Efficiency Improvement of Homomorphic E-Auction

Kun Peng and Feng Bao

Institute for Infocomm Research
dr.kun.peng@gmail.com

Abstract. A design is proposed in this paper to apply a special membership proof technique and a range test technique to homomorphic e-auction. It answers three open questions. On one hand, the special membership proof technique has some limitations such that so far few appropriate applications have been found for it. Moreover, although only needing a constant cost and achieving very high efficiency the range test technique is so new that no appropriate application has been proposed for it. On the other hand, so far no efficient and secure solution has been found for homomorphic e-auction, especially in bid validity check and range test of sum of bids. In this paper, the special membership proof technique and the range test technique are applied to homomorphic e-auction such that all of them benefit from our new design. On one hand, the membership proof technique and the range test technique find an appropriate application and become practical technologies. On the other hand, homomorphic e-auction overcomes its bottlenecks in efficiency and achieves great improvement in performance.

1 Introduction

In a sealed-bid auction scheme, each bidder chooses his evaluation from a number of biddable prices and submits it to some auctioneers, who then open the bids and determine the winning price and winner(s) according to a pre-defined auction rule. The commonly applied auction rules include first bid auction (the bidder with the highest bid wins and pays the highest bid), Vickrey auction (the bidder with the highest bid wins and pays the second highest bid) and the κ^{th} bid auction (the bidders with the κ highest bids win, pay the κ^{th} or the $\kappa + 1^{th}$ highest bid and each gets an identical item). The first-bid auction and Vickrey auction can be regarded as special cases of the κ^{th} bid auction, which is a general solution. An auction must be correct, namely the auction result is strictly determined according to the auction rule. Fairness is necessary in any auction such that no bidder can take advantage over other bidders. A general e-auction scheme should be flexible enough to support various auction rules. Usually, bid privacy must be kept in an auction scheme, which means in the course of bid opening no information about any losing bid is revealed.

When bid privacy must be kept in a non-interactive auction, an efficient bid opening function is homomorphic bid opening [13,15,8,14,1,5,16,17]. To adopt

S. Katsikas, J. Lopez, and M. Soriano (Eds.): TrustBus 2010, LNCS 6264, pp. 238–249, 2010.

this bid opening function, one-selection-per-price principle and homomorphic bid sealing must be employed. Each bidder has to submit a bidding selection at every biddable price to indicate whether he is willing to pay that price (e.g. 1 for "YES" or 0 for "NO"). Every selection is sealed with an additive homomorphic secret sharing or encryption algorithm (as will be explained in details in Section 2.3), so that the auctioneers can test at a price whether the sum of the bidding selections (and thus the number of bidders willing to pay the price) is smaller than κ without revealing any bidding selection. With this homomorphic bid opening mechanism, the winning bid can be determined without opening the separate bidding selections.

In homomorphic e-auction, each bidding selection must be in some special format (the certain values standing for "YES" or "NO") to guarantee correctness and fairness of the auction. So validity of the bids must be proved by the bidders and then publicly verified. However, proof and verification of bid validity is highly inefficient in the existing homomorphic e-auction schemes. Moreover, although binary search for the winning price only tests the sum of bidding selections at a small number of prices, each test is a range test (as will be explained in details in Section 2.2), which is not efficient in the existing homomorphic e-auction schemes when no privacy is compromised. Some methods [18,19,20,23] are proposed to improve efficiency of homomorphic e-auction. The methods in [18,19] strictly limit the auction rule and thus lose generality and flexibility. Short exponents are employed in [20,23] to improve efficiency, but this method has two drawbacks. Firstly, it weakens soundness of e-auction. Secondly, its advantage in efficiency is not very fair as other homomorphic e-auction schemes can improve their efficiency by employing shorter exponents and weakening soundness too. In this paper, we are interested in general and flexible e-auction with the same level of soundness as the existing homomorphic e-auction schemes [13,15,8,14,1,5,16,17]. So these improvements [18,19,20,23] are uncomparable with our new technique.

In this paper, an efficient homomorphic e-auction scheme is proposed. Its main idea is inspired by three observations. Firstly, although the membership proof technique in [6] is strictly limited in application area, it can efficiently implement bid validity proof in homomorphic e-auction. Secondly, although the range test technique in [21,22,24,25] has no other practical application but an inefficient e-auction design in [25], it is efficient and applicable to range test of sum of bidding selections in homomorphic e-auction. Thirdly, after these two techniques are employed in homomorphic e-auction, most exponentiations in computation are combined into some products of multiple powers, which are more efficient than the same number of separate exponentiations according to [3,2]. The new e-auction scheme employs these three optimisations and greatly improves efficiency of homomorphic e-auction.

2 Background

Application background and necessary preliminary knowledge are recalled and commented in this section.

2.1 The Membership Proof by Camenisch *et al* [6]

Camenisch *et al.* [6] propose a range proof scheme, which proves that a secret committed integer is in an interval range. A membership proof protocol is designed in [6] as a building block of the range proof scheme. In membership proof, a prover commits to a secret message s, publishes the commitment and then proves that s is in a finite set $S = \{s_1, s_2, \ldots, s_n\}$ without revealing it. The membership proof protocol in [6] employs a simple idea: the digital signature algorithm in [4] is employed and a verifier signs every message in S using his own private key and sends all the signatures to the prover, who then proves that he knows the signature on the message in the commitment.

In [6], an appropriate application is proposed for the range proof scheme, but no practical application is mentioned for the underlying membership proof protocol except for employing it as a building block in the range proof scheme, as it has the following limitations and concerns in application. Firstly, it is not universally verifiable. Secondly, it is compulsorily interactive. Thirdly, although the computational cost of a prover becomes constant (independent of n) and low, communicational cost and the computational cost on the verifier's side are both $O(n)$ and thus costly. So Camenisch *et al* do not recommend their membership proof technique as a general solution to membership proof due to the following reasons. Therefore, in most applications, the naive membership proof through zero knowledge proof of partial knowledge [9] must be employed, which proves that the committed message may be each message in the set one by one and then link the multiple proofs with OR logic. It is the only general membership proof technique although there are some other special membership proof techniques for very special environments like [7], which strictly limits the set S. However, the naive membership proof is too costly as it costs the prover and a verifier each $O(n)$ exponentiations and transfers $O(n)$ integers.

2.2 The Range Test by Peng et al [21,22,24,25]

Range test is a cryptographic operation to test whether a secret message is in an interval range without revealing any other information about it. Peng *et al* [24] propose an efficient range test protocol, which enables two parties to cooperate to test whether a secret integer is in an interval range or not. It only needs a constant cost independent of the size of the range, so is very efficient. Especially, when the range size is not very small, its advantage in efficiency is great over the previous range test schemes. However, its application to publicly verifiable multiparty computation systems like e-auction is limited. Peng and Bao [25] optimise applicability of the range test protocol in [24] and propose a practical way to employ it in e-auction with multiple auctioneers. However, the way to apply range test to e-auction in [25] is not based on homomorphic bid sealing and bid opening and thus is quite inefficient although its multiparty model is a useful improvement.

2.3 Homomorphic E-Auction

In homomorphic e-auction [13,15,8,14,1,5,16,17], Each bidder has to submit a bidding selection at every biddable price to indicate whether he is willing to pay the price. Every selection is sealed with a homomorphic bid-sealing function, so that the auctioneers can recover the sum of the selections of all the bidders at any price to detect whether enough bidders are willing to pay the price without revealing any bidding selection or their distribution. Correctness of homomorphic bid opening depends on validity of the bids. An invalid bid can compromise correctness of a homomorphic e-auction scheme, so must be detected and deleted before the bid opening phase. Homomorphic bid-sealing can employ secret sharing or additive homomorphic encryption, while the unsealing power is shared among the auctioneers. An encryption algorithm with decryption function $D()$ is additive homomorphic if $D(c_1) + D(c_2) = D(c_1 c_2)$ for any ciphertexts c_1 and c_2. A typical additive homomorphic encryption algorithm with a distributed decryption function is Paillier encryption with distributed decryption proposed by Fouque *et al* [10], which employs a multiplicative modulus N^2 and encryption algorithm $E(s) = g^s r^N$ where $N = pq$ and p, q are large secret primes. The decryption function is denoted as $D()$. With this encryption algorithm to seal the bids, homomorphic e-auction can be abstracted into the following protocol.

1. Suppose there are n bidders $V_1, V_2, \ldots, V_n$ and w biddable prices $p_1, p_2, \ldots, p_w$. It is required that $w < n$ and $n < N$, which is easily satisfied in any practical auction application.
2. Each bidder V_i chooses his bid p_ρ and generates his bidding vector $(s_{i,1}, s_{i,2}, \ldots, s_{i,w})$ where $s_{i,l} = 1$ for $l = \rho$ and $s_{i,l} = 0$ otherwise.
3. Paillier encryption with distributed decryption is employed to encrypt the bids where the private key is shared among the auctioneers $A_1, A_2, \ldots, A_m$. Each bidding vector $(s_{i,1}, s_{i,2}, \ldots, s_{i,w})$ is encrypted into $(c_{i,1}, c_{i,2}, \ldots, c_{i,w})$ where $c_{i,l} = g^{s_{i,l}} r_{i,l}^N$ and $r_{i,l}$ is randomly chosen from Z_N^* for $l = 1, 2, \ldots, w$.
4. Each V_i illustrates validity of his bid through proof of

$$KN\ [\ c_{i,l}^{1/N}\ ]\ \vee\ KN\ [\ (c_{i,l}/g)^{1/N}\ ] \text{ for } l = 1, 2, \ldots, w \quad (1)$$

and

$$KN\ [\ ((\prod_{l=1}^{w} c_{i,l})/g)^{1/N}\ ] \quad (2)$$

where $KN(X)$ denotes knowledge of X, (1) is proved by running the proof protocol in Figure 1 for $l = 1, 2, \ldots, w$ and (2) is a proof of knowledge of N^{th} root [12].

5. The sealed bids are adjusted: $c'_{i,l} = \prod_{j=l}^{w} c_{i,j}$ for $i = 1, 2, \ldots, n$ and $l = 1, 2, \ldots, w$. The final sealing result $c'_{i,l}$ contains 1 iff V_i is willing to pay p_l.
6. The auctioneers cooperate to search for the winning bids. Usually there are two searching strategies: downward search and binary search. The former starts from the highest biddable price and goes downwards, testing whether there are enough bidding selections of "1" at each price on its route until they are found at a price, which becomes the winning price. The latter follows the binary searching route among all the biddable prices, doing the same test at

each price on its route until just enough bidding selections of "1" are met at the winning price. No matter which search strategy is employed, at each price on the searching route, p_l, the auctioneers cooperate to compare $D(\prod_{i=1}^{n} c'_{i,l})$ and κ where κ is the number of items on sale and thus the number of winners. This comparison is usually implemented through a range test and its detailed implementation are different in the existing homomorphic e-auction schemes. Due to space limit, the details are not recalled here and interested readers are referred to the homomorphic e-auction papers. Note that some existing homomorphic e-auction schemes ignore the possibility $\kappa > 1$ and few of them completely maintain privacy in the range test. A detailed and completely private test will be designed in our new homomorphic e-auction scheme in Section 3. Both searching strategies can find the winning price.

- In a downward search, if $D(\prod_{i=1}^{n} c'_{i,l}) = \kappa$ is met p_l is the winning price; otherwise the search goes to the next lower price.
- In a binary search, if $D(\prod_{i=1}^{n} c'_{i,l}) < \kappa$ the search goes to the lower price; otherwise the search goes to the higher price.

The search goes on until it stops at the winning price.

7. The bidding selections at the winning price are decrypted to identify the winners. Note that the number of winners may be larger than κ and a tie may occur. Most existing homomorphic e-auction schemes do not provide detailed solution to a tie. A detailed winner identification mechanism able to handle a tie will be designed in our new homomorphic e-auction scheme in Section 3.

There are two efficiency bottlenecks in the existing homomorphic e-auction schemes. Firstly, bid validity check is too inefficient: repeating the proof and

1. V_i publishes
$$a_{s_{i,l}} = r^N$$
$$a_{1-s_{i,l}} = u_{1-s_{i,l}}^N / (c_{i,l}/g^{1-s_{i,l}})^{\lambda_{1-s_{i,l}}}$$
where $r \in Z_N^*$, $\lambda_{1-s_{i,l}} \in Z_N$, and $u_{1-s_{i,l}} \in Z_N^*$ are randomly chosen.
2. A verifier or a (pseudo)random function publicly generates a random integer λ in Z_N.
3. V_i publishes u_0, u_1, λ_0 and λ_1 where
$$u_{s_{i,l}} = r s_{i,l}^{\lambda_{s_{i,l}}}$$
$$\lambda_{s_{i,l}} = \lambda - \lambda_{1-s_{i,l}} \bmod Z_N$$
Public verification:
$$u_0^N = a_0 c_{i,l}^{\lambda_0}$$
$$u_1^N = a_1 (c_{i,l}/g)^{\lambda_1}$$
$$\lambda = \lambda_0 + \lambda_1 \bmod Z_N$$

Fig. 1. Repeated w times to implement proof and verification of (1)

verification protocol in Figure 1 to prove and verify (1) brings each bidder much higher a cost than bid encryption and a verifier at least $O(wn)$ exponentiations. Secondly, although binary search only goes through $\log_2 w$ prices, at each price on its route a range test in a range with a size κ is needed. So the search for the winning price is still not efficient enough, especially when privacy must be maintained or κ is large.

3 Efficient Homomorphic E-Auction

Several special characters of public proof and verification of bid validity in homomorphic e-auction are noticed as follows.

- In bid validity check in homomorphic e-auction, verifiers can be classified into two types: auctioneers and independent observers. The auctioneers are key players in e-auction and have contradictory interest against the bidders. They want to reach a dealing price as high as possible, while each bidder wants to beat the other bidders at a price as low as possible. So the auctioneers are keen to verify validity of the bids. The other verifiers are not involved in the auction application and are only independent observers, who have no interest in the e-auction. So usually they assume that the auctioneers (or at least some of them) try their best to challenge the bidders and they only act as witnesses, who do not input anything and only passively verify whether the bidders' responses match the auctioneers' challenges. Therefore, the auctioneers act as a main verifier and the other verifiers are their witnesses.
- In e-auction, usually only the bidders want to be non-interactive in bid validity check. On the other hand, the auctioneers as managers of the e-auction system should be able to interactively publish their initial challenges (in the form of signatures on the biddable prices). Actually they do not need to interact with each bidder. Instead they only need a bulletin board to publish the initial challenges.
- In e-auction, usually the auctioneers have powerful servers and high-speed communication channels, while the bidders may have low computing capability or low communication bandwidth. Moreover, there are many bidders, each of which must prove validity of his bid. So bid validity check (based on membership proof) must be repeated many times where the biddable prices are the same and the auctioneers are always the main verifier no matter which bidder is the prover. The other verifiers are only independent witnesses.

As these characters meet the application conditions of the special membership proof technique in [6], it can be employed in bid validity check in homomorphic e-auction. In our design, each bidder's bidding selections are combined into an integer, which is then proved to be in a set using the membership proof technique in [6]. The combination operation calculates a product of w powers, whose computation is more efficient than w separate exponentiations according to [3,2]. For high efficiency, binary search is adopted in the bid opening phase. The efficient

range test technique in [21,22,24,25] is employed in the range test of the sum of bidding selections at the prices on the binary searching route. Therefore, the efficiency bottlenecks in homomorphic e-auction can be overcome. The homomorphic e-auction protocol with such improvements is as follows where κ same items are on sale.

1. Initial setting
   (a) Paillier encryption with distributed decryption is set up and the private key is shared among the auctioneers $A_1, A_2, \ldots, A_m$ where the parameters are the same as in Section 2.3, the message space is Z_N and the multiplicative modulus is N^2.
   (b) It is required that $n < N$, which is always satisfied with any practical n and secure N.
   (c) The digital signature algorithm in [4] is set up for the auctioneers.
   (d) A bulletin board is set up for the auctioneers and bidders to publish information.
2. Bidding phase (including bid validity check)
   (a) Each bidder V_i chooses his bid p_ρ and generates his bidding vector $(s_{i,1}, s_{i,2}, \ldots, s_{i,w})$ where $s_{i,l} = 1$ for $l = \rho$ and $s_{i,l} = 0$ otherwise. Each bidding vector $(s_{i,1}, s_{i,2}, \ldots, s_{i,w})$ is encrypted into $(c_{i,1}, c_{i,2}, \ldots, c_{i,w})$ where $c_{i,l} = g^{s_{i,l}} r_{i,l}^N$ and $r_{i,l}$ is randomly chosen from Z_N^* for $l = 1, 2, \ldots, w$.
   (b) The auctioneers cooperate to generate a set $S = \{S_1, S_2, \ldots, S_w\}$, where each S_i is a random integer in Z_N corporately chosen by all the auctioneers. S is published on the bulletin board.
   (c) The auctioneers cooperate to sign all the integers in S one by one using the digital signature algorithm in [4]. They publish the signatures $\gamma_1, \gamma_2, \ldots, \gamma_w$ on the bulletin board such that anyone can verify validity of the signatures.
   (d) The auctioneers calculate $C_i = \prod_{l=1}^{w} c_{i,l}^{S_l}$ for $i = 1, 2, \ldots, n$ and each bidder V_i proves that he knows the signature on the message in C_i by the auctioneers using the proof protocol in Figure 2 where $e()$ stands for bilinear mapping and more details can be found in [6].
3. Bid opening phase
   (a) The sealed bids are adjusted: $c'_{i,l} = \prod_{j=l}^{w} c_{i,j}$ for $i = 1, 2, \ldots, n$ and $l = 1, 2, \ldots, w-1$ such that $c'_{i,l}$ contains 1 iff V_i is willing to pay p_l.
   (b) The auctioneers cooperate to search for the winning bid. To achieve high efficiency, binary search is employed. At each price on the searching route, p_l, the auctioneers cooperate to test whether $D(\prod_{i=1}^{n} c'_{i,l}) < \kappa$ as detailed in Figure 3. If $D(\prod_{i=1}^{n} c'_{i,l}) < \kappa$ the search goes to the lower prices; otherwise the search goes to the higher prices. The search goes along the binary searching route until it stops at the winning price.
4. Winner identification phase
   Suppose the binary search stops at price p_K. The auctioneers cooperate to decrypt all the bidding selections at p_K.

- If the number of selections of "1" at p_K is κ, no tie occurs. The bidders with selection "1" at p_K are the winners.
- If the number of selections of "1" at p_K is smaller than κ, the auctioneers cooperate to decrypt all the bidding selections at p_{K+1}. Suppose the number of selections of "1" at p_K is δ. The bidders with selection "1" at p_K and the first $\kappa - \delta$ bidders with selection "1" at p_{K+1} are the winners.
- If the number of selections of "1" at p_K is larger than κ the first κ bidders with selection "1" at p_K are the winners.

Suppose $C_i = g^{\alpha}\beta^N$ and $\alpha = S_\sigma$. Bidder V_i proves that α is in S as follows where $\gamma_l = g^{1/(x+S_l)}$.

1. V_i randomly picks ν in Z_N and publishes $\mu = \gamma_\sigma^\nu$. He proves that he knows $\alpha, \nu, S_\sigma, \beta$ such that $C_i = g^{\alpha}\beta^N$ and $\mu = g^{\nu/(x+S_\sigma)}$ as detailed in [6].
2. V_i randomly picks ϵ, τ, ω in Z_N and publishes $a = e(\mu, g)^{-\epsilon} e(g, g)^{\tau}$ and $d = g^{\epsilon}\omega^N$.
3. $c = H(\mu, C_i, a, d)$ where H is a hash function to generate (pseudo)random challenges.
4. V_i publishes $z_1 = \epsilon - cS_\sigma$, $z_2 = \tau - c\nu$ and $z_3 = \omega/\beta^c$.

Public verification:

$$d = C_i^c z_3^N g^{z_1}$$
$$a = e(\mu, y)^c e(\mu, g)^{z_1} e(g, g)^{z_2}$$

Fig. 2. Membership Proof to implement bid validity check

4 Analysis and Comparison

Security of the new homomorphic e-auction scheme is illustrated in the following.

- The new homomorphic e-auction scheme employs the same main strategy as the existing homomorphic e-auction schemes: bid sealing through additive homomorphic encryption, homomorphic bid opening, binary search for the winning bid and test of the sum of the bidding selections at each searched price. As security of such a homomorphism-exploiting strategy has been formally proved in the existing homomorphic e-auction schemes, applying it to the new homomorphic e-auction scheme is secure as well.
- The new bid validity check mechanism in the new homomorphic e-auction scheme is based on the membership proof technique by Camenisch *et al* [6] and a new combination mechanism to combine the bidding selections of a bidder into an integer in the set of the membership proof. The already-formally-proved security of the membership proof technique [6] and Theorem 1 guarantee that bid validity check in the new homomorphic e-auction scheme is secure.

1. $C'_l = \prod_{i=1}^{n} c'_{i,l}$.
2. – If κ is small (e.g. ≤ 3), the auctioneers runs the basic test as follows.
   (a) The auctioneers calculate
   $$B_k = C'_l / g^{k-1} \text{ for } k = 1, 2, \ldots, \kappa.$$
   (b) All of them take turns to shuffle $B_1, B_2, \ldots, B_\kappa$ using a shuffling protocol (e.g. [11]), which re-encrypts and re-orders the input ciphertexts. The output of the last shuffling is $B'_1, B'_2, \ldots, B'_\kappa$.
   (c) The auctioneers test whether a zero is encrypted in $B'_1, B'_2, \ldots, B'_\kappa$ as follows.
      i. $k = 1$
      ii. For $j = 1, 2, \ldots, m$, each A_j randomly selects a non-zero integer t_j in Z_N and calculates $B'_{k,j} = {B'}^{t_j}_{k,j-1}$ where $B'_{k,0} = B'_k$. Each A_j publicly proves validity of his operation by proving knowledge of $\log_{B'_{k,j-1}} B'_{k,j}$ using zero knowledge proof of knowledge of discrete logarithm [26].
      iii. The auctioneers cooperate to decrypt $B'_{k,m}$. If the decryption result is zero, return $TURE$ and jump out of the loop.
      iv. If $k = \kappa$, return $FALSE$ and jump out of the loop; otherwise $k \leftarrow k + 1$ and goto Step 2(c)i to continue the loop.

   If $TURE$ is returned, a zero is encrypted in $B'_1, B'_2, \ldots, B'_\kappa$.
   If a zero is encrypted in $B'_1, B'_2, \ldots, B'_\kappa$, the basic test shows that $D(\prod_{i=1}^{n} c'_{i,l}) < \kappa$.
   – If κ is not small and the cost is high with the basic test, the range test technique (called advanced test in this paper) in [21,22,24,25] is employed to test whether $D(\prod_{i=1}^{n} c'_{i,l})$ is in $\{0, 1, \ldots, \kappa - 1\}$ more efficiently. The detailed implementation can be found in [21,22,24,25].

Fig. 3. Range test of the sum of the bidding selections at a price p_l

– The basic test of sum of bidding selections is straightforward and its security is obvious. The advanced test of sum of bidding selections in the new homomorphic e-auction scheme is based on the range test technique by Peng *et al* [21,22,24,25], whose security has been formally proved. So range test of sum of bidding selections in the new homomorphic e-auction scheme is secure.

Theorem 1. *If the bidding vector in* $(c_{i,1}, c_{i,2}, \ldots, c_{i,w})$ *is invalid, the probability that the message encrypted in* C_i *lies in* S *is negligible.*

Proof: As $(c_{i,1}, c_{i,2}, \ldots, c_{i,w})$ is invalid, there are the following two possibilities where $(s_{i,1}, s_{i,2}, \ldots, s_{i,w})$ is the bidding vector encrypted into $(c_{i,1}, c_{i,2}, \ldots, c_{i,w})$.

– There is only one non-zero integer in $s_{i,1}, s_{i,2}, \ldots, s_{i,w}$.
– There are more than one non-zero integers in $s_{i,1}, s_{i,2}, \ldots, s_{i,w}$.

In the first case, suppose $s_{i,L} \neq 0$. As $(c_{i,1}, c_{i,2}, \ldots, c_{i,w})$ is invalid, $s_{i,L} \neq 1 \bmod N$. So

$$D(C_i) = D(\prod_{l=1}^{w} c_{i,l}^{S_l}) = \sum_{l=1}^{w} s_{i,l} S_l = s_{i,L} S_L \neq S_L \bmod N$$

and the probability that

$$D(C_i) = D(\prod_{l=1}^{w} c_{i,l}^{S_l}) = \sum_{l=1}^{w} s_{i,l} S_l = s_{i,L} S_L = S_{L'} \bmod N \text{ and } L' \neq L \text{ and } 1 \leq L' \leq w$$

is $(w-1)/N$ as $S_1, S_2, \ldots, S_w$ are randomly chosen in Z_N. Therefore, the probability that

$$D(C_i) = S_{L'} \bmod N \text{ and } 1 \leq L' \leq w$$

is negligible.

In the second case, suppose only $s_{i,T_1}, s_{i,T_2}, \ldots, s_{i,T_\pi}$ are non-zero integers in $s_{i,1}, s_{i,2}, \ldots, s_{i,w}$ where $1 \leq T_1, T_2, \ldots, T_\pi \leq w$ and $\pi > 1$. Then

$$D(C_i) = D(\prod_{l=1}^{w} c_{i,l}^{S_l}) = \sum_{l=1}^{w} s_{i,l} S_l = \sum_{l=1}^{\pi} s_{i,T_l} S_{T_l} \bmod N.$$

So, as $S_1, S_2, \ldots, S_w$ are randomly chosen in Z_N the probability that

$$D(C_i) = S_{L'} \bmod N \text{ and } 1 \leq L' \leq w$$

is w/N and thus negligible.

Therefore, in both cases the probability that the message encrypted in C_i lies in S is negligible. □

Due to space limit no further detail is given to illustrate security of the new homomorphic e-auction scheme. Interested readers can find more details in the references [13,15,8,14,1,5,16,17,6,24,25]. Our analysis focuses on efficiency comparison with the existing homomorphic e-auction schemes. The number of exponentiations needed for a bidder and an auctioneer are estimated in Table 1 to compare efficiency between the new homomorphic e-auction scheme and the existing homomorphic e-auction schemes. Suppose general e-auction application is supported and multiple identical items may be on sale. For simplicity, suppose $\kappa = 6$ and no tie occurs. For fairness of comparison, suppose Paillier encryption with distributed decryption and binary search are employed in all the schemes. Range test of the sum of bidding selections at any price should be completely private, so the basic test in Figure 3 is supposed to be employed in the existing homomorphic e-auction schemes. In the new homomorphic e-auction scheme, the most costly computation is $C_i = \prod_{l=1}^{w} c_{i,l}^{S_l}$ for $i = 1, 2, \ldots, n$, which requires an auctioneer to calculate n products of w powers. In the current security standard, N is 1024 bits long, so according to [2], each such product costs $2^{3-1}w + 1024 + 1024w/(3+1) = 260w + 1024$ multiplications, while an exponentiation with an exponent in Z_N cost $2^{3-1} + 1024 + 1024/(3+1) = 1284$ multiplications. So, cost of the n products of w powers is equivalent to $n(260w+1024)/1284$

exponentiations. It is illustrated in Table 1 that the new homomorphic e-auction scheme is more efficient for both the bidders and the auctioneers. An example is given in the table to more clearly and convincingly show the advantage of the new scheme in efficiency, where $n = 1000$ and $w = 1024$.

Table 1. Efficiency Comparison of Homomorphic E-Auction Schemes

scheme	bidder		auctioneer	
	cost	example	cost	example
secure existing	$6w$	6144	$4nw + 7\kappa \log_2 w + 3n$	4051420
new	$2w + 8$	2056	$\approx 0.2nw + 20 \log_2 w + 16n$	221000

5 Conclusion

The new homomorphic e-auction scheme is an appropriate application of the membership proof technique in [6] and the range test technique in [21,22,24,25]. Its efficiency is much higher than the existing homomorphic e-auction schemes.

References

1. Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n signatures from a variety of keys. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 415–432. Springer, Heidelberg (2002)
2. Avanzi, R., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography, HEHCC (2005)
3. Bellare, M., Garay, J.A., Rabin, T.: Fast batch verification for modular exponentiation and digital signatures. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 236–250. Springer, Heidelberg (1998)
4. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)
5. Brandt, F.: Cryptographic protocols for secure second-price auctions (2001), `http://www.brauer.in.tum.de/~brandtf/papers/cia2001.pdf`
6. Camenisch, J.L., Chaabouni, R., Shelat, A.: Efficient protocols for set membership and range proofs. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 234–252. Springer, Heidelberg (2008)
7. Camenisch, J., Lysyanskaya, A.: Dynamic accumulators and application to efficient revocation of anonymous credentials. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 61–76. Springer, Heidelberg (2002)
8. Chida, K., Kobayashi, K., Morita, H.: Efficient sealed-bid auctions for massive numbers of bidders with lump comparison. In: Davida, G.I., Frankel, Y. (eds.) ISC 2001. LNCS, vol. 2200, pp. 408–419. Springer, Heidelberg (2001)
9. Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of partial knowledge and simplified design of witness hiding protocols. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 174–187. Springer, Heidelberg (1994)

10. Fouque, P., Poupard, G., Stern, J.: Sharing decryption in the context of voting or lotteries. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 90–104. Springer, Heidelberg (2001)
11. Groth, J., Lu, S.: Verifiable shuffle of large size ciphertexts. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 377–392. Springer, Heidelberg (2007)
12. Guillou, L., Quisquater, J.: A "paradoxical" identity-based signature scheme resulting from zero-knowledge. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 216–231. Springer, Heidelberg (1990)
13. Kikuchi, H., Harkavy, M., Tygar, J.: Multi-round anonymous auction. In: IEEE Workshop on Dependable and Real-Time E-Commerce Systems '98, pp. 62–69 (1998)
14. Kikuchi, H. (m+1)st-price auction. In: Syverson, P.F. (ed.) FC 2001. LNCS, vol. 2339, pp. 291–298. Springer, Heidelberg (2002)
15. Kikuchi, H., Hotta, S., Abe, K., Nakanishi, S.: Distributed auction servers resolving winner and winning bid without revealing privacy of bids. In: NGITA '00, pp. 307–312 (2000)
16. Omote, K., Miyaji, A.: A second-price sealed-bid auction with the discriminant of the p-th root. In: Blaze, M. (ed.) FC 2002. LNCS, vol. 2357, pp. 57–71. Springer, Heidelberg (2003)
17. Peng, K., Boyd, C., Dawson, E., Viswanathan, K.: Robust, privacy protecting and publicly verifiable sealed-bid auction. In: Deng, R.H., Qing, S., Bao, F., Zhou, J. (eds.) ICICS 2002. LNCS, vol. 2513, pp. 147–159. Springer, Heidelberg (2002)
18. Peng, K., Boyd, C., Dawson, E.: A multiplicative homomorphic sealed-bid auction based on Goldwasser-Micali encryption. In: Zhou, J., López, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 374–388. Springer, Heidelberg (2005)
19. Peng, K., Boyd, C., Dawson, E.: Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS, vol. 3715, pp. 84–98. Springer, Heidelberg (2005)
20. Peng, K., Boyd, C., Dawson, E.: Batch verification of validity of bids in homomorphic e-auction. Computer Communications 29, 2798–2805 (2006)
21. Peng, K., Boyd, C., Dawson, E., Okamoto, E.: A novel range test. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058, pp. 247–258. Springer, Heidelberg (2006)
22. Peng, K., Dawson, E.: Range test secure in the active adversary model. In: ACM International Conference Proceeding Series, AISW2007, vol. 249, pp. 159–162 (2007)
23. Peng, K., Dawson, E.: Efficient bid validity check in elGamal-based sealed-bid E-auction. In: Dawson, E., Wong, D.S. (eds.) ISPEC 2007. LNCS, vol. 4464, pp. 209–224. Springer, Heidelberg (2007)
24. Peng, K., Bao, F., Dawson, E.: Correct, private, flexible and efficient range test. Journal of Researchand Practice in Information Technology 40(4), 275–291 (2008)
25. Peng, K., Bao, F.: Practicalization of a range test and its application to e-auction. In: EuroPKI '09 (2009)
26. Schnorr, C.: Efficient signature generation by smart cards. Journal of Cryptology 4, 161–174 (1991)