Receipt-free Electronic Auction Schemes Using Homomorphic Encryption

Xiaofeng Chen[1], Byoungcheon Lee[2] and Kwangjo Kim[1]

[1] International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{crazymount,kkj}@icu.ac.kr
[2] Joongbu University,
101 Daehak-Ro, Chuboo-Meon, Kumsan-Gun, Chungnam, 312-702, KOREA
sultan@joongbu.ac.kr

Abstract. Bid-rigging is a dangerous attack in electronic auction. Abe and Suzuki firstly introduced the idea of receipt-free to prevent this attack. In this paper we point out that Abe and Suzuki's scheme only provides receipt-freeness for losing bidders. We argue that it is more important to provide receipt-freeness for winners and propose a new receipt-free sealed bid auction scheme using the homomorphic encryption technique. In contrast to Abe and Suzuki's scheme, our scheme satisfies privacy, correctness, public verifiability and receipt-freeness for all bidders. Also, our scheme is not based on *threshold trust model* but *three-party trust model*, so it is more suitable for real-life auction. Furthermore, we extend our scheme to $M+1$-st price receipt-free auction.

Key words: Bid-rigging, Receipt-free, Homomorphic encryption, Auction.

1 Introduction

Auction has become a major phenomenon of electronic commence in the recent years. The most common auctions are English auction, Dutch auction and Sealed bid auction. In the former two auctions, the communication cost is high and the bidder information will be revealed after the auction is finished. Though the sealed bid auction can be finished in one round communication, it does not support the optional distribution of the goods [11]. Nobel Prize winner, economist Vickrey presented a second-price auction: the bidder with the highest price wins, but he only pays the second-price [25]. Vickrey auction is celebrated in economics for having the property of *incentive compatibility*, *i.e.*, the dominant strategy for each bidder is always to bid his true value. However, it is rarely used in practice for some crucial weakness [17]. $M+1$-st price auction is a type of sealed-bid auction for selling M units of a single kind of goods. In this auction, M highest bidders win and only pay $M+1$-st winning price. Vickrey auction can be regarded as a special case of $M+1$-st price auction for $M=1$. Wurman

[26] proved that $M+1$-st price auction also satisfies the property of *incentive compatibility*.

Sakurai *et al.* [22] firstly pointed out there exists the problem of bid-rigging in the electronic auction, *i.e.*, coercer/buyer orders other bidders to bid the price he specifies to control the winning price. For instance, the coercer/buyer orders other bidders (victims) to bid very low prices, then can win the auction at an unreasonably low price. Hence, if bid-rigging occurs, the auction fails to establish the appropriate price, so it is important to prevent bid-rigging. Sakurai *et al.* presented an anonymous auction protocol based on a new convertible group signature scheme to hide the identity of the winner. However, it does not solve the bid-rigging essentially. Recently, Abe and Suzuki [2] introduced the idea of receipt-free to prevent bid-rigging in the auction protocol.[1] They also proposed a receipt-free sealed-bid auction scheme under the assumption of bidding booth and a one-way untappable channel. However, the scheme is based on *threshold trust model*, *i.e.*, a major fraction of auctions are assumed to be honest, which is not suitable for many real life electronic auctions [5, 17, 18]. Also, it is not suit for $M+1$-st price auction.

Moreover, in Abe and Suzuki's scheme, all auctioneers together recover the secret seeds of each bidder to determine the winning price and the winners, that is, the secret identity number j of the winners is revealed to all auctioneers. Therefore a dishonest auctioneer may tell this information to the coercer/buyer. The coercer/buyer can know all victims' secret identity number beforehand. If the winner is one of the victims he ordered, the coercer/buyer will punish the winner. Therefore, the scheme only provides the receipt-freeness for losing bidders. We argue that it is more important to provide receipt-freeness for winners in electronic auctions. The aim of a coercer/buyer is to win the auction and the losers do not affect the result of the auction. So, if the victim is not the winner, the coercer/buyer never care whether the victim cheats him or not. However, if a bidder violates the rule of coercer/buyer and wins the auction, the coercer/buyer will be sure to punish the bidder for he cannot get the auction item.

In this paper, we propose a new receipt-free sealed bid auction scheme based on homomorphic encryption technique. In contrast to Abe and Suzuki's scheme, our scheme is not based on *threshold trust model* but *three-party trust model* [18]. Our scheme satisfies the properties of secrecy, correctness, public verifiability and receipt-freeness for all bidders. Furthermore, we present receipt-free $M+1$-st price auction.

The rest of the paper is organized as follows: The next section gives some properties and security requirements of an electronic auction. Section 3 proposes the receipt-free sealed bid auction scheme. Section 4 presents the receipt-free $M+1$-st auction scheme. In Section 5, the security and efficiency analysis about our proposed auction scheme are presented. Section 6 concludes this paper.

[1] The concept of receipt-free is firstly introduced by Benaloh and Tuinstra [4] to solve the misbehaver of "vote buying" or "coercion" in the electronic voting. There are plenty of researches on receipt-freeness in the electronic voting [12, 19, 21].

1.1 Related Works

There are plenty of works on the sealed bid (highest price) auction and Vickrey auction. Franklin and Reiter [10] presented a protocol for implementing a sealed-bid auction. Their solution is focused on using a cryptographic technique to provide protections to monetary bids, such as digital money. In their protocol, auctioneers use atomic multicast to communicate with each other, which is a bottleneck in a large system. Also the protocol has the disadvantage of revealing the bids after the auction is finished. Kikuchi *et al.* [11] proposed a protocol for a sealed-bid auction based on the Shamir's secret sharing scheme. The scheme enjoys the privacy of the bids, but it does not guarantee that the winning bidder will pay for the bid item. These schemes are not well suited for handing tie bids, *i.e.*, when two or more bidders happen to submit the same winning bid [20]. If tie-bidding occurs, the schemes will not specify who the winners are, or even how many winners there are. Also, both of the schemes distribute the trust onto multi auctioneers. Recently, Cachin [6] proposed an auction scheme involving two auction servers, but requiring bidders to contact just a single server. Lipmaa *et al.* [17] proposed a secure Vickrey auction without threshold trust.

The $M+1$-st price auction is a type of sealed-bid auction for selling M units of a single kind of item. Due to its attractive property of incentive compatibility, there are many works on $M+1$-st price auction [2, 5, 14]. Kikuchi [14] proposed an $M+1$-st price auction using homomorphic encryption. Brandt [5] proposed an $M+1$-st price auction where bidders compute the result by themselves. However, there is no receipt-free $M+1$-st price auction to the best of our knowledge.

1.2 Trust Model

There are numerous researches on electronic auction in recent years. Based on the trust model, the researches can be classified into the following cases:

Threshold Trust Model

There are m auctioneers in threshold trust model, out of which a fraction (e.g. more than $m/3$ or $m/2$) are assumed to be trustworthy. The auctioneers jointly compute the winning price by using inefficient techniques of secure multiparty function evaluation [18]. Some researchers claimed that the threshold trust model is not suitable for real-life electronic auctions [5, 17, 18, 23].

Three-party Trust Model

A new third-party is introduced in this trust model. The third-party is not a fully trusted party but assumed not to collude with the auctioneer [17, 18] or other parties [3, 6]. Also, the third-party is not required to interact with bidders and just generates the program for computing the result of the auction.

No Auctioneers Trust Model

Brandt [5] introduced the concept of bidder-resolved auctions, which distribute the trust onto all of the bidders. Unless all involved parties collude, no information of the bids will be revealed. It is a reasonable assumption that all bidders will never share their information simultaneously due to competition among them. A drawback of this model is low efficiency.

2 Properties and Security Requirements of Auction

In this section, we briefly describe the properties and security requirements of the electronic auction.

2.1 Properties

In this paper, we focus on sealed-bid auctions: bids are keep secret during the bidding phase. In the bidding phase, the bidders sends their sealed bidding price. In the opening phase, the auctioneer (or with a third party) determines the winning price according to a predetermined auction rule.

- **Bidding:** The auctioneer advertises the auction and calls the bidders to bid for the auction item. Each bidder decides his bidding price and sends the sealed price (better in an "encrypted" manner) to the auctioneer. The auctioneer cannot recover the information about the bids.
- **Opening:** After all bidders have sent their bidding price, the auctioneer determines the winning price and finds the bidder who bids the highest price. The information of the loser's identity and bidding price should not be revealed even after the auction. Furthermore, it is crucial to protect the identity of the winners in receipt-free auction. Otherwise, a coercer/buyer will punish the winners who do not bid the specified price.
- **Trading:** The winner buys the auction item with a certain price according to the auction rule. If the winner wants to repudiate his price, the auctioneer (or collaborating with other entities) can identity the winner.

2.2 Security Requirements

- *Privacy*: No information of the bids and the corresponding bidder's identity is revealed during and after the auction. The only information to be revealed is the winning price.
- *Correctness*: The winner and the winning price are determined correctly by a certain auction rule.
- *Public verifiability*: Anyone can verify the correctness of the auction.
- *Non-repudiation*: No bidder can repudiate his bid. The winner must buy the auction item with a certain price according the auction rule.
- *Efficiency*: The communication and computation in the auction should be reasonable for implementation.
- *Receipt-freeness*: Anyone, even if the bidder himself, must not be able to prove any information about the bidding price to any party.

3 Receipt-free Sealed Bid Auctions

In this section, we present receipt-free sealed bid auctions. Our scheme is not based on threshold trust model but three-party trust model, where the entity called *Auction Issuer* is not fully trusted but assume not collude with Auctioneer.

3.1 Physical Assumptions

Bulletin Board: In Abe and Suzuki's scheme, a physical assumption called bidding booth is used: no one can control or watch the bidder in the bidding booth. In our scheme, we will use a weaker assumption called bulletin board: any one can read the information in the bulletin board, but no one can delete the information. Also, only active bidders can append information in the designated fields. We suppose the bidders who register with auction service are assigned a secret identity number and the corresponding fields in the bulletin board. As Stubblebine *et al.* [23] discussed, registration may incorporate an identity escrow mechanism [15] so that the identity of a winner might only be revealed if he repudiates his price.

Untappable Channel: This is a one-way communication channel and the message through this channel remains secret for any third party. In our scheme, we assume that two untappable channels from auctioneer issuer and auctioneer to seller are separately available. Also, there exist untappable channels between each bidder and seller. Therefore, the coercer/buyer can not know the communication between the bidders and the seller, *i.e.*, he can not control the victims during the bidding.

3.2 System Parameters

There are m bidders $\{B_i | i = 1, 2, \cdots, m\}$, a seller S, an auctioneer A and an auctioneer issuer AI. Consider the subgroup G_q of order q of Z_p^*, where p and $q|p-1$ are large primes and g is a generator of G_q. Let G_1 and G_2 be independently selected generators of G_q which mean "I bid" and "I do not bid", respectively.

- A: chooses his secret key x_1 and publishes his public key $h_1 = g^{x_1}$.
- AI: chooses his secret key x_2 and publishes his public key $h_2 = g^{x_2}$.
- S: publishes a price list $P = \{j | j = 1, 2, \cdots, n\}$.
- B_i: chooses his secret key x_{B_i} and publishes his public key $h_{B_i} = g^{x_{B_i}}$. He decides his bidding price $p_i \in P$ and computes the encrypted bidding vector

$$C_{i,j} = (x_{i,j}, y_{i,j}) = \begin{cases} (g^{a_{ij}}, (h_1 h_2)^{a_{i,j}} G_1), \text{ if } j = p_i \\ (g^{a_{ij}}, (h_1 h_2)^{a_{i,j}} G_2), \text{ if } j \neq p_i \end{cases}$$

  where $a_{i,j} \in_R Z_q$, $j = 1, 2, \cdots, n$.

3.3 High-level Description of the Scheme

For $j = 1, 2, \cdots, n$, each bidder B_i firstly sends the bidding vector $C_{i,j}$ to the seller S. Then the seller S generates the receipt-free biding vector $C_{i,j}^* = (x_{i,j}^*, y_{i,j}^*) = (x_{i,j} u_j, y_{i,j} v_j)$, where $u_j = g^{\beta_j}$ and $v_j = (h_1 h_2)^{\beta_j}$. Meanwhile, the seller S proves that u_j and v_j have the common exponent β_j without exposing the value of β_j with the designated-verifier re-encryption knowledge proof [16].

If the proof is valid, the bidder B_i and the seller S jointly generate a proof of the validity of the bidding vector $C^*_{i,j}$ (see Appendix B and C). The bidder then posts the bidding vector and the proof to the designated fields in the bulletin board.

In the opening phase, the auctioneer and the Auctioneer Issuer together determine the winning (highest) price with $\prod_{i=1}^{m} C^*_{i,j}$ for $j = n, n-1, \cdots, 1$. Unless the auctioneer and the Auctioneer Issuer collude, the bidder's privacy will not be revealed.

3.4 Proposed Receipt-free Sealed Bid Auction Scheme

In our scheme, we do not rely on any trusted party. Assume that auctioneer will never work in tandem with Auctioneer Issuer. Also, we argue that the seller S will never collude with a coercer/buyer because the seller is *benefit-collision* with the coercer/buyer. If the bid-rigging occurs, the auction fails to establish the appropriate price and the coercer/buyer may win the auction at an unreasonable low price. So, the bid-rigging is benefit to the coercer/buyer while the seller suffers a great loss.

Bidding : Each bidder B_i generates the receipt-free biding vector $C^*_{i,j}$ with the help of the seller S, where $j = 1, 2, \cdots, n$. Also, they jointly generate the proof of the validity of the bidding vector.

- B_i sends $C_{i,j} = (x_{i,j}, y_{i,j})$ to S, where $j = 1, 2, \cdots, n$.
- For $j = 1$ to n, S chooses β_j and then computes $u_j = g^{\beta_j}$ and $v_j = (h_1 h_2)^{\beta_j}$. Let the receipt-free biding vector is $C^*_{i,j} = (x^*_{i,j}, y^*_{i,j}) = (x_{i,j}u_j, y_{i,j}v_j)$.
- For $j = 1$ to n, S chooses $\gamma_j, \zeta_j, \delta_j \in_R Z_q$ and computes

$$(a_j,\, b_j) = (g^{\gamma_j},\, (h_1 h_2)^{\gamma_j}),\ D_j = g^{\zeta_j} h_{B_i}^{\delta_j}$$

- S computes $H_j = H(a_j, b_j, D_j, x^*_{i,j}, y^*_{i,j})$, $U_j = \gamma_j - \beta_j(H_j + \zeta_j)$. He then sends $(H_j,\, \zeta_j,\, \delta_j,\, U_j)$ and $C^*_{i,j}$ to B_i.
- B_i verifies the equation

$$H_j = H(g^{U_j}(x^*_{i,j}/x_{i,j})^{H_j+\zeta_j}, (h_1 h_2)^{U_j}(y^*_{i,j}/y_{i,j})^{H_j+\zeta_j}, g^{\zeta_j} h_{B_i}^{\delta_j}, x^*_{i,j}, y^*_{i,j})$$

  holds.
- For $j = 1$ to n, B_i chooses $w_j, d_j, r_j \in_R Z_q$.
- If $j = p_i$, B_i computes

$$a_{1,j} = g^{w_j},\ b_{1,j} = (h_1 h_2)^{w_j},\ a_{2,j} = g^{r_j} x_{i,j}^{d_j},\ b_{2,j} = (h_1 h_2)^{r_j}(y_{i,j}/G_2)^{d_j};$$

  else, B_i computes

$$a_{1,j} = g^{r_j} x_{i,j}^{d_j},\ b_{1,j} = (h_1 h_2)^{r_j}(y_{i,j}/G_1)^{d_j},\ a_{2,j} = g^{w_j},\ b_{2,j} = (h_1 h_2)^{w_j};$$

- B_i sends $(a_{1,j}, b_{1,j})$ and $(a_{2,j}, b_{2,j})$ to S, where $j = 1, 2, \cdots, n$.

- For $j = 1$ to n, S chooses $r_{1,j}, r_{2,j}, d_{1,j} \in Z_q$
- S computes $a'_{1,j} = a_{1,j} g^{r_{1,j}} x_{i,j}^{d_{1,j}}$, $b'_{1,j} = b_{1,j}(h_1 h_2)^{r_{1,j}}(y_{i,j}/G_1)^{d_{1,j}}$, $a'_{2,j} = a_{2,j} g^{r_{2,j}} x_{i,j}^{-d_{1,j}}$, $b'_{2,j} = b_{2,j}(h_1 h_2)^{r_{2,j}}(y_{i,j}/G_2)^{-d_{1,j}}$.
- S sends $P_1 = (a'_{1,j}, b'_{1,j}, a'_{2,j}, b'_{2,j})$ to B_i
- B_i computes $c_j = H(a'_{1,j}, b'_{1,j}, a'_{2,j}, b'_{2,j})$, $e_j = c_j - d_j$, $f_j = w_j - a_{ij} e_j$, where $j = 1, 2, \cdots, n$.
- Let $X = e_{p_i}$, $e_{p_i} = d_{p_i}$, $d_{p_i} = X$; $Y = f_{p_i}, f_{p_i} = r_{p_i}, r_{p_i} = Y$;
- For $j = 1$ to n, B_i sends (d_j, r_j), (e_j, f_j) to S.
- For $j = 1$ to n, S computes $d'_{1,j} = d_j + d_{1,j}$, $d'_{2,j} = e_j - d_{1,j}$, $r'_{1,j} = r_j + r_{1,j} - d'_{1,j}\beta_j$, $r'_{2,j} = f_j + r_{2,j} - d'_{2,j}\beta_j$ and sends $P_2 = (d'_{1,j}, d'_{2,j}, r'_{1,j}, r'_{2,j})$ to B_i.
- B_i computes $c_j = d'_{1,j} + d'_{2,j}$ and verifies

$$c_j = H(g^{r'_{1,j}}(x^*_{i,j})^{d'_{1,j}}, (h_1 h_2)^{r'_{1,j}}(y^*_{i,j}/G_1)^{d'_{1,j}}, g^{r'_{2,j}}(x^*_{i,j})^{d'_{2,j}}, (h_1 h_2)^{r'_{2,j}}(y^*_{i,j}/G_2)^{d'_{2,j}})$$

- B_i sends $C^*_{i,j}$, P_1 and P_2 to the corresponding fields of the bulletin board.

Opening : AI and A compute the auction result.

- Let $j = n$, AI and A compute separately the final price vector

$$(X_j, Y_j) = (\prod_{i=1}^{m} x^*_{i,j}, \prod_{i=1}^{m} y^*_{i,j})$$

  They then separately publish $X_j^{x_1}$, $X_j^{x_2}$ and provide a non-interactive zero-knowledge proof of common exponent with their public key h_1, h_2. Let

$$R_j = Y_j / X_j^{x_1 + x_2} = G_1^{l_j} G_2^{m - l_j}$$

  where $0 \le l_j \le m$.[3] If $l_j = 0$, $j = j - 1$; else terminated.
- AI and A determine the first j which satisfies $l_j \neq 0$, and the winning price is the certain j, denote P_w.[4]
- AI and A publish the winning price P_w.

Trading : The winner proves that his bidding price is P_w and buys the auction item. The winner can not repudiate his price, because S can identity the winner with the help of AI and A.

- The winner B_i sends C_{i,P_w} to the seller.
- Since S knows all $C_{i,j}$ for $j = 1, 2, \cdots, n$, and $i = 1, 2, \cdots, m$, he can check the validity of C_{i,P_w} easily. If C_{i,P_w} is valid, go to the next step; else, terminated.

[3] From the result of [8], we know the complexity of computing l_j is $m^{1/2}$. Therefore, m can not be very large, *i.e.*, our scheme is unfit for very large scale auction

[4] If $l_j > 1$, the case of tie-bids occurred for there are l_j winner candidates. However, compare with the previous schemes, we know the numbers of winner candidates. Then these candidates perform the next round of auction.

On the other hand, if n is chosen reasonable large, the bidders can submit the price as his will so that the tie-bids can be avoided.

- The winner provides a knowledge of common exponent to x_{i,P_w} and $y_{i,P_w}/G_1$.
- If the winner wants to cancel the trading, AI and A compute $(x^*_{i,P_w})^{x_1}$ and $(x^*_{i,P_w})^{x_2}$, respectively, where $i = 1, 2, \cdots, m$. So, S can identity the winner i which satisfies $G_1 = y^*_{i,P_w}/(x^*_{i,P_w})^{x_1+x_2}$. S sends the number of the corresponding fields in the bulletin board to the auction service and the service publics the identity of the winner. The winner must be answered for his dishonest deeds, for example, the seller announces his name in the black lists, or the down payment will be expropriated.

4 Receipt-free $M+1$-st Price Auctions

In this section we will extend our scheme for $M+1$-st price auction. The above scheme cannot be extended to $M+1$-st price directly because the winner must prove his bidding price to S in the trading, *i.e.*, S will know all the winners' price.

Abe and Suzuki [1] proposed an $M+1$-st price auction using homomorphic encryption, which enjoys privacy, public verifiability. We will extend this for receipt-free $M+1$-st auction. Firstly, we introduce some definitions as [1].

Definition 1. *Let $E_a(M)$ denotes $(g^a, h^a M)$. Define*

$$E_a(M)E_b(N) = (g^{a+b}, h^{a+b}MN)$$

and

$$(E_a(M))^{-1} = (g^{-a}, h^{-a}M^{-1})$$

Definition 2. *Given a vector*

$$A(j) = (E_{a_1}(M), \cdots, E_{a_j}(M), E_{a_{j+1}}(1), \cdots, E_{a_n}(1))$$

the "differential" vector $\Delta A(j)$ of A_j is defined

$$\Delta A(j) = (E_{b_1}(1), \cdots, E_{b_{j-1}}(1), E_{b_j}(M), E_{b_{j+1}}(1), \cdots, E_{b_n}(1))$$

and satisfies

$$A(j)_n = \Delta A(j)_n, A(j)_{n-1} = \Delta A(j)_{n-1}A(j)_n, \cdots, A(j)_1 = \Delta A(j)_1 A(j)_2$$

where $A(j)_i$ and $\Delta A(j)_i$ denote the i-th components of vectors $A(j)$ and $\Delta A(j)$, respectively. We call $A(j)$ the "integral" vector of $\Delta A(j)$. Therefore, given the "differential" vector of a vector, the vector can be recovered efficiently, vice versa.

In general, we have

Definition 3. *Given a vector*

$$A(j) = (E_{a_1}(M), \cdots, E_{a_j}(M), E_{a_{j+1}}(N), \cdots, E_{a_n}(N))$$

the "differential" vector $\Delta A(j)$ of A_j is defined

$$\Delta A(j) = (E_{b_1}(N), \cdots, E_{b_{j-1}}(N), E_{b_j}(M), E_{b_{j+1}}(N), \cdots, E_{b_n}(N))$$

and satisfies

$$A(j)_n = \Delta A(j)_n, A(j)_{n-1} = \Delta A(j)_{n-1} A(j)_n (A(j)_n)^{-1} = \Delta A(j)_{n-1}$$

$$A(j)_{n-2} = \Delta A(j)_{n-2} A(j)_{n-1} (A(j)_n)^{-1}, \cdots, A(j)_1 = \Delta A(j)_1 A(j)_2 (A(j)_n)^{-1}$$

where $A(j)_i$ and $\Delta A(j)_i$ denote the i-th components of vectors $A(j)$ and $\Delta A(j)$, respectively. Therefore, given the "differential" vector of a vector, the vector can be recovered efficiently, vice versa.

In the $M+1$-st price auction, the bidder B_i proves not only that each component of the bidding vector suits the form of $E(G_1)$ or $E(G_2)$ but also that there is only one component is the form of $E(G_1)$. Otherwise, a malicious bidder will submit an invalid bidding vector to destroy the result of the auction.[5]

We will construct our receipt-free $M+1$-st price auction scheme based on Abe and Suzuki's scheme:

Bidding : Each bidder B_i generates the receipt-free biding vector with the help of the seller S. They then jointly generate the proof of validity of the bidding vector. This is same with the first price sealed bid auction but adding a knowledge proof of that there is only one component in the bidding vector is the form of $E(G_1)$: the bidder B_i proves S that $\prod_{j=1}^{n} x_{i,j}$ and $\prod_{j=1}^{n} y_{i,j}/(G_1 G_2^{n-1})$ have the same exponent.

Opening : AI and A compute the $M+1$-st price.

- AI and A compute the "integral" vector $C_{i,j}^{**} = (x_{i,j}^{**}, y_{i,j}^{**})$ of $C_{i,j}^{*}$.
- Let $j = 1$, AI and A compute separately

$$(X_j, Y_j) = (\prod_{i=1}^{m} x_{i,j}^{**}, \prod_{i=1}^{m} y_{i,j}^{**})$$

  Then they publish $X_j^{x_1}$ and $X_j^{x_2}$, respectively and provide a non-interactive knowledge proof of common exponent with their public key h_1 and h_2. Let

$$R_j = Y_j / X_j^{x_1+x_2} = G_1^{l_j} G_2^{m-l_j}$$

  where $0 \le l_j \le m$. If $l_j \ge M+1$, $j = j+1$; else terminated.

[5] In the first price sealed bid auction, AI and A determine the first j which satisfies $l_j \neq 0$ for $j = n, n-1, \cdots, 1$, and the winning price is j. Then the protocol is terminated. Therefore, the bidder B_i only proves that each component of the bidding vector suits the form of $E(G_1)$ or $E(G_2)$ and the result of the auction will not be affected.

- AI and A determine the first j which satisfies $l_{j-1} \geq M+1$ and $l_j \leq M$, and the winning price is the certain j, denote P_w.
- AI and A publish the winning price P_w.

Trading : The winners prove that their bidding price is large than P_w and buys one of the auction items at the price of P_w. The winners can not repudiate his price, because S can identity them with the help of AI and A.

- The winner B_i sends $C_{i,j}$ to the seller.
- The seller firstly check the validity of $C_{i,j}$ and then compute the "integral" vector vector $C'_{i,j}$ of $C_{i,j}$.
- The winner B_i provides a knowledge proof of common exponent to x'_{i,P_w} and $y'_{i,P_w}/G_1$.
- If some winners want to cancel the trading, for $i = 1, 2, \cdots, m$, AI and A compute $(x^{**}_{i,P_w})^{x_1}$ and $(x^{**}_{i,P_w})^{x_2}$, respectively and then send them to S via the untappable channel.
- S can identity the winner i which satisfies $G_1 = y^{**}_{i,P_w}/(x^{**}_{i,P_w})^{x_1+x_2}$.

5 Analysis of the Proposed Scheme

5.1 Security

The proposed scheme satisfies the following properties:

Privacy. In the first price auction, only the highest price is computed. Unless the auctioneer A and auctioneer issuer AI collude, the information of all losers remains secret. In the $M+1$-st price auction, only the $M+1$-st price is revealed, all other bidding price is secret. Also, the winner remains anonymous unless he wants to repudiate his bidding.

Correctness. It is trivial. No malicious bidders can affect the result of the auction due to the interactive proof of knowledge, which ensures each bidder must generate a valid bidding vector.

Public verifiability. Any entity can obtain the information to verify the correctness of the auction from the designated fields in the bulletin board.

Non-repudiation. With the help of both AI and A, S can know the designated field of the winners in the bulletin board. So, the winner cannot repudiate his bidding.

Receipt-freeness. In our scheme, $D_j = g^{\zeta_j} h_{B_i}^{\delta_j}$ is a trapdoor commitment (or chameleon commitment). Since B_i knows his private key x_{B_i}, he can compute ζ'_j and δ'_j such that $\zeta'_j + x_{B_i}\delta'_j = \zeta_j + x_{B_i}\delta_j$, *i.e.*, he can freely open the commitment as he wants and generate the re-encryption proof for any bidding. For details, see appendix B. Also, we suppose that S will not collude with the coercer/buyer. The coercer/buyer can not know the secret β_j of S. Therefore, the designated-verifier re-encryption proof can not be used to construct a receipt.

5.2 Efficiency

In our schemes, the seller S is involved in the auction to help the bidders to construct the receipt-free bidding. In the previous schemes, this work should be done by the auctioneer. However, there is no special trusted parities in our scheme and the auctioneer may collude with the coercer/buyer. We argue that it is the seller mainly suffered from the bid-rigging so we only trust that the seller will never collude with the coercer/buyer. The auctioneer is responsible for advertising the auction, computing the result of the auction and identifying the winner who wants to repudiate his price with the help of the auctioneer issuer. The auctioneer will not be the bottleneck of the auction. Furthermore, the seller should pay less for the auction since he shares some work of the auctioneer.

In the following we analyze the computation and communication of our scheme (the first price auction). Let n and m represent the number of bidding prices and bidders, respectively. Note that the computation and communication as shown in the tables are for all bidders, not for each bidder.

Table 1 presents the communication patterns, the numbers of the rounds and volume per round in the proposed scheme.

Table 2 shows the computation complexity of our scheme. It is easy to see that the efficiency of the proposed scheme is comparable to that of Abe and Suzuki's scheme.

On the other hand, the complexity of each bidder is proportional to n and the complexity of the seller is proportional to mn. Therefore, as we have mentioned above, our scheme is unsuitable for large scale auction and the price range should be reasonable large.

	Pattern	*Round*	*Volume*
Bidding (bidding vector)	$B_i \leftrightarrow S$	2m	O(n)
Bidding (proof)	$B_i, S \rightarrow$ *Bulletin board*	m	O(n)
Opening	$AI, A \rightarrow$ *Bulletin board*	*at most* m	$O(1)$
Trading (normal case)	$Winner \rightarrow S$	1	$O(1)$
Trading (repudiation case)	$AI, A \rightarrow S$	*at most* m	$O(1)$

Table 1. The communication complexity of our scheme

	Computational Complexity
One Bidder	n *encryptions and proofs*
Seller	mn *verfications and proofs*
A and AI	*at most* 2mn *multiplications*, n *decryptions and verifications*

Table 2. The computation complexity of our scheme

6 Conclusion

Bid-rigging is a dangerous attack in electronic auction. Abe and Suzuki firstly introduced the idea of receipt-free auction to prevent this attack. We point out that their auction scheme only provides receipt-freeness for losing bidders because the secret identity number of the winner can be revealed to the coercer/buyer by the dishonest auctioneers. Also, their scheme is not suitable for $M+1$-st price auction. We claim that it is more important to provide receipt-freeness for winners in the electronic auction. In this paper we propose a new receipt-free sealed bid auction scheme based on three-party trust model by using homomorphic encryption technique, and we extend it suitable for $M+1$-st price auction. Our scheme provides privacy, correctness, public verifiability and receipt-freeness for all bidders.

Acknowledgement

The first author is grateful to K. Suzuki for his meaningful discussion and valuable comments to this paper.

References

1. M. Abe and K. Suzuki, *M+1-st Price Auction using Homomorphic Encryption*, Proceedings of Public Key Cryptography 2002, LNCS 2274, pp.115-124, Springer-Verlag, 2002.
2. M. Abe and K. Suzuki, *Receipt-Free Sealed-Bid Auction*, ISC 2002, LNCS 2433, pp.191 -199, Springer-Verlag, 2002.
3. O. Baudron and J. Stern, *Non-interactive Private Auctions*, Proceedings of Financial Cryptography 2001, LNCS 2339, pp.364-377, Springer-Verlag, 2002.
4. J. Benaloh, D. Tuinstra, *Receipt-free secret-ballot elections*, In Proc. of 26th Symp. On Theory of Computing (STOC'94), pp.544-553, 1994.
5. F. Brandt, *Secure and private auctions without auctioneers*, Technical Report FKI-245-02, Institut fur Informatik, Technische Universitat Munchen, 2002.
6. C. Cachin, *Efficient private bidding and auctions with an obvilious third party*, Proceeding of the 6th ACM Conference on Computer and Communications Security, pp.120-127, 1999.
7. R. Cramer, I. Damgkd and B. Schoenmakers, *Proofs of partial knowledge and simplified design of witness hiding protocols*, Advances in Cryptology-CRYPTO 1994, LNCS 839, pp.174-187, Springer-Verlag, 1994.
8. R. Cramer, R. Gennaro and B. Schoenmakers, *A Secure and Optimally Efficient Multi- Authority Election Scheme*, Advances in Cryptology - EUROCRYPT 1997, LNCS 1233, pp.103-118, 1997.
9. D. Chaum and T.P. Pedersen, *Wallet databases with observers*, Advances in Cryptology-CRYPTO 1992, LNCS 740, pp.89-105, Springer-Verlag, 1993.
10. M.K. Franklin and M.K. Reiter, *The design and implementation of a secure auction server*, IEEE Trans. on Software Engineering, 22(5), pp.302–312, 1996.
11. M. Harkavy, H. Kikuch and J.D. Tygar, *Electronic Auction with Private Bids*, Proceeding of the 3rd USENIX Workshop on Electronic Commence, 1998.

12. M. Hirt and K.Sako, *Efficient receipt-free voting based on homomorphic encryption*, Advances in Cryptology-EUROCRYPT 2000, LNCS 1807, pp.393-403, Springer-verlag, 2000.
13. A. Juels and M. Szydlo, *A Two-Sever, Sealed-Bid Auction Protocol*, Proceedings of Financial Cryptography 2002, LNCS 2357, Springer-Verlag, 2002.
14. H. Kikuchi, *(M+1)st-Price Auction Protocol*, Proceedings of Financial Cryptography 2001, LNCS 2339, pp.351-363, Springer-Verlag, 2002.
15. M. Kilian and E. Pertrank, *Identity Escrow*, Advance in Cryptology-CRYPTO 1998, LNCS 1462, pp.169-185, Springer-Verlag, 1998.
16. B. Lee and K. Kim, *Receipt-free electronic voting scheme with a tamper-resistant randomizer*, ICISC 2002, LNCS 2587, pp.389-406, Springer-Verlag, 2002.
17. H. Lipmaa, N. Asokan and V. Niemi, *Secure Vickrey Auctions without Threshold Trust*, Proceedings of Financial Cryptography 2002, LNCS 2357, pp.87-101, Springer-Verlag, 2002.
18. M. Naor, B. Prinkas and R. Summer, *Privacy Preserving Auctions and Mechanism Design*, Proceedings of ACM conference on E-commerce, pp.129-139, Springer-Verlag, 1999.
19. T. Okamoto, *Receipt-free electronic voting schemes for large scale elections*, In Proceeding of Workshop on Security Protocols'97, LNCS 1361, pp.25-35, Springer-Verlag, 1997.
20. K. Sako, *An Auction Protocol Which Hides Bids of Losers*, Proceedings of Public Key Cryptography 2000, LNCS 1751, pp.422-433, Springer-Verlag, 2000.
21. K. Sako and J. Kilian, *Receipt-free mix-type voting scheme: a practical solution to the implementation of a voting booth*, Advance in Cryptology-EUROCRYPT'95, LNCS 921, pp.393-403, Springer-verlag, 1995.
22. K. Sakurai and S. Mkiyazaki, *An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme*, ACISP 2000, LNCS 1841, Springer-Verlag, pp.385-399, 2000
23. S.G. Stubblebine and P.F. Syverson, *Fair On-line Auction without Special Trusted Parties*, Proceedings of Financial Cryptography 1999, LNCS 1648, pp.230-240, Springer-Verlag, 1999.
24. K. Suzuki, K. Kobayashi and H. Morita, *Efficient Sealed-bid Auction Using Hash Chain*, ICICS 2000, LNCS 2015, pp.183-191, Springer-Verlag, 2000.
25. W. Vickrey, *Counterspeculation, Auctions, and Competitive Sealed Tenders*, Journal of Finance, pp.8-37, 1961.
26. P. R. Wurman, W. E. Walsh and M. P. Wellman, *Flexible Double Auctions for Electronic Commerce: Theory and Implementation*, Decision Support Systems, 24, pp.17-27, 1998.

Appendix A: Proof of Knowledge of Common Exponent

A prover with possession a secret number $\beta \in Z_q$ wants to show that $\log_g u = \log_h v$ while without exposing β, where $u = g^\beta$, $v = h^\beta$. Chaum and Pedersen [9] firstly proposed an interactive protocol to solve this problem.

Let $c = H(a, b, u, v)$, the above protocol could be easily converted into a non-interactive proof of knowledge, where $H()$ is one way hash function.

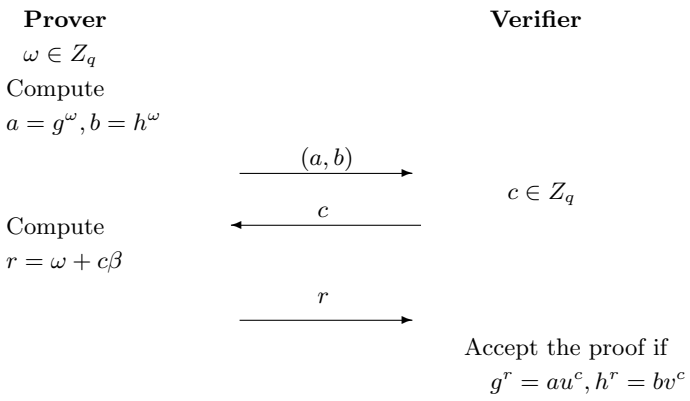

Fig. 1. Proof of knowledge of common exponent

Appendix B: Designated-Verifier Re-encryption Proof

Let $(x, y) = (g^a, h^a m)$ be an original encrypted ElGamal ciphertext for the message m with a public key $h = g^s$ and $(x_f, y_f) = (xg^w, yh^w)$ be a re-encrypted ciphertext by a prover. The prover wants to prove that x_f/x and y_f/y have the same exponent w without exposing the value of w. Suppose $h_v = g^{s_v}$ be the public key of the verifier.

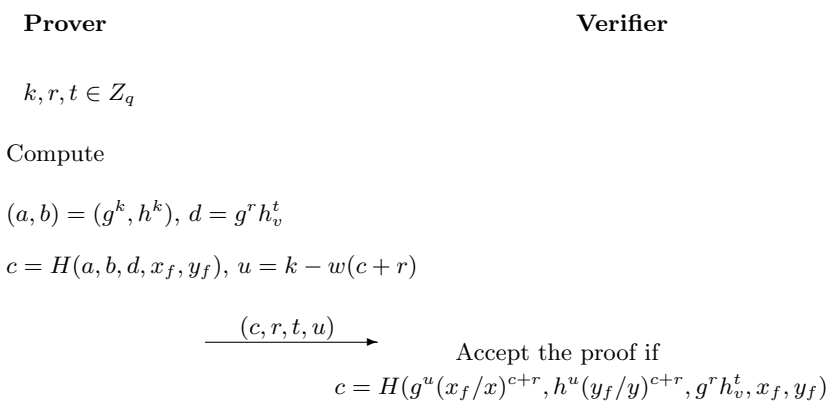

Fig. 2. Designated-verifier re-encryption knowledge proof

The verifier can open the commitment d freely with his private key s_v, *i.e.*, he can compute another pair (r', t') such that $r' + s_v t' = r + s_v t$ holds. Therefore,

the verifier can generate the re-encryption knowledge proof (c', r', t', u') for any pair (x', y') of his choice, where (α, β, u') are randomly chosen numbers, $c' = H(g^{u'}(x_f/x')^{\alpha}, h^{u'}(y_f/y')^{\alpha}, g^{\delta}, x_f, y_f)$, $r' = \alpha - c'$, $t' = (\delta - r')/s_v$.

Appendix C: Prove the Validity of the Bidding Vector

Each bidder and the seller jointly generate a proof of the validity of the bidding vector.

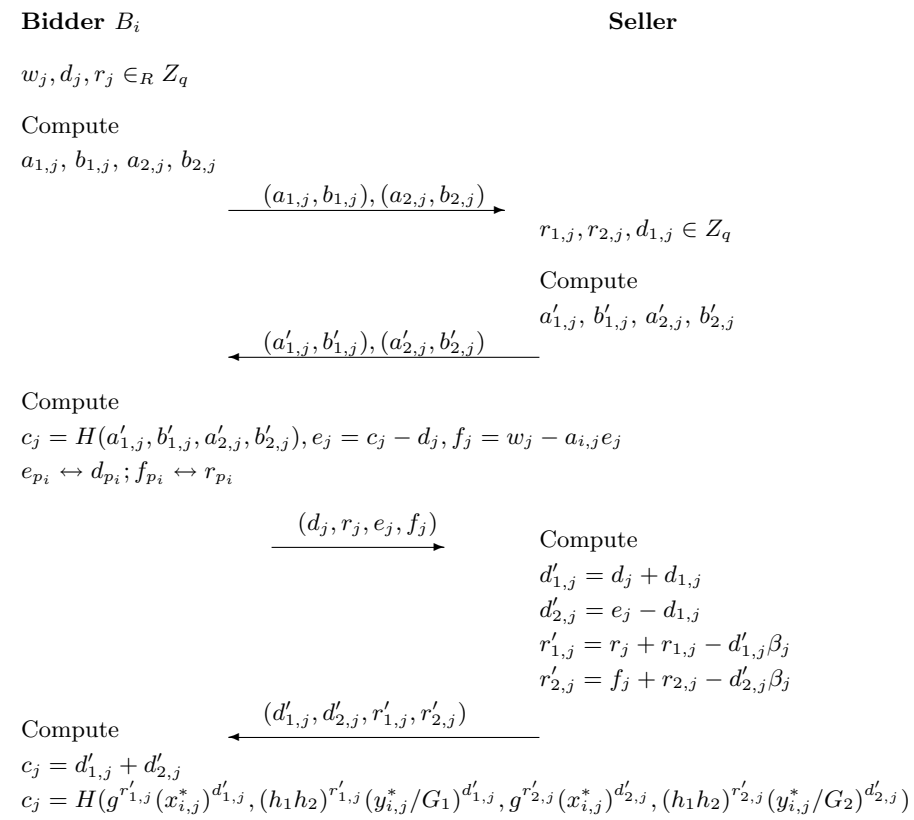

Fig. 3. Proof the validity of the bidding vector

In figure 3, if $j = p_i$, let $a_{1,j} = g^{w_j}$, $b_{1,j} = (h_1h_2)^{w_j}$, $a_{2,j} = g^{r_j}x_{i,j}^{d_j}$, $b_{2,j} = (h_1h_2)^{r_2}(y_{i,j}/G_2)^{d_2}$; else, let $a_{1,j} = g^{r_j}x_{i,j}^{d_j}$, $b_{1,j} = (h_1h_2)^{r_j}(y_{i,j}/G_1)^{d_j}$, $a_{2,j} = g^{w_j}$, $b_{2,j} = (h_1h_2)^{w_j}$.

Correspondingly, let $a'_{1,j} = a_{1,j}g^{r_{1,j}}x_{i,j}^{d_{1,j}}$, $b'_{1,j} = b_{1,j}(h_1h_2)^{r_{1,j}}(y_{i,j}/G_1)^{d_{1,j}}$, $a'_{2,j} = a_{2,j}g^{r_{2,j}}x_{i,j}^{-d_{1,j}}$, $b'_{2,j} = b_{2,j}(h_1h_2)^{r_{2,j}}(y_{i,j}/G_2)^{-d_{1,j}}$.