Optimization of Electronic First-Bid Sealed-Bid Auction Based on Homomorphic Secret Sharing

Kun Peng, Colin Boyd, and Ed Dawson

Information Security Institute,
Queensland University of Technology
{k.peng, c.boyd, e.dawson}@qut.edu.au
http://www.isrc.qut.edu.au

Abstract. Although secret sharing techniques have been applied to implement secure electronic sealed-bid auction for a long time, problems and attacks still exist in secret-sharing-based electronic sealed-bid auction schemes. In this paper, a new secret-sharing-based first-bid e-auction scheme is designed to achieve satisfactory properties and efficiency. Correctness and fairness of the new auction are based on hard computation problems and do not depend on any trust. Complete bid privacy based on a threshold trust is achieved in the new scheme. Attacks to existing secret-sharing-based sealed-bid e-auction schemes are prevented.

1 Introduction

The first secure electronic sealed-bid auction scheme [3] is based on threshold secret sharing. Since then, more secret-sharing-based sealed-bid e-auction schemes [4,6,5,10] have been proposed. Most of them [4,6,10] are supposed to support first-bid sealed-bid e-auction. However as will be shown many security problems exist in these auction schemes and they are vulnerable to various attacks. The newest and most advanced of them, [10], pointed out lack of secret sharing verification and vulnerability to three attacks in the previous secret-sharing-based sealed-bid e-auctions. However, the countermeasures in [10] cannot completely prevent these three attacks. In this paper, drawbacks of the previous secret-sharing-based sealed-bid e-auction schemes are listed and analysed. Then a new secret-sharing-based sealed-bid auction scheme is proposed, which can implement secure and efficient first-bid sealed-bid e-auction. Several attacks in the existing secret-sharing-based sealed-bid e-auction schemes are prevented in the new scheme.

2 Requirements and Related Work

Auction is a useful tool to distribute resources. The principle of auction is to sell goods at the highest possible price. Sealed-bid auction usually contains four phases: preparation phase, bidding phase, bid opening phase and winner determination phase.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 84–98, 2005.

1. In the preparation phase, the auction system is set up and the auction rule is published.
2. In the bidding phase, every bidder submits a sealed bid through a communication network.
3. In the bid opening phase, the bids are opened to determine the winning price.
4. In the winner determination phase, the winner is identified.

The following properties are often desired in sealed-bid auction.

1. **Correctness**: The auction result is determined strictly according to the auction rule. For example, if first bid auction is run, the bidder with the highest bid wins and pays the highest bid.
2. **Bid confidentiality**: Each bid remains confidential to anyone other than the bidder himself before the bid opening phase starts.
3. **Fairness**: No bidder can take advantage of other bidders (e.g. recover other bids and choose or change his own bids according to other bids).
4. **Unchangeability**: Any bidder, especially the winner, cannot change or deny his bid after it is submitted.
5. **Public verifiability**: Correctness of the auction (including validity of the bids, correctness of bid opening and correctness of winner identification) must be publicly verifiable.
6. **Bid Privacy**: Confidentiality of the losing bids must be still retained after the auction finishes. Strictly speaking, no information about any losing bid is revealed except what can be deduced from the auction result.
7. **Robustness**: The auction can still run properly in abnormal situations like existence of invalid bid.

The commonly used auction rules in sealed-bid auctions include first bid auction and Vickrey auction. In a first bid auction, the bidder with the highest bid wins and pays the highest bid. In a Vickrey auction, the bidder with the highest bid wins and pays the second highest bid. Another popular rule, the i^{th} bid auction [5] is a multiple-item version of first bid auction or Vickrey auction.

In a secure auction scheme, secrecy of the bid is very important. Usually, bid confidentiality must be achieved without any trust on the auctioneers, as loss of confidentiality is fatal to fairness of the auction. If a bidder can collude with some auctioneers to know other bids before submitting his own bid, he can win at a price as low as possible in a first bid auction, which violates the principle and fairness of auction. On the other hand, bid privacy can be based on some trust, like a threshold trust on the auctioneers as breach of a bidder's personal privacy is not so serious and is tolerable in some cases. Implementation of bid privacy is rule-dependent. Although Vickery auction is preferred in many applications, it is difficult to achieve bid privacy in Vickrey auction. As the winner's bid and the identity of the bidder submitting the winning bid must be kept secret as required in bid privacy, there is no practical method to achieve bid privacy in Vickrey auction. As bid privacy is required in this paper, we focus on first-bid auction.

Except [3], all the secret-sharing-based sealed-bid e-auction schemes employ one-choice-per-price strategy. Under this strategy, the price space (containing all the biddable prices) is much smaller than the input domain of the sealing function and each bidder must make a choice (indicating willingness or unwillingness to pay) at every biddable price to form his bidding vector. If a bidder is willing to pay a price, he chooses a non-zero integer standing for "YES" as his choice at that price. If a bidder is unwilling to pay a price, he chooses zero standing for "NO" as his choice at that price. The bidders seal their bidding vectors (including choices at all the biddable prices) and submit the sealed bidding vectors in the bidding phase. These sealed-bid e-auction schemes also employ additive homomorphic secret sharing and binary search. The bidders use additive homomorphic secret sharing (e.g. Shamir's secret sharing [12] and its variants) to seal their bidding choices. Then a binary search for the winning price is performed along a binary route among the biddable prices. In the search, the auctioneers exploit additive homomorphism of the sharing function (the summed shares of all the choices at a price can reconstruct the sum of the choices at that price) to implement bid opening at every price on the binary searching route until finally the winning price is met.

Among the existing secret-sharing-based first-bid e-auction schemes [3,4,6,10], the most recent and advanced one is [10]. The auction scheme in [3] is simple, but does not support bid privacy. Secret bid sharing in [3,4,6] is not verifiable, so the bids are changeable and a bidder can collude with an auctioneer to compromise correctness and fairness. Besides lack of verifiability [10] points out three attacks to the previous schemes [4,6], ABC (auctioneer-bidder collusion) attack, BBC (bidder-bidder collusion) attack and dispute attack. In an ABC attack, some auctioneers collude with a bidder to compromise correctness or fairness. In a BBC attack, some bidders collude to compromise correctness or fairness. In a dispute attack, an auctioneer accuses a bidder of submitting an invalid (encrypted) choice share and the bidder cannot prove his innocence without revealing the share. However, the auction scheme in [10] cannot completely prevent these three attacks.

The auction scheme in [10] prevented an ABC attack in [4,6]: an auctioneer helps a bidder to change his bid after submitting it. However, [10] is vulnerable to another ABC attack in first-bid auction. As bid sealing depends on threshold secret sharing, any submitted sealed bid can be opened before the bid opening phase if the number of malicious auctioneers is over the sharing threshold. These malicious auctioneers then can reveal the opened bids to a waiting colluding bidder, who can bid just higher than the submitted bids and win at a price as low as possible. This attack is an ABC attack and definitely compromises fairness of the auction. Although a threshold trust on the auctioneers is assumed in [10] and this ABC attack does not exist under the threshold trust, this threshold trust assumption is too strong for correctness and fairness of the auction. It is appropriate to base less important properties like bid privacy on the threshold trust assumption. However, as stated before, bid confidentiality must be achieved without any trust on the auctioneers as it affects correctness and fairness of the

auction. So this ABC attack against correctness and fairness must be prevented without any assumption on the auctioneers.

The existing secret-sharing-based sealed-bid e-auction schemes are vulnerable to BBC attack as well. For example, three colluding bidders B_1, B_2 and B_3 may perform the following attack against first bid auction where in a bidding choice no-zero integer Y and 0 stand for "YES" and "NO" respectively.

- B_1, B_2 and B_3 estimate that the other bidders' bids are lower than p_μ while their own evaluation is p_ν, which is higher than p_μ. They try to win the auction and pay as low as possible.
- B_1 bids Y at prices no higher than p_μ and zero at other prices; B_2 bids Y at prices no higher than p_ν and zero at other prices; B_3 bids $-Y$ at prices higher than p_μ but no higher than p_ν and zero at other prices.
- If all other bidder submits a bid lower than p_μ as expected, the sum of choices at p_μ is non-zero and the sum of choices at prices higher than p_μ is 0. So p_μ is the winning price and there is a tie between B_1 and B_2. One of them gives up and the other wins at p_μ.
- If other bidders' highest bid, p_H is no lower than p_μ but lower than p_ν, the sum of choices at p_H is larger than zero and the sum of choices at prices higher than p_H is 0. So some other bidder wins the auction at p_H together with B_2. B_2 disputes the tie and publishes his bid to win the auction at p_ν.
- If other bidders' highest bid is p_ν, the sum of choices at p_ν is larger than zero and the sum of choices at prices higher than p_ν is 0. So some other bidder draws with B_2 at p_ν. B_2 still has a chance to win the auction in the following tie-breaking operation.

With this attack, either B_1 or B_2 win unless another bidder submits a bid higher than the attackers' evaluation. The attackers can pay a price lower than their evaluation if the other bids are as low as the attackers expect.

It is pointed out in [10] that the previous secret-sharing-based e-auction schemes [3,4,6,5] are not publicly verifiable when bid privacy must be retained. As a result of lack of pubic verifiability, these schemes cannot deal with dispute between bidders and auctioneers, so are vulnerable to the dispute attack. To prevent the dispute attack, [10] suggests to use publicly verifiable secret sharing (PVSS) to distribute the bids. A PVSS protocol based on Bao's proof of equality of logarithms in different cyclic groups with different orders [1] is proposed in [10]. However, Bao's proof is neither specially sound nor zero knowledge. Bao only used it in a special verifiable encryption scheme, where he believes soundness and ZK property of the proof is not necessary. Application of Bao's proof in [10] is not appropriate. The PVSS in [10] cannot prevent the dispute attack as invalid bid can pass its verification. Moreover, the PVSS reveals some information about the bids.

To protect bid confidentiality and privacy when the bidding choices are in a small set, information-theoretically hiding secret sharing scheme proposed by Pedersen [9] is employed in [10] to share the bidding choices, whose computational and communication cost is twice as high as a computationally hiding verifiable secret sharing scheme like [8]. However, as will be shown later in the

new auction scheme in this paper a computationally hiding verifiable secret sharing is enough to protect bid confidentiality and privacy if the auction protocol is well designed. Although information-theoretically hiding property is achieved in the bid sharing in [10] at a high cost, bids in that scheme are not information-theoretically confidential and not even semantically confidential as Paillier encryption is simplified in [10] to lose semantic security. In addition, bid privacy is not complete in [10]. At every price on the binary searching route, the number of "YES" choices is revealed.

In this paper, a new secret-sharing-based first-bid e-auction is designed, which can prevent the three attacks and achieve complete bid privacy more efficiently.

3 Pedersen's Verifiable Secret Sharing

Since Shamir proposed the first threshold secret sharing scheme [12], many threshold secret sharing techniques have appeared. Using these techniques, a secret holder can share a secret among multiple share holders. The secret can be recovered if the number of cooperating share holders is over a certain threshold, T. If the secret holder is not trusted, there must be a mechanism the share holders can use to verify that they get a set of valid shares of a unique secret. This requirement is very important for the robustness of applications like auctions. Secret sharing with this mechanism is called VSS (verifiable secret sharing). Shamir's secret sharing was extended by Pedersen to be verifiable as follows [8].

1. G is the subgroup of Z_p^* with order q where p and q are large primes such that q divides $p-1$. Integer g is a generator of G.
2. A builds a polynomial $f(x) = \sum_{j=0}^{T} a_j x^j$ where $a_0 = s$ and a_j for $j = 1, 2, \ldots, T$ are random integers.
3. A publishes $E_j = g^{a_j}$ for $j = 0, 1, \ldots, T$.
4. A sends $s_i = f(i)$ as a share to share holder P_i.
5. P_i verifies $g^{s_i} = \prod_{j=0}^{T} E_j^{i^j}$. If the verification is passed, P_i can be sure that s_i is the i^{th} share of $\log_g E_0$.
6. If at least $T+1$ share holders get correct shares, $\log_g E_0$ can be recovered by them corporately.

In this paper, Pedersen's verifiable secret sharing will be employed, which has the following three properties.

- Correctness: if the secret holder follows the VSS protocol, he can share his secret such that each share can pass the verification.
- Soundness: if the verification is passed, any share set containing more than T shares can be used to recover secret $\log_g E_0$.
- Homomorphism: if multiple secrets are shared among the same sets of share holders, they can sum up the shares to recover the sum of the secrets.

4 The New Auction Scheme

The basic structure of a secret-sharing-based sealed-bid e-auction is inherited in this new scheme. Like in other secret-sharing-based sealed-bid e-auction schemes,

the bidders share their bids among the auctioneers, who employ homomorphic bid opening and binary search to determine the winning price. However, in the new auction schemes, certain measures are taken to prevent the attacks and overcome the drawbacks in the existing secret-sharing-based sealed-bid e-auction schemes. Two rounds of communication are employed between the bidders and the auctioneers, while only one round of communication is employed in the existing schemes. In the first round the bidders commit to their bids and publish the commitments. The committing function is information-theoretically hiding, such that it is impossible for anyone to recover any bid from the commitments. The committing function is computationally binding, such that to find two different ways to open the commitments is as hard as the discrete logarithm problem. In the second round the bidders share the bid opening information among the auctioneers through an additive homomorphic VSS mechanism, so that the auctioneers can cooperate to recover sum of the bidding choices. Hiding property of the committing function prevents ABC attack, while binding property of the committing function guarantees unchangeability. The auctioneers randomize the bidding choices before they are summed up, so that BBC attack is prevented. The verifiable secret sharing in [8] is employed in the new scheme, which is additive homomorphic and efficient. A dispute-settling function based on that VSS technique and verifiable encryption is designed to settle dispute on validity of encrypted shares. As the bidding choices are randomized before they are summed up, no information about the losing bids is revealed although the sum of the bidding choices is published at the prices on the binary searching route.

Suppose there are w biddable prices $p_1, p_2, \ldots, p_w$ in decreasing order, n bidders $B_1, B_2, \ldots, B_n$ and m auctioneers $A_1, A_2, \ldots, A_m$. The auction protocol is as follows.

1. **Preparation phase**
   A bulletin board is set up as a broadcast communication channel. Each A_j establishes his Paillier encryption [7]) algorithm with public key N_j (product of two secret large primes) and g_j (whose order is a multiple of N_j), message space Z_{N_j}, multiplicative modulus N_j^2, encryption function $E_j(x) = g_j^x r^{N_j} \bmod N_j^2$ and a corresponding decryption function $D_j()$. A_j publishes on the bulletin board his encryption function and public key for $j = 1, 2, \ldots, m$. Large primes p and q are chosen such that q is a factor of $p - 1$ and $nq^2 < N_j$ for $j = 1, 2, \ldots, m$. Cyclic group G contains all the quadratic-residues in Z_p^* and has an order q. Random primes f, g and h are chosen such that $\log_g f$ and $\log_h g$ are unknown. The bid committing function is $Com(x) = f^x g^r \bmod p$ where x is a bidding choice in Z_q and r is a random integer in Z_q. A sharing threshold parameter T smaller than m is chosen. System parameters p, q, f, g, h, T and N_j for $j = 1, 2, \ldots, m$ are published on the bulletin board.
2. **Bidding phase**
   Each bidder B_i selects his bidding vector $(b_{i,1}, b_{i,2}, \ldots, b_{i,w})$ as his choices at $p_1, p_2, \ldots, p_w$ where $b_{i,l} \in Z_q$ for $l = 1, 2, \ldots, w$. If he is willing to pay p_l, $b_{i,l}$ is a random non-zero integer modulo q; if he is unwilling to pay p_l,

$b_{i,l} = 0$. Then he signs and publishes $c_{i,l} = Com(b_{i,l}) = f^{b_{i,l}} g^{r_{i,l}} \bmod p$ for $l = 1, 2, \ldots, w$ on the bulletin board where $r_{i,l}$ is randomly chosen from Z_q.

3. **Bid opening phase**

(a) Bid randomization
Each auctioneer A_j publishes a commitment (e.g. one-way hash function) of random integer $R_{j,i,l}$ from Z_q for $i = 1, 2, \ldots, n$ and $l = 1, 2, \ldots, w$. After all the commitments have been published, the auctioneers publish $R_{j,i,l}$ for $j = 1, 2, \ldots, m$ as randomizing factors of $b_{i,l}$ on the bulletin board.

(b) Secret sharing
Each B_i calculates $R_{i,l} = \sum_{j=1}^{m} R_{j,i,l} \bmod q$. Then he calculates $s_{i,l} = r_{i,l} R_{i,l} \bmod q$ as his secret at p_l for $l = 1, 2, \ldots, w$. B_i chooses polynomials $F_{i,l}(x) = \sum_{k=0}^{T} a_{i,l,k} x^k \bmod q$ for $l = 1, 2, \ldots, w$ where $a_{i,l,0} = s_{i,l}$ and $a_{i,l,k}$ for $k = 1, 2, \ldots, T$ are randomly chosen. B_i publishes encrypted shares $S_{i,l,j} = E_j(F_{i,l}(j)) = g_j^{F_{i,l}(j)} t_{i,l,j}^{N_j} \bmod N_j^2$ for $l = 1, 2, \ldots, w$ and $j = 1, 2, \ldots, m$ on the bulletin board where $t_{i,l,j}$ is randomly chosen from $Z_{N_j}^*$. B_i publishes sharing commitments $C_{i,l,k} = h^{a_{i,l,k}} \bmod p$ for $l = 1, 2, \ldots, w$ and $k = 0, 1, \ldots, T$ on the bulletin board.

(c) Binary search
The auctioneers cooperate to perform a binary search. At a price p_l on the searching route, the following operations are performed.

i. Share verification
Each A_j calculates his summed shares $v_{j,l} = D_j(\prod_{i=1}^{n} S_{i,l,j} \bmod N_j^2)$ and the corresponding commitments $u_{l,k} = \prod_{i=1}^{n} C_{i,l,k} \bmod p$ for $k = 0, 1, \ldots, T$. He then verifies $h^{v_{j,l}} = \prod_{k=0}^{T} u_{l,k}^{j^k} \bmod p$. If the verification is passed, he goes on to next step. Otherwise, he verifies $h^{D_j(S_{i,l,j})} = \prod_{k=0}^{T} C_{i,l,k}^{j^k} \bmod p$ for $i = 1, 2, \ldots, n$ and will meet at least one failed verification. If the verification fails when $i = I$, A_j accuses bidder B_I of submitting an invalid encrypted share $S_{I,l,j}$. If B_I disputes on the accusation, the following dispute settling procedure is used. A_j publishes $z_{I,l,j} = D(S_{I,l,j})$ such that anyone can verify $h^{z_{I,l,j}} \neq \prod_{k=0}^{T} C_{I,l,k}^{j^k} \bmod p$. If $h^{z_{I,l,j}} \neq \prod_{k=0}^{T} C_{I,l,k}^{j^k} \bmod p$, B_I has to publish $t_{I,l,j}$ and proves his knowledge of $\log_{g_j}(S_{I,l,j} / t_{I,l,j}^{N_j})$ using the zero knowledge proof of knowledge of logarithm in [11][1]. B_I asks the auctioneers to verify his proof and $S_{I,l,j} \neq g_j^{z_{I,l,j}} t_{I,l,j}^{N_j} \bmod N_j^2$. If

$$h^{z_{I,l,j}} = \prod_{k=0}^{T} C_{I,l,k}^{j^k} \bmod p \vee$$
$$(S_{I,l,j} \neq g_j^{z_{I,l,j}} t_{I,l,j}^{N_j} \bmod N_j^2 \ \wedge \ B_I\text{'s proof is correct})$$

[1] Although the parameter setting in [11] is a little different from the parameter setting in Paillier encryption (When [11] was proposed, Paillier encryption had not appeared), the proof protocol in [11] can be applied here without compromising its correctness, soundness or zero knowledge property.

the accusation against B_I is wrong and A_j is removed. Otherwise, B_I is removed from the auction and may be punished; share verification is run again.

ii. Homomorphic secret recovery
Each A_j publishes $v_{j,l}$, whose validity can be verified by anyone against $C_{i,l,k}$ for $i = 1, 2, \ldots, n$ and $k = 0, 1, \ldots, T$. If at least $T + 1$ summed shares are correct, the summed secret can be recovered. For simplicity, suppose the first $T + 1$ summed shares are correct, then the summed secret is recovered: $d_l = \sum_{i=1}^{n} s_{i,l} = \sum_{j=1}^{T+1} v_{j,l}^{x_j} \bmod q$ where $x_j = \prod_{1 \le k \le t+1, k \ne j} \frac{k}{k-j} \bmod q$.

iii. Homomorphic bid opening
Equation $\prod_{i=1}^{n} c_{i,l}^{R_{i,l}} = g^{d_l} \bmod p$ is tested. If this equation is correct, the sum of the randomized bidding choices at p_l is zero, the binary search at p_j ends negatively and the search goes down. If this equation is incorrect, the sum of randomized bidding choices at p_l is not zero, the binary search at p_j ends positively and the search goes up.

In the end of the binary search, the winning price is found.

4. **Winner identification phase**
Suppose the winning price is p_L. Decrypted shares $d_{i,L,j} = D_j(S_{i,L,j})$ for $i = 1, 2, \ldots, n$ are published. $h^{d_{i,L,j}} = \prod_{k=0}^{T} C_{i,L,k}^{j^k} \bmod p$ is verified for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$. If any bidder's secret is found to be incorrectly shared, he is removed from the auction and may be punished. If he disputes, the dispute can be solved like in Step 3(c)i. If at least $T+1$ correct shares can be found for B_i, his secret $d_{i,L}$ can be recovered: $d_{i,L} = \sum_{j=1}^{T+1} d_{i,L,j}^{x_j} \bmod p$ (For simplicity, assume the first $T + 1$ shares are correct). Then equation $c_{i,L}^{R_{i,L}} = g^{d_{i,L}} \bmod p$ is tested for $i = 1, 2, \ldots, n$. Only when $c_{i,L}^{R_{i,L}} \ne g^{d_{i,L}} \bmod p$, is B_i a winner. Suppose $c_{I,L}^{R_{I,L}} \ne g^{d_{I,L}} \bmod p$. Then B_I must prove that he is really a winner by proving knowledge of $\log_f(c_{I,L}^{R_{I,L}} / g^{d_{I,L}})$ using the zero knowledge proof of knowledge of logarithm in [11]. Any B_I failing to give this proof is a cheater and punished. The winner's signature is verified and his identity is published. If there is more than one winner, a new auction is run among the winners.

Table 1. Comparison of homomorphic secret-sharing-based first-bid auction schemes

Operation	[4,6,10]	New auction
the first round of communication	share bidding choice $b_{i,l}$	commit bidding choice $b_{i,l}$ in $c_{i,l} = f^{b_{i,l}} g^{r_{i,l}}$
the second round of communication	non-existent	randomize $r_{i,l}$ into $s_{i,l} = r_{i,l} R_{i,l}$ and share $s_{i,l}$
bid opening	recover $\sum_{i=1}^{n} b_{i,l}$ and test whether $\sum_{i=1}^{n} b_{i,l} > 0$	recover $d_l = \sum_{i=1}^{n} s_{i,l}$ and test whether $\prod_{i=1}^{n} c_{i,l}^{R_{i,l}} = g^{d_l}$
dispute settlement	non-existent or vulnerable	solved by VSS and verifiable encryption

In Table 1, the new secret-sharing-based first-bid auction scheme is compared against the existing homomorphic secret-sharing-based first-bid auction schemes [4,6,10]. It is clear that in the new scheme, two-round communication and commitment prevent the ABC attack; the randomization prevents the BBC attack and strenghens bid privacy; the dispute settling procedure prevents the dispute attack.

5 Analysis

Security and efficiency of the new auction scheme is analysed in this section. Readers can check that if the bidders and auctioneers follow the protocol, the auction outputs a correct result. Note that although two different kinds of additive modulus p and N_j are used in the protocol, no modulus conflict happens as $r_{i,l}$, $R_{i,l}$ are chosen from Z_q and $nq^2 < N_j$.

5.1 Security Analysis

In the following, it is demonstrated that the auction is correct as long as at least one auctioneer is honest.

Theorem 1. *The auction protocol is correct with an overwhelmingly large probability if at least one auctioneer is honest. More precisely, the bidder with the highest bid wins with an overwhelmingly large probability if at least one auctioneer is honest.*

To prove this theorem, the following three lemmas must be proved first.

Lemma 1. *If* $\sum_{i=1}^{n} y_i s_i = 0 \bmod q$ *with a probability larger than* $1/q$ *for random* $s_1, s_2, \ldots, s_n$ *from* Z_q*, then* $y_i = 0 \bmod q$ *for* $i = 1, 2, \ldots, n$*.*

Proof: Given any integer k in $\{1, 2, \ldots, n\}$, there must exist integers $s_1, s_2, \ldots, s_{k-1}, s_{k+1}, \ldots, s_n$ in Z_q and two different integers s_k and $\hat{s}_k$ in Z_q such that the following two equations are correct.

$$\sum_{i=1}^{n} y_i s_i = 0 \bmod q \tag{1}$$

$$(\sum_{i=1}^{k-1} y_i s_i) + y_k \hat{s}_k + \sum_{i=k+1}^{n} y_i s_i = 0 \bmod q \tag{2}$$

Otherwise, for any $s_1, s_2, \ldots, s_{k-1}, s_{k+1}, \ldots, s_n$ there is at most one s_k to satisfy equation $\sum_{i=1}^{n} y_i s_i = 0 \bmod q$. This deduction implies among the q^n possible combinations of $s_1, s_2, \ldots, s_n$, equation $\sum_{i=1}^{n} y_i s_i = 0 \bmod q$ is correct for at most q^{n-1} combinations. This conclusion leads to a contradiction: given random integers s_i from Z_q for $i = 1, 2, \ldots, n$, equation $\sum_{i=1}^{n} y_i s_i = 0 \bmod q$ is correct with a probability no larger than $1/q$.

Subtracting (2) from (1) yields

$$y_k(s_k - \hat{s}_k) = 0 \bmod q$$

Note that $s_k - \hat{s}_k \neq 0 \bmod q$ as $s_k \neq \hat{s}_k \bmod q$. So, $y_k = 0 \bmod q$. Note that k can be any integer in $\{1, 2, \ldots, n\}$. Therefore $y_i = 0 \bmod q$ for $i = 1, 2, \ldots, n$. □

Lemma 2. *When the binary search at a price p_l ends negatively, $b_{i,l} = 0$ for $i = 1, 2, \ldots, n$ with an overwhelmingly large probability if at least one auctioneer is honest where $b_{i,l}$ is B_i's choice at p_l and committed in $c_{i,l}$.*

Proof: That the binary search at a price p_l ends negatively implies

$$\prod_{i=1}^{n} c_{i,l}^{R_{i,l}} = g^{d_l} \bmod p$$

where d_l is the summed secret recovered at p_l. So

$$\prod_{i=1}^{n} (f^{b_{i,l}} g^{r_{i,l}})^{R_{i,l}} = g^{d_l} \bmod p$$

Namely

$$f^{\sum_{i=1}^{n} R_{i,l} b_{i,l}} g^{\sum_{i=1}^{n} R_{i,l} r_{i,l}} = g^{d_l} \bmod p$$

Note that $b_{i,l}$ is committed in $c_{i,l} = f^{b_{i,l}} g^{r_{i,l}}$ by B_i and d_l is recovered from the shares from the bidders. So the bidders can cooperate to find $\sum_{i=1}^{n} R_{i,l} b_{i,l}$, $\sum_{i=1}^{n} R_{i,l} r_{i,l}$ and d_l in polynomial time.

So, if $\sum_{i=1}^{n} R_{i,l} b_{i,l} \neq 0$, the bidders can cooperate to find in polynomial time

$$\log_g f = (d_l - \sum_{i=1}^{n} R_{i,l} r_{i,l}) / \sum_{i=1}^{n} R_{i,l} b_{i,l},$$

which is contradictory to the assumption that $\log_g f$ is unknown and the discrete logarithm problem is hard to solve. So, $\sum_{i=1}^{n} R_{i,l} b_{i,l} = 0$. Note that $R_{i,l}$ for $i = 1, 2, \ldots, n$ are random integers in Z_q as they are corporately chosen by the auctioneers, at least one of which is honest. Therefore, according to Lemma 1. $b_{i,l} = 0$ for $i = 1, 2, \ldots, n$ with an overwhelmingly large probability. □

Lemma 3 guarantees that no bidder can change a "YES bid into a "NO bid.

Lemma 3. *If the binary search at a price p_l ends positively, then there exists I in $\{1, 2, \ldots, n\}$ such that one of the following two statements is true: 1) $b_{I,l} \neq 0$; 2) $b_{I,l} = 0$ but B_I cannot find $\log_f(c_{I,l}^{R_{I,l}} / g^{d_{I,l}})$ in polynomial time.*

Proof: That the binary search at a price p_l ends positively implies

$$\prod_{i=1}^{n} c_{i,l}^{R_{i,l}} \neq g^{d_l} \bmod p$$

where d_l is the summed secret recovered at p_l.

Soundness and homomorphism of the employed VSS [8] guarantees that

$$h^{d_l} = u_{l,0} = \prod_{i=1}^{n} C_{i,l,0} \bmod p$$

So,

$$\prod_{i=1}^{n} c_{i,l}^{R_{i,l}} \neq g^{\log_h \prod_{i=1}^{n} C_{i,l,0}} \bmod p$$

Namely,

$$\prod_{i=1}^{n} c_{i,l}^{R_{i,l}} \neq g^{\sum_{i=1}^{n} \log_h C_{i,l,0}} \bmod p,$$

which implies

$$\prod_{i=1}^{n} c_{i,l}^{R_{i,l}} \neq \prod_{i=1}^{n} g^{\log_h C_{i,l,0}} \bmod p$$

So there must exists integer I such that $1 \leq I \leq n$ and

$$c_{I,l}^{R_{I,l}} \neq g^{\log_h C_{I,l,0}} \bmod p$$

Suppose $g^{\log_h C_{I,l,0}}/(c_{I,l}^{R_{I,l}}) = f^{e_I}$, then $e_I \neq 0 \bmod q$. So

$$c_{I,l}^{R_{I,l}} = f^{e_I} g^{\log_h C_{I,l,0}} \bmod p$$

Namely

$$(f^{b_{I,l}} g^{r_{I,l}})^{R_{I,l}} = f^{e_I} g^{\log_h C_{I,l,0}} \bmod p$$

where $b_{i,l}$ is B_i's choice at p_l, which is committed in $c_{i,l}$.

Note that B_I knows $b_{I,l}$ and $r_{I,l}$ as he committed to $b_{I,l}$ as $c_{I,l} = f^{b_{I,l}} g^{r_{I,l}}$; B_I can find $\log_h C_{I,l,0}$ in polynomial time as his shares at p_j enable anyone to calculates $\log_h C_{I,l,0}$ in polynomial time. So, if B_I can find e_I in polynomial time, he can find $\log_g f = (\log_h C_{I,l,0} - r_{I,l} R_{I,l})/(b_{I,l} R_{I,l} - e_I)$ in polynomial time. So, when $b_{I,l} = 0$ either a contradiction to the assumption that $\log_g f$ is unknown and the discrete logarithm problem is hard to solve is found or B_I cannot find $e_I = \log_f(c_{I,l}^{R_{I,l}}/g^{d_{I,L}})$. Therefore, there exists I in $\{1, 2, \ldots, n\}$ such that one of the following two statements is true.

- $b_{I,l} \neq 0$;
- $b_{I,l} = 0$ but B_I cannot find $\log_f(c_{I,l}^{R_{I,l}}/g^{d_{I,l}})$ in polynomial time. □

Proof of Theorem 1:
Lemma 2 and Lemma 3 guarantee that if there is at least one honest auctioneer

- when a bidder submits a "YES" choice at a price, he can open it as a "NO" choice with an overwhelmingly small probability;
- when a bidder b_i submits a "NO" choice at a price p_l but opens it as a "YES" choice, he cannot find $\log_f(c_{i,l}^{R_{i,l}}/g^{d_{i,l}})$ in polynomial time.

So the binary search guarantees that if there is at least one honest auctioneer

- when a bidder submitted a "YES" choice at a price on the searching route, the search always go upwards at that price with an overwhelmingly large probability;
- when a bidder b_i submitted a "NO" choice at a price p_l on the searching route, either the search always go downwards at p_l or he cannot find $\log_f(c_{i,l}^{R_{i,l}}/g^{d_{i,l}})$ in polynomial time.

So when winning price p_L is determined in the bid opening phase,

- there is no "YES" choice at higher prices with an overwhelmingly large probability if there is at least one honest auctioneer;
- if there is at least one honest auctioneer, then at the winning price
  - either there is at least one "YES" choice,
  - or a bidder B_i submits "NO" choice at p_L, open it as "YES", but cannot find $\log_f(c_{i,L}^{R_{i,L}}/g^{d_{i,L}})$ in polynomial time.

  Note that in the winner identification phase, any bidder B_I opening his choice as "Yes" at the winning price must prove that he is really a winner by proving knowledge of $\log_f(c_{I,L}^{R_{I,L}}/g^{d_{I,L}})$. So in the winner identification phase either some winner or some cheating bidder is identified with an overwhelmingly large probability if there is at least one honest auctioneer. If a winner is found, the auction ends correctly. If only cheating bidder(s) is found, the cheating bidder is removed and the auction runs again. Finally a correct winner can be definitely found when all the cheating bidders have been removed. □

If a penalty to identified cheating bidders is applied, the bidders will be deterred from cheating and re-running can be avoided. If no strong penalty is available and the re-running mechanism after finding a cheating bidder is not appropriate in some special applications, the auction protocol can be slightly modified so that the winning price found in the bid opening phase is always correct and a real winner can always be found at the winning price. Only a simple additional operation is needed in the modification: each bidder has to prove that his submitted bid hidden by $Com()$ is consistent with the secret shares provided by him in the bid opening phase. In the proof B_i shows that at each biddable price p_l he knows two secrets $b_{i,l}$ and $r_{i,l}$ such that $c_{i,l} = f^{b_{i,l}} g^{r_{i,l}}$ and $C_{i,l,0} = h^{r_{i,l} R_{i,l}}$ without revealing $b_{i,l}$ or $r_{i,l}$. This proof can be built on ZK proof of knowledge of logarithm [11] and ZK proof of equality of logarithms [2]. With this modification Lemma 3 can be modified to Lemma 4, which is simpler.

Lemma 4. *If the binary search at a price p_l ends positively, then there exists I in $\{1, 2, \ldots, n\}$ such that $b_{I,l} \neq 0$.*

The proof of Lemma 4 is simpler than that of Lemma 3, so is not provided here. With this modification and Lemma 4, Theorem 1 can be proved more easily, winner identification becomes simpler and rerunning can be avoided. However, bidding becomes less efficient with additional $O(nw)$ ZK proof and verification

operations. In most cases, we believe that punishment can deter the bidders from cheating and rerunning can be avoided. So usually, this additional proof is not adopted for the sake of efficiency, which is assumed in efficiency analysis later.

Table 2. Property comparison

Auction schemes	Correct--ness	Bid confi--dentiality	Fairness	Unchan--geability	Public verifiability	Bid privacy	Robust--ness
[3]	Vulnerable to attacks	Trust -de--pendent	Trust -de--pendent	No	Yes	No	Yes
[4] [6]	Vulnerable to attacks	Trust de--pendent	Trust de--pendent	No	No	Trust de--pendent	No
[10]	Vulnerable to attacks	Trust de--pendent	Trust de--pendent	Yes	Yes	Trust de--pendent	No
New auction	Yes	Yes	Yes	Yes	Yes	Trust de--pendent	Yes

As the commitment function $Com()$ is information-theoretically hiding, bid confidentiality is information-theoretically achieved and the ABC attack is information-theoretically prevented. Binding of $Com()$ and usage of digital signature guarantees unchangeability. As the bidding choices are randomized before they are summed up, the BBC attack can be prevented if at least one auctioneer is honest. The employed VSS [8] and the new dispute settling procedure[2] in Step 3(c)i can solve the dispute attack. With these three attacks prevented, the new auction protocol is fair and robust. Every operation in the auction protocol is publicly verifiable. If the number of malicious auctioneers is not over the sharing threshold, bid privacy can be achieved.

A property comparison of the secret-sharing-based sealed-bid e-auction schemes is provided in Table 2. [3] cannot achieve bid privacy and public verifiability at the same time. It is assumed in Table 2 that public verifiability, a more important property is achieved while bid privacy is sacrificed.

5.2 Efficiency Analysis

An efficiency comparison of the secret-sharing-based sealed-bid e-auction schemes is provided in Table 3. In Table 3, full-length exponentiations are counted, where Paillier encryption and RSA signature are assumed to be employed. It is illustrated in the two tables that compared to the previous secret-sharing-based sealed-bid e-auction schemes, the new scheme does not compromise efficiency while achieving much better properties. It is even more efficient than [10].

[2] A honest bidder can successfully settle a dispute as it is impossible to encrypt two different messages into the same ciphertext in Paillier encryption.

Table 3. Efficiency comparison

Auction schemes	bidder	auctioneer
[3]	3	$2n+1$
[4,6]	$2mw+1$	$1+2n+2\log_2 w$
[10]	$(2T+2+4m)w+1$	$1+6n+6\log_2 w$
New auction	$(T+3+2m)w+1$	$1+5n+5\log_2 w$

6 Conclusion

A new secret-sharing-based first-bid e-auction scheme is proposed. It can achieve all the desired properties for sealed-bid auctions at a reasonable cost. Moreover, attacks existing in the current secret-sharing-based sealed-bid e-auction schemes are prevented in the new scheme.

References

1. Feng Bao. An efficient verifiable encryption scheme for encryption of discrete logarithms. In *the Smart Card Research Conference, CARDIS'98*, volume 1820 of *Lecture Notes in Computer Science*, pages 213–220, Berlin, 1998. Springer-Verlag.
2. D. Chaum and T. P. Pedersen. Wallet databases with observers. In *CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105, Berlin, 1992. Springer-Verlag.
3. Matthew K Franklin and Michael K Reiter. The design and implementation of a secure auction service. In *IEEE Transactions on Software Enginerring*, volume 5, pages 302–312, May 1996.
4. H Kikuchi, Michael Harkavy, and J D Tygar. Multi-round anonymous auction. In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62–69, June 1998.
5. Hiroaki Kikuchi. (m+1)st-price auction. In *The Fifth International Conference on Financial Cryptography 2001*, volume 2339 of *Lecture Notes in Computer Science*, pages 291–298, Berlin, 2001. Springer-Verlag.
6. Hiroaki Kikuchi, Shinji Hotta, Kensuke Abe, and Shohachiro Nakanishi. Distributed auction servers resolving winner and winning bid without revealing privacy of bids. In *proc. of International Workshop on Next Generation Internet (NGITA2000), IEEE*, pages 307–312, July 2000.
7. P Paillier. Public key cryptosystem based on composite degree residuosity classes. In *EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238, Berlin, 1999. Springer-Verlag.
8. Torben P. Pedersen. Distributed provers with applications to undeniable signatures. In *EUROCRYPT '91*, pages 221–242, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science 547.
9. Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *EUROCRYPT '91*, pages 129–140, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science 547.

10. Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan. Robust, privacy protecting and publicly verifiable sealed-bid auction. In *4th International Conference of Information and Communications Security, ICICS 2002*, volume 2513 of *Lecture Notes in Computer Science*, pages 147 – 159, Berlin, 2002. Springer.
11. C Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology, 4, 1991*, pages 161–174, 1991.
12. Adi Shamir. How to share a secret. *Communication of the ACM*, 22(11):612–613, Nov 1979.