Sealed-Bid Micro Auctions

Kun Peng, Colin Boyd, and Ed Dawson

Information Security Institute
Queensland University of Technology, Australia
{k.peng, c.boyd, e.dawson}@qut.edu.au

Abstract. In electronic auction applications, small-value merchandise is often distributed. We call this kind of auction micro auction. Compared to traditional general-purpose electronic auction, micro electronic auction has its own special requirements. Especially, micro auction must be very efficient: the cost of the auction protocol must not be over the cost of the merchandise for sale. Although the merchandise to distribute are of small value in micro auctions, bid privacy is still needed in many circumstances. So sealed-bid auction mechanism has to be employed in micro auction. Therefore, a question is raised: how to balance between the high efficiency requirement of micro auction and the high cost needed to keep bid privacy. In this paper, the traditional sealed-bid e-auction techniques are modified to satisfy the special requirements of sealed-bid micro auction. Two existing general-purpose electronic sealed-bid auction schemes are modified into micro sealed-bid auction schemes. The new schemes are secure and suitable for micro auction. One of them is further improved in efficiency to meet more critical requirements in certain micro auction applications.

1 Introduction

Auctions have a long history as an effective method to distribute goods fairly. In recent years, electronic auctions on the Internet are becoming more and more popular. Due to security concerns for the network environment and payment method (often through the Internet too), electronic auction is more often used to distribute small-value merchandise. We call auction of small-value merchandise micro auction, which needs studying in the electronic form (through computer network). In any kind of auction, a basic principle should be followed: the cost of the auction protocol must not be over the value of the merchandise to distribute. So high efficiency is a key requirement for micro auction.

In this paper, after detailed analysis sealed-bid auction is chosen as an appropriate mechanism to implement micro auction. Unfortunately, all the existing sealed-bid auction schemes with bid privacy are only suitable for large-value merchandise. Although they are more efficient than double auction, they are still too inefficient for micro auction. They need a large number of exponentiations in computation, whose cost may be over the value of merchandise in micro auctions. So special sealed-bid auction schemes suitable for micro auction must be designed. To our knowledge there is no research work focused on sealed-bid micro auctions. In this paper, security and efficiency of sealed-bid micro auction are discussed and sealed-bid micro auction schemes with satisfactory security properties are designed.

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

A simple and practical solution to efficient secure micro sealed-bid e-auction is to modify and optimize appropriate existing secure general-purpose sealed-bid e-auction into micro auction schemes. Among the two common methods to design secure sealed-bid e-auction, secure evaluation and one-choice-per-price strategy, one-choice-per-price strategy is more suitable for micro auction as it can more easily achieve high efficiency in micro auction. In this paper two secure micro sealed-bid e-auction schemes are designed based on existing sealed-bid auction schemes employing one-choice-per-price strategy. Both schemes can satisfy the security requirements for micro auction and are efficient, thus are suitable for auction of small-value merchandise. The second scheme is especially efficient as it is improved in efficiency by using the idea of batch proof. Batch proof in this paper employs an idea similar to efficiency improvement measures in some micro payment systems [1]. It aggregately proves validity of a few random subsets of bid opening operations to publicly prove validity of bid opening with a large probability. After the improvement, only a small constant number of exponentiations are needed in the second scheme. Although the improvement sacrifices instant verifiability and cannot detect invalid operation by the auctioneers until a final verification, the sacrifice is tolerable in micro auctions.

2 Requirements

As stated in Section 1, high efficiency is a very important requirement for micro auction. The most efficient auction in computation is open cry auction. In the open cry auctions, the bids are cried out openly and the auction result is publicly decided. As no bid is sealed, it is very efficient in computation. However, open cry auction cannot satisfy many micro auction applications as it is inefficient in communication and reveals all the bids. The open cry mechanism requires each bidder to remain on-line and repeatedly communicate with the auctioneer to update their bids. Very few bidders are willing to pay such a communicational cost for low-value merchandise. There are many reasons to keep bids secret. For example, a bidder may not want to permit other bidders to choose their bids according to his bid; the bidders may not want to permit the seller (or auctioneer) to design selling strategy in the future according to their bids; a bidder may want to keep his bid secret for personal privacy. All these reasons are independent of the value of the merchandise to sell. So like in auctions with large-value merchandise, confidentiality (or privacy) of bids are often required in micro auctions. An auction mechanism to achieve efficient communication and conceal the bids is double auction, which supports multiple sellers and bidders and a deal is made once a bid is no lower than a seller's offer. Double auction supports real-time deal, which may be preferred in micro auction. However, double auction is too inefficient in computation for micro auction.

Sealed-bid auction seems to be a good auction mechanism for micro auction, especially when high efficiency (both in computation and communication) and bid privacy are required. In a sealed-bid auction, a bidder has to submit a sealed bid before a closing time. After the closing time one or more auctioneers open the bids to decide the winners according to a pre-defined rule. Sealed-bid auction is more efficient than double auction while many existing sealed-bid auction schemes conceal the bids. Most security

requirements in existing sealed-bid e-auction [3, 4] are also desired in micro auction. They are as follows.

1. Correctness: the auction result must be determined exactly according to the auction rule.
2. Public Verifiability: correctness of the auction must be publicly verifiable.
3. Fairness: no bidder can get more information than other bidders at each stage of the auction.
4. Bid confidentiality: each bid must remain confidential to other bidders and the auctioneer(s) before the bid opening phase starts.
5. Non-repudiation: no bidder can deny his bid.
6. Robustness: the auction can still work properly in abnormal situations
7. Rule Flexibility: various auction rules must be supported.
8. Bid Privacy: the losing bids are kept secret even after the auction.

As the cost of an auction protocol must not be over the value of the merchandise on sale, high efficiency is very important to micro auction. Implementation of any security property must be efficient. When necessary, appropriate trade-off must be made between security and efficiency. For example, correctness and public verifiability of micro auction may be achieved only with a large probability instead of absolutely, so that high efficiency is not compromised. On the condition that any incorrect operation can be publicly detected with a large probability, it is reasonable to assume that nobody will risk his reputation and qualification for a small-value merchandise. This idea has been used in some micro payment systems [1], where only a small subset of operations are verified. As these verified operations are randomly chosen, their validity can guarantee that the whole protocol is correctly carried out with a large probability. This idea of partial verification is also adopted in this paper, with different implementation of course.

As the merchandise to sell in micro auctions are of small value, the number of biddable prices is often not very large in micro auctions. Especially when multiple copies of the merchandise are available (e.g. when they are merchandise in electronic form like music, newspaper and document) and thus tie is not a problem, a small number of biddable prices are enough in micro auctions. So efficient auction mechanisms only dealing with a small number of biddable prices can be employed to achieve high efficiency in many micro auction applications.

3 Bid Privacy and Two Strategies

Bid privacy has a great influence on implementation of sealed-bid auctions including sealed-bid micro auctions. Without bid privacy the other properties can be easily achieved in a sealed-bid auction. Bid privacy actually implies that sealed-bid auction should be an application of secure computation, which evaluates a function with encrypted inputs without revealing the inputs. As secure computation is usually complex, sealed-bid auction is more difficult to design when bid privacy is required. However, bid privacy is necessary in many sealed-bid auction applications including micro auction. No matter whether the merchandise to sell is of small value or not, the following two reasons support the need of bid privacy.

1. Bidders want their bidding behaviours to be untraceable. Especially a bidder does not want other people to know that he submits a certain bid in a certain auction, which is a violation of his personal privacy and may violate his benefit in a later auction.
2. Sellers should be prevented from knowing the bids or their distribution. Otherwise they may gain some advantage when selling an identical or similar merchandise in the future.

Currently, there are two methods to implement bid privacy: secure evaluation and one-choice-per-price strategy. Secure evaluation is also called multiparty computation, which employs an evaluation circuit composed of a few logic gates to evaluate the encrypted bids and output the auction result. All of the auction schemes in this category seal the bid bit-by-bit and employ an evaluation circuit composed of a large number of logic gates to evaluate the sealed bids. A drawback of secure computation is low efficiency.

One-choice-per-price strategy is also frequently applied in sealed-bid auctions [6, 5, 3, 4] to achieve bid privacy. Under this strategy, each bidder must make a choice (indicating willingness or unwillingness to pay) at every biddable price while all his choices form his bidding vector. If a bidder is willing to pay a price, he chooses an integer standing for "YES" as his choice at that price. If a bidder is unwilling to pay a price, he chooses an integer standing for "NO" as his choice at that price. Two common bid opening functions in one-choice-per-price auction are downward searching function [5] and binary searching function [6, 3, 4]. Downward searching function unseals the sealed choices price by price downwards from the highest biddable price until a "YES" choice is unsealed at a price. With binary searching function, a much shorter binary route is searched.

4 Micro Sealed-bid Auction

Note that the most important requirement for micro auction is low cost. So one-choice-per-price strategy is chosen to implement micro auction as it is more efficient. Our idea is choosing appropriate existing secure sealed-bid auction schemes and optimize them into secure sealed-bid micro auction schemes. As the first paper about micro auction, this paper only considers first bid auction for simplicity. Namely, the bidder with the highest bid wins and pays the highest bid. Solutions to more complex auction rules are left as a future work. Two such attempts are made in this section. The first one employs binary search while the second employs downward search.

4.1 Protocol 1 — Micro Sealed-bid Auction Employing Binary Search

As pointed out in [3, 4], most existing first-bid sealed-bid auction schemes employing binary search are vulnerable to attacks and cannot guarantee correctness when there is invalid bid. On the other hand, proof and verification of bid validity are too costly (at least $4w$ exponentiations for a bidder and $4nw$ exponentiations for an auctioneer). So although bid opening through binary search is efficient, there was not any efficient

and publicly verifiable sealed-bid auction scheme employing binary search until very recently two new sealed-bid auction scheme employing binary search [3,4] were proposed. These two schemes can publicly guarantee correctness of auction without bid validity check. So these two schemes [3,4] can be used as prototype when sealed-bid micro auction is designed. As [3] is more complex than [4] and has no advantage in efficiency when the number of biddable prices is small, [4] is chosen as a prototype, which is simplified and optimized into a secure sealed-bid micro auction scheme called Protocol 1. The two-round submission in [4] is too complex and costly for a low-cost micro auction. So it is simplified into one round. As a result, unconditional bid confidentiality and fairness in [4] become dependent on a threshold trust on the auctioneers. Bid confidentiality and fairness based on threshold trust should be strong enough for micro auction. Threshold secret sharing in [4] is replaced by simpler and more efficient ElGamal encryption with threshold distributed decryption to seal the bids. 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 $A_1, A_2, \ldots, A_m$. Protocol 1 is as follows.

1. **Preparation phase**
   A bulletin board is set up as a broadcast communication channel. An ElGamal encryption system is set up. Large primes p and q are chosen such that q is a factor of $p-1$. The cyclic group with order q modulo p is denoted as Q. Integer g is a generator Q. Private key x is randomly chosen from Z_q. Public key $y = g^x$ is published. The private key is shared among the auctioneers using threshold secret sharing such that any set of auctioneers can cooperate to perform decryption if and only if the number of cooperating auctioneers is over the sharing threshold. See [2] for more details about ElGamal encryption algorithm with distributed decryption.
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 integer in Q; if he is unwilling to pay p_l, $b_{i,l} = 1$. Then he encrypts and signs his bid vector and publishes the encrypted bid vector $(c_{i,1}, c_{i,2}, \ldots, c_{i,w})$ and signature on it on the bulletin board where $c_{i,j} = (g^{r_{i,j}},\ b_{i,j}y^{r_{i,j}})$ and $r_{i,j}$ is randomly chosen from Z_q.
3. **Bid opening phase**
   The auctioneers cooperate to perform a binary search among the biddable prices. At a price p_l on the searching route, the auctioneers perform as follows.
   (a) Bid randomization and combination
   Each auctioneer A_j publishes a commitment (e.g. one-way hash function) of random integer $R_{j,i,l}$ from Z_q for $i = 1, 2, \ldots, n$. After all the commitments have been published, the auctioneers publish $R_{j,i,l}$ for $i = 1, 2, \ldots, n$ as randomizing factors of $b_{i,l}$. Finally, they compute $R_{i,l} = \sum_{j=1}^{m} R_{j,i,l}$ for $i = 1, 2, \ldots, n$ and $c_l = \prod_{i=1}^{n} c_{i,l}^{R_{i,l}}$.
   (b) Decryption
   The auctioneers cooperate to decrypt c_l and gets the decryption result d_l. If $d_l = 1$, the search goes downwards. If $d_l > 1$, the search goes upwards.
   Finally, the largest l satisfying $d_l > 0$ is found, which is denoted as L. p_L is declared as the winning price.

4. **Winner identification phase**
   All the bid choices at $p_L, c_{1,L}, c_{2,L}, \ldots, c_{n,L}$, are decrypted by the auctioneers into $d_{1,L}, d_{2,L}, \ldots, d_{n,L}$ Any bidder submitting a bid choice larger than 1 at p_L is the winner. The winner's signature is verified and his identity is published.

Theorem 1. *Protocol 1 is correct. More precisely, with an overwhelmingly large probability $d_l > 0$ if and only if there is at least a bid choice indicating the willingness to pay at p_l.*

Proof: Suppose $D()$ is the decryption function of the employed ElGamal encryption. If $b_{1,l}, b_{2,l}, \ldots, b_{n,l}$, all the bid choices at p_l, are 1, $d_l = D(c_l) = D(\prod_{i=1}^{n} c_{i,l}^{R_{i,l}}) = \prod_{i=1}^{n} d_{i,l}^{R_{i,l}} = 1 \bmod p$. If at least one of $b_{1,l}, b_{2,l}, \ldots, b_{n,l}$ is a random integer uniformly distributed in Q, $d_l = D(c_l) = D(\prod_{i=1}^{n} c_{i,l}^{R_{i,l}}) = \prod_{i=1}^{n} d_{i,l}^{R_{i,l}} \bmod p$ is uniformly distributed in Q. So the probability that $d_l = 1$ when there is a bid choice indicating the willingness to pay at p_l is $1/q$, which is overwhelmingly small. □

Theorem 2. *Protocol 1 achieves bid privacy. More precisely, no information about the losing bids is revealed except what can be deduced from the auction result if the number of colluding auctioneers is not over the sharing threshold of the private key.*

Proof: When all the bid choices at p_l are 1, the only revealed information about these bid choices is $d_l = 1$ if the number of colluding auctioneers is not over the sharing threshold of the private key. From the knowledge that $d_l = 1$, it can be deduced that with an overwhelmingly large probability all the bid choices at p_l is 1. However this revealed information can be deduced from the auction result. So bid privacy is not compromised.

When there is at least one bid choice uniformly distributed in Q at p_l, if the number of colluding auctioneers is not over the sharing threshold of the private key the only revealed information about these bid choices is d_l, which is uniformly distributed in Q. In this case the value of d_l reveals that there is at least one none-one bid choice at p_l with an overwhelmingly large probability. However this revealed information can be deduced from the auction result. No other information is revealed if the number of colluding auctioneers is not over the sharing threshold of the private key as given two different sets of bid choices at p_l from Q^n, the two distributions of d_l are indistinguishable (both are uniformly distributed in Q). □

Protocol 1 is publicly verifiable and achieves bid confidentiality and fairness with a threshold trust on the auctioneers. If a reliable digital signature scheme is employed for the bidders to sign their bids, this scheme achieves non-repudiation. If a bid choice indicating willingness to pay is randomly chosen from $Q - \{1\}$, the auction scheme is correct with an even larger probability.

4.2 Protocol 2 — Micro Sealed-bid Auction Employing Downward Search

Usually downward search needs much more searching rounds than binary search, so often compromises efficiency. However, as mentioned in Section 2, only a small number

of biddable prices are needed in micro auction when tie is not a problem (e.g. when multiple copies of the merchandise are available). In this case there is not a great difference between w and $\log_2 w$ as w, the number of biddable prices, is very small. So, if each searching round is very efficient, downward search can also achieve high efficiency. To our knowledge, it is very difficult to achieve high efficiency in each searching round with binary search (a few exponentiations are always needed as no bidding choice can be revealed), while it is possible to achieve high efficiency in each searching round with downward search (computation of exponentiation may be avoided as the bid choices can be simply directly decrypted). Therefore a downward search mechanism with efficient computation in each round is needed to design a micro sealed-bid auction with a small number of biddable prices. At the same time, communication must be efficient and non-interactive bid opening (without communication between the bidders and auctioneers) must be employed.

Unfortunately, none of the existing sealed-bid auction schemes employing downward search can provide this searching mechanism as they are inefficient either in computation or communication. So none of the existing sealed-bid auction schemes employing downward search can be used as a prototype.

However, a solution can still be found to design an efficient micro sealed-bid auction scheme with downward search: modify the auction scheme in [3] and replace the binary search in [3] with downward search. In the auction scheme in [3], bid sealing and bid opening are very efficient. Goldwasser-Micali encryption is employed in [3] for bid sealing, which averagely only costs 1.5 multiplications. Goldwasser-Micali decryption is employed in [3] for bid opening, which costs no more than several multiplications. However, to implement binary search without revealing any bid, complex and costly cut-and-choose strategy and zero knowledge proof are implemented in each round of search. So the binary search in [3] is complex and not very efficient. As the number of biddable prices is small in micro auction, the auction scheme in [3] can be optimized by replacing binary search with downward search, during each round of which all the bid choices at the corresponding price are simply decrypted. The new opening function is very simple and efficient as in each round only n instances of Goldwasser-Micali decryption are employed. After the optimization, the new auction scheme is very simple and efficient in both bid sealing and bid opening. The new micro sealed-bid auction scheme is called Protocol 2 and described as follows.

1. **Preparation phase**
   A bulletin board, acting as a broadcast communication channel, is set up, where the auction rule is published. m auctioneers $A_1, A_2, \ldots, A_m$ are employed. Each A_k sets up a Goldwasser-Micali encryption scheme with modulus N_k, public key y_k, encryption function $E_k()$ and decryption function $D_k()$ for $k = 1, 2, \ldots, m$ where N_k is the product of two secret large primes and y_k is a quadratic non-residue modulo N_k with Jacobi symbol 1. The existing Goldwasser-Micali encryption algorithm is slightly modified as follows.
   - Message space and ciphertext space: $\{1, -1\} \longrightarrow Q$ where Q contains all the integers with Jacobi symbol 1.
   - Encryption
     - If the message is 1, a ciphertext for the k^{th} auctioneer is $x^2 \bmod N_k$ where x is randomly chose from $Z^*_{N_k}$.

- If the message is -1, the ciphertext for the k^{th} auctioneer is $yx^2 \bmod N_k$ where x is randomly chose from $Z^*_{N_k}$.

– Decryption: If an integer with Jacob symbol -1 is given as the ciphertext, the decryption fails and the integer is declared as an invalid ciphertext[1]. If a valid ciphertext is given, output the Legendre symbol of the ciphertext. When necessary, validity of decryption can be publicly proved: publishing a square root of the ciphertext when the decryption outputs 1 or publishing a square root of product of the ciphertext and the public key when the decryption outputs -1.

The modified Goldwasser-Micali encryption algorithm is semantically secure like the original Goldwasser-Micali encryption algorithm as the only change in the modification is replacing 0 with -1 in the message space.

2. **Bidding phase**
   Each bidder B_i chooses $b_{i,j}$, his bidding choice at the j^{th} biddable price for $j = 1, 2, \ldots, w$. If he is willing to pay p_j, B_i chooses $b_{i,j} = -1$. If he is not willing to pay p_j, B_i chooses $b_{i,j} = 1$. Then B_i randomly chooses $b_{i,j,k}$ from $\{1, -1\}$ for $k = 1, 2, \ldots, m$ such that $b_{i,j} = \prod_{k=1}^{m} b_{i,j,k}$. Finally, B_i calculates $c_{i,j,k} = E_k(b_{i,j,k})$ for $j = 1, 2, \ldots, w$ and $k = 1, 2, \ldots, m$, then signs and publishes them on the bulletin board.
3. **Bid opening phase**
   At price p_1, each auctioneer A_k calculates $d_{i,1,k} = D_k(c_{i,1,k})$ for $i = 1, 2, \ldots, n$ and proves validity of decryption. Then $d_{i,1} = \prod_{k=1}^{m} d_{i,1,k}$ is calculated for $i = 1, 2, \ldots, n$. If there is any bid choice $d_{i,1}$ equivalent to -1, it is the winning bid. If $d_{i,1} = 1$ for $i = 1, 2, \ldots, n$, there is no bidder willing to pay p_1 and $c_{i,2,k}$ for $i = 1, 2, \ldots, n$, the bid choices at p_2, are opened with proof of validity of decryption. The search goes downwards until bid choice equivalent to -1 is found as the winning bid.
4. **Winner identification phase**
   The signature on the winning bid is verified and the winner is identified.

Theorem 3. *Protocol 2 is correct. More precisely, there exist i in $\{1, 2, \ldots, n\}$ such that $d_{i,j} = -1$ if and only if there is at least a bid choice indicating the willingness to pay at p_j.*

Proof: $d_{i,j} = \prod_{k=1}^{m} d_{i,j,k} = \prod_{k=1}^{m} D_k(c_{i,1,k}) = \prod_{k=1}^{m} D_k(E_k(b_{i,1,k})) = \prod_{k=1}^{m} b_{i,1,k} = b_{i,j}$ So there exist i in $\{1, 2, \ldots, n\}$ such that $d_{i,j} = -1$ if and only if there is at least a bid choice indicating the willingness to pay at p_j. □

Theorem 4. *Protocol 2 achieves bid privacy. More precisely, no information about the losing bids is revealed except what can be deduced from the auction result if at least one auctioneer does not conspire.*

Proof: As downward search is employed, only the bid choices no lower than the winning price are opened. Every bid choice lower than the winning price is shared

[1] Computation for Jacob symbol is efficient and comparable to a multiplication, so invalid ciphertext can be discovered easily.

among the auctioneers. Every bid choice is the product of its shares, which are randomly chosen. Also note that the modified Goldwasser-Micali encryption algorithm is semantically secure and no information is revealed from an encrypted bid choice or bid choice share. So at a price p_j lower than the winning price, even if $m-1$ colluding auctioneers put their shares together, they get no information about any $b_{i,j}$ as no matter whether $b_{i,j}=1$ or $b_{i,j}=-1$, the $m-1$ shares of it are uniformly distributed in $\{1,-1\}^{m-1}$, which is indistinguishable. So no bid choice lower than the winning price is revealed except what can be deduced from the auction result if at least one auctioneer does not conspire. □

Protocol 2 is publicly verifiable and achieves bid confidentiality and fairness with a m-out-of-m trust on the auctioneers. If a reliable digital signature scheme is employed for the bidders to sign their bids, this scheme achieves non-repudiation. As no exponentiation computation is needed in bid sealing and bid opening, this auction scheme is efficient, especially when the number of biddable prices is small.

5 Further Improvement

Protocol 1 is more efficient than the existing sealed-bid auction schemes with bid privacy and is suitable for micro auction. Protocol 2 provides an efficient solution to micro auction as well when the number of biddable prices is small. However they still have drawbacks. Firstly, they are still not efficient enough for micro auction with a computational cost of at least $O(m(n+(n+1)\log_2 w))$ exponentiations and $O(wmn)$ exponentiations respectively. So their cost may still be higher than the value of the merchandise in some micro auction applications. Secondly, Protocol 2 is only efficient when the number of biddable prices is small. When tie is concern and the number of biddable prices cannot be too small,Protocol 2 is not efficient enough for micro auction.

So further improvement work (especially in efficiency) is still needed in these two protocols. Unfortunately, efficiency improvement is difficult in Protocol 1. However, in Protocol 2 a dramatic efficiency improvement can be made. The efficiency bottleneck in Protocol 2 lies in proof of validity of decryption of the bid choices in Step 3 (bid opening phase): to publicly prove validity of a decryption, a square root must be calculated, whose cost approximately equals $O(1)$ exponentiations. A solution to this efficiency bottleneck is to batch prove validity of multiple decryptions, which is similar to the idea of aggregate verification in micro payment system [1]. Namely, when M integers $c_1, c_2, \ldots, c_M$ need proving to be quadratic residues, a batch proof instead of M separate proofs can be used, so that invalid decryption by the auctioneers can be detected. The batch proof is described in Figure 1.

1. S, a random subset of $\{1,2,\ldots,M\}$, is chosen.
2. Square root of $\prod_{i\in S} c_i$ is provided.
3. Repeat the operations above T times.

Fig. 1. Batch proof of quadratic residues.

Theorem 5. *If there is at least one quadratic non-residue among* $c_1, c_2, \ldots, c_M$, *the proof in Figure 1 can succeed with a probability no more than* 2^{-T}.

Proof: Suppose c_v is a quadratic non-residue where $1 \leq v \leq M$ Note that half of the subsets of $\{c_1, c_2, \ldots, c_M\}$ contain c_v and the other half do not contain c_v. So all the subsets of $\{c_1, c_2, \ldots, c_M\}$ can be divided into pairs such that in each pair the only difference between the two subsets is that one of them contains c_v and the other does not contain c_v. Note that in each pair of the subsets, the product of one subset's elements must be a quadratic residue while the product of the other subset's elements must be a quadratic non-residue. Namely, half of the subsets of $\{c_1, c_2, \ldots, c_M\}$ contain elements whose product is a quadratic residue and the other half of the subsets of $\{c_1, c_2, \ldots, c_M\}$ contain elements whose product is a quadratic non-residue. So square root of $\prod_{i \in S} c_i$ can be provided with a probability 0.5 when S is randomly chosen from $\{1, 2, \ldots, M\}$. Therefore, if there is at least one quadratic non-residue among $c_1, c_2, \ldots, c_M$, proof in Figure 1 can succeed with a probability no more than 2^{-T}. □

The batch proof technique in Figure 1 can be employed to improve efficiency of Protocol 2, where each auctioneer acts as a prover and the random subsets are chosen according to a one-way hash function of the decryption result[2]. In Protocol 2, each auctioneer has to perform $O(nw)$ decryptions, so has to give $O(nw)$ instances of proof of quadratic residue. Normally, computation of $O(nw)$ square roots (costing $O(nw)$ exponentiations) is needed in every auctioneer's proof of decryption validity. When the batch proof technique in Figure 1 is applied to prove validity of decryption, only T square roots need calculating for each auctioneer. Although each auctioneer has a probability of 2^{-T} to cheat successfully, it is worthless for him to risk his reputation or qualification with so low a success rate for a small-value merchandise. Actually, when T is larger than 20, the success rate is less than 0.000001 when there is incorrect decryption, which is small enough to deter an auctioneer from cheating in a micro auction. So this efficiency improvement by batch proof is appropriate in micro auction. After this improvement, only a small constant number of exponentiations are needed in protocol 2. Besides greatly improving efficiency, this optimisation is not affected by the number of biddable prices. Namely, even when tie is a concern and a large number of biddable prices is needed, high efficiency can still be achieved. Moreover, batch proof can be further extended so that each auctioneer's proof of quadratic residue in multiple micro auction processes during a fixed period can be batched into computation of T square roots.

6 Conclusion

Requirements for micro auctions and methods to design sealed-bid micro auctions are surveyed in this paper. The first two secure micro sealed-bid e-auctions schemes are

[2] For example, the hash function has an N-bit output $z = z_1 z_2 \ldots z_N$ while an auctioneer has to prove N quadratic residues $c_1, c_2, \ldots, c_N$. c_i is chosen into the random subset if and only if $z_i = 1$.

proposed in this paper. They can satisfy all the security requirements necessary for micro auction. Moreover, these two schemes are efficient, especially when the number of biddable prices is small (as in most micro auctions). The second scheme is further improved in efficiency by batch proof such that only a small constant number of exponentiations are needed. Although instant verification is sacrificed after the optimisation, the sacrifice is tolerable in micro auctions.

Efficiency of the micro auction schemes in this paper and their prototypes are compared in Table 1, where ElGamal encryption and RSA signature are employed and the number of exponentiations are counted. An example is given in Table 1, where $w = 16$, $n = 200$, $m = 5$ and $T = 20$. Table 1 clearly demonstrates that the micro auction schemes proposed in this paper (especially the optimised Protocol 2) are very efficient. Contributions of the paper are illustrated in Table 2. It is clearly demonstrated in Table 2 that very high efficiency can be achieved for micro auction without compromising bid privacy by sacrificing unconditional fairness and instant verification, which can be tolerated in micro auction.

Table 1. Efficiency of Micro Auction Schemes.

Schemes	Computation			
	bidder	example	auctioneer	example
[4]	$(3m+3)w+1$	289	$1+5n+5n\log_2 w$	5001
Protocol 1	$2w+1$	33	$(n+2)\log_2 w+2n+1$	1209
[3]	1	1	about $(mn+4m+n)\log_2 w$	4880
Protocol 2	1	1	$0.5wn$	1600
Optimised Protocol 2	1	1	T	20

Table 2. Contribution of the Micro Auction Schemes.

Schemes	Fairness	Communi--cation	Search style	Biddable prices	Verification	Computation efficiency
[4]	Unconditional	2 rounds	Binary	Limited	Instant	Normal
Protocol 1	Trust-based	1 round	Binary	Limited	Instant	High
[3]	Trust-based	1 round	Binary	Limited	Instant	Normal
Protocol 2	Trust-based	1 round	Downward	Limited	Instant	High
Optimised Protocol 2	Trust-based	1 round	Downward	Unlimited	Batched	Very high

References

1. Silvio Micali and Ronald Rivest. Micropayments revisited. In *CT-RSA*, volume 2271 of *Lecture Notes in Computer Science*, pages 149–163, Berlin, 2002. Springer.
2. Torben P. Pedersen. *Distributed Provers and Verifiable Secret Sharing Based on the Discrete Logarithm Problem*. PhD thesis, Computer Science Department, Aarhus University,Aarhus, Denmark, 1992.
3. Kun Peng, Colin Boyd, and Ed Dawson. A multiplicative homomorphic sealed-bid auction based on Goldwasser-Micali encryption. In *ISC 2005*, volume 3650 of *Lecture Notes in Computer Science*, pages 374–388, Berlin, 2005. Springer-Verlag.
4. Kun Peng, Colin Boyd, and Ed Dawson. Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing. In *Mycrypt 2005*, volume 3715 of *Lecture Notes in Computer Science*, pages 84–98, Berlin, 2005. Springer-Verlag.
5. Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan. Non-interactive auction scheme with strong privacy. In *5th International Conference of Information Security and Cryptology - ICISC 2002*, volume 2587 of *Lecture Notes in Computer Science*, pages 407 – 420, Berlin, 2002. Springer.
6. 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.