the threshold access structure, and the evaluation of participants is obtained by using Lagrange interpolation as follows:

$$\prod_{k=1}^{t} (g^{p(k)})^{\lambda_k} = g^{\sum_{k=1}^{t} p(k)\lambda_k} = g^{p(0)}, \qquad (14)$$

where $\lambda_k = \prod_{i \neq k} \dfrac{i}{i-k}$ is a Lagrange coefficient and $p(0) = l_e$.

Public Verifiability. In the proposed protocol, any one can check the validity of submitted signatures and offers from traders. This is achieved by the publicly verifiable secret sharing scheme, the signature of knowledge, and some zero-knowledge proofs.

B. Efficiency

Communication. Our protocols have very low communication overheads: one round for registration, one round for bid/ask submission, one round for bid/ask opening, one round for determining the trading price and winners.

Computation. In terms of computation overheads, we compare the proposed protocols with Wang *et al.*'s protocols [4], because both schemes are based on McAfee's PMD and Yokoo's TPD protocols. Excluding the computational cost of registration, we only consider the cost from the bid/ask submission phase to the bid/ask opening phase. The computational cost is considered in terms of modular arithmetic, including modular exponentiation (E) and modular multiplication (M), and zero-knowledge (ZK) for proving the correctness of private key, encrypted shares and decrypted shares. We assume that both protocols use the same zero-knowledge.

Table 2 represents the total computational overheads, from which we can see the price w has no effect on the computational overheads in our protocols. As a result, our protocols are more efficient than Wang *et al*'s protocols, especially when w becomes large, where m and n are the number of buyers and sellers, respectively.

Note that in the proposed two protocols, there is no difference in terms of computation loads even though the trading price of protocols are based on McAfee's MCD and Yokoo's TPD protocols, respectively. That is, the process for the determination of trading price does not

give the computational loads buyers, sellers and manager directly.

Computational cost		Wand and Leung's protocols	Proposed protocols
Buyer	E	$2mw$	$3mn$
	M	$3mw$	$2m$
	ZK	$w(2m+1)$	$2mn$
Sellers	E	$2nw$	$3mn$
	M	$3nw$	$2n$
	ZK	$w(2n+1)$	$2mn$
Manager	E	-	$2t$
	M	$2\{(m-1)^w+(m-1)^w +w(m+n+1)\}$	-

VI. DISCUSSIONS

We proposed two double auction protocols according to the determination of the trading price, which are based on McAfee's MCD and Yokoo's TPD protocols, respectively. The TPD protocol is the first non-trivial double auction protocol that is dominant-strategy incentive compatible even if participants can submit false-name bids [16]. However, the TPD protocol has some weakness. One limitation is that the revenue of the auctioneer becomes large compared with the MCD protocol. This fact is not desirable, since if the revenue of the auctioneer is large, the buyers/sellers are discouraged from participating in trading. The auctioneer cannot simply return the revenue to the participants since it will affect incentives of participants [17]. Another weakness is that the auctioneer may desire to make more profit by choosing the relevant threshold price r even though he cannot attend an auction process. We give an example where the earnings of the auctioneer and the number of traders change with the threshold price r.

Example1. Let us assume the true valuation of buyers and sellers are as follows.

- Buyers' valuations: $9 > 8 > 7 > 4$
- Sellers' valuations: $2 < 3 < 4 < 12$

1. When the auctioneer chooses $r = 6$, because this corresponds to case (1) of TPD protocol, the buyers and sellers from (1) to (3) trade at the price $r = 6$. At this time, the auctioneer cannot have any profit by the rules of TPD protocol.
2. When the auctioneer chooses $r = 3.5$, because this corresponds to case (2) of TPD protocol, the buyers and sellers from (1) to (2) trade. Each seller gets the threshold price $r = 3.5$ and each buyer pays 7. At this time, the auctioneer gets the profit $2 \cdot (7 - 3.5) = 7$.

3. When the auctioneer selects $r = 8.5$, because this corresponds to case (3) of TPD protocol, only buyer and seller can trade. The buyer pays the threshold price $r = 8.5$ and the seller gets 3. At this time, the auctioneers gets the profit $1 \cdot (8.5 - 3) = 5.5$.

In the above example, the auctioneer's profit depends on his choice of the threshold price r, so that the auctioneer will determine the threshold price r as 3.5 to get the maximum profit. (*In fact, the auctioneer can choose another threshold price r by considering not only above 3 cases but also other cases.*)

In TPD protocol, since the threshold price is released after all participants have bidden, the auctioneer can choose the relevant r to make more earnings. His action can determine not only his own earnings but also the number of traders. That is, the number of traders including both winning buyers and sellers is 6, 4, 2 in cases (1), (2), (3), respectively. Even though many buyers and sellers participate in the auction process, the number of traders can be limited by the auctioneer due to his profit. In fact, this property is not desirable because the trading price does not depend on the demand and supply of buyers and sellers but is determined by the auctioneer's profit.

VII. CONCLUSION

We presented secure and practical double auction protocols with hybrid trust model under realistic assumptions, which are based on McAfee's and Yokoo's protocols. As a threshold access structure is used, even if some participants dropped out of the auction process early due to an unstable network or misbehavior, the proposed protocols are still able to be successfully completed. Our proposal satisfies most properties for secure double auction, and is relatively efficient in terms of computation and communication.

REFERENCES

[1] D. Friedman and J. Rust, "The double auction market, " *Addison-Wesley Publishing Company*, 1993.
[2] K. Omote and A. Miyaji, "A practical English auction with one-time registration," *ACISP'01*, LNCS 2119, pp. 221-234, 2001.
[3] W. Vickrey, "Counterspeculation, auction and competitive sealed tenders," *Journal of Finance*, 16(1): 8-37, 1961.
[4] C. Wang, F. Leung and Y. Wang, "Secure double auction protocols with full privacy protection," *ICISC'03*, LNCS 2971, pp. 215-229, Springer Verlag, 2003.
[5] C. Boyd and W. Mao, "Security issues for electronic auctions," *HPL-2000-90*, Hewlett Packard, 2000.

[6] H. Kikuchi, "*M+1*st-Price Auction Protocol," *Financial Cryptography'01*, LNCS 2339, Springer Verlag, 2001.

[7] O. Baudron and J. Stern, "Non-interactive private auctions.," *Financial Cryptography'01*, LNCS 2339, pp. 364-378, Springer Verlag, 2001.

[8] F. Brandt, "Fully private auctions in a constant number of rounds," *Financial Cryptography'03*, LNCS 2742, pp. 223-228, Springer Verlag, 2003.

[9] B. Lee, K. Kim, and J. Ma, "Efficient public auction with one-time registration and public verifiability," *Indocrypt'01*, LNCS 2247, Springer Verlag, 2001.

[10] J. Camenisch and M. Stadler, "Efficient group signature scheme for large groups," *CRYPTO'97*, LNCS 1294, Springer Verlag, 1997.

[11] D. Chaum and T.P. Pedersen, "Wallet databases with observers," *CRYPTO'92*, LNCS 740, pp. 89-105, Springer Verlag, 1992.

[12] M. Stadler, "Publicly verifiable secret sharing," *EUROCRYPT'96*, LNCS 1070, pp. 190-199, Springer Verlag, 1996.

[13] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting.," *CRYPTO'99*, LNCS 1666, pp. 148-164, Springer Verlag, 1999.

[14] E. Fujisaki and T. Okamoto, "A practical and provably secure scheme for publicly verifialbe secret sharing and its applications," *EUROCRYPT'98*, LNCS 1403, pp. 32-46, Springer Verlag, 1998.

[15] M. Preston, "A dominant strategy double auction," *Journal of Economic Theory*, (56), pp 434-450, 1992.

[16] M. Yokoo, Y. Sakurai and S. Matsubara, "Robust double auction protocol against false-name bids," *Decision Support Systems*, (39), pp. 241-252, 2005.

[17] H. R. Varian, "Intermediate microeconomics: a modern approach," 5th *ed., W. W. Norton*, New York, 1999.

International Conference on Applied Cryptography and Network Security (ACNS).

SangJae Moon received his B.E. and M.E. degrees in Electronic from Seoul National University, Korea in 1972 and 1974 respectively. He received Ph.D. in Communication Engineering from the University of California, Los Angeles, USA, in 1984. He was working on a consultant of Omnet, co., USA from 1984 to 1985. Currently, he is a professor with the School of Electrical Engineering and Computer Science, Kyungpook National University, Korea, and the director of Mobile Network Security Technology Research Center(MSRC). He is also an honorary president of the Korean Institute of Information Security and Cryptology. His current research interests are the information security in mobile, ubiquitous, and RFID networks including the physical security on smart system card. He took part in the Korea Certificate-based Digital Signature Algorithm(KCDSA) Standard project. He has a number of issued patents in the areas of information security.

Junghoon Ha received his B.E. and M.E. degrees in Electronics from Kyungpook National University, Korea, in 2002 and 2004, respectively, and now is Ph.D. candidate. Currently, he is a research engineer with Mobile Network Security Research Center (MSRC), where he conducts research and development of public-key cryptosystems, digital signature schemes, cryptographic security protocols, and formal security analysis methodology. His research interests also include network security, ubiquitous communication security for cellular, mobile ad-hoc, RFID networks, and development of secure auction protocol for e-commerce.

Jianying Zhou is a lead scientist at Institute for Infocomm Research, and heads the Internet Security Lab. He is also an adjunct professor in University of Science and Technology of China and in Shanghai Jiaotong University, and an adjunct senior scientist in University of Malaga. Dr. Zhou obtained PhD degree in Information Security from University of London. His research interests are in computer and network security, cryptographic protocol, digital signature and non-repudiation, mobile communications security, public-key infrastructure, and secure electronic commerce. He is a world-leading researcher on non-repudiation, and authored the book *"Non-repudiation in Electronic Commerce"* which was published by Artech House in 2001. He is a co-founder and steering committee member of