An efficient multi-round anonymous auction protocol

Cheng-Chi Lee

Department of Management Information Systems

National Chung Hsing University

250 Kuo Kuang Road

402 Taichung, Taiwan

R.O.C.

Min-Shiang Hwang *

Department of Computer Science

National Chung Hsing University

250 Kuo Kuang Road

402 Taichung, Taiwan

R.O.C.

and

Department of Computer of Communication Engineering

Asia University

No. 500, Lioufeng Raod

Wufeng Shiang

Taichung, Taiwan

R.O.C.

Chih-Wei Lin

Department of Computer Science

National Tsing Hua University

Hsinchu, Taiwan 300

R.O.C.

* *E-mail*: `mshwang@nchu.edu.tw`

Journal of Discrete Mathematical Sciences & Cryptography
Vol. ( ), No. , pp. 1–11

Abstract

In this paper, we shall propose an efficient multi-round anonymous auction protocol. In the many literatures concerned, when more than one party bidding the same highest price for merchandise, all the bidders must re-participate in the auction again. It is inefficient. In this paper, the proposed protocol can make the auction easier. In our system, we first pick out the bidders offering the same highest price as the winners of the first round. Then, all the bidders need not re-participate in the auction again; only the winners of the first round have to come back for the second round.

Keywords and phrases : *Anonymity, auction, knapsack problem, multiparty computation, security.*

1. Introduction

Due to the fast development of the Internet, more and more business is done in the form of electronic commerce [7, 12]. Electronic transfer of goods and information is efficient. Likewise, in this modern world, more and more traditional auctions have been replaced by electronic auctions. Electronic auctions are an important part of electronic commerce; such business opportunities on line actually make bidders around the world able to make their deals anywhere through the Internet. However, electronic auctions suffer from some security problems such as revealing, stealing, and altering [8]. Several properties have been defined for electronic auction as follows [3, 4, 17, 18]:

The privacy of sealed bids: The auctioneer must not know how much the bidders offer until the auction finishes. Otherwise, the auctioneer could possibly reveal information to bidders. Thus, the result of the bidding will be influenced.

The anonymity of sealed bids: All of the bidders' identities must be anonymous during the bidding.

Validity: Everyone will be allowed to check the source and completion of a bid. However, nobody can submit a falsified bid to the auctioneer even if they disguise as a legitimate bidder.

Non-repudiation: No one can repudiate his/her bid. Every bidder has a certificate to identify his/her bid.

Fast execution: The auction should support many bidders and efficiently find out the winner of this auction.

Recently, a lot of studies have been published [6, 9, 10, 13]. In 1996, Franklin and Reiter proposed a sealed-bid auction which uses a verifiable signature sharing mechanism to prevent the single auctioneer from cheating during auction [6]. In 1998, Kudo proposed a secure electronic sealed-bid auction protocol which uses a third party's public key to encrypt the bidders' bids [10]. This protocol can effectively seal the bids.

Based on Shamir's secret sharing scheme [16], Kikuchi *et al.* [9] and Liu *et al.* [13] individually proposed muti-round auction protocols. The protocols ensure that the bid values will not be revealed. However, the protocols have the following weakness. When more than one bidder bid the same highest price for one merchandise, namely when a *tie of auction* occurs, all the bidders must reparticipate in the auction again, because the protocols cannot detect the definite identities of the bidders who bid the same highest price. It is inefficient.

In this paper, based on the Knapsack theory [2, 5, 11, 14], we shall propose an efficient multi-round anonymous auction protocol. The proposed protocol can detect the definite identities of the bidders who bid the same price. In addition, all the bidders need not re-participate in the auction again when there is a tie; only the winners of the first round can come back for the second round. Our proposed protocol is quite efficient.

2. Our proposed protocol

In our proposed protocol, suppose we have n bidders, m auctioneers and a seller S in this model. Assume that at most $(t-1)$ auctioneers may divulge bids.

The basic concept develops from the secure multiparty computation of addition [1, 15]. The protocol operates as follows. First, the seller posts k bidding prices $(w_1, w_2, \ldots, w_k)$ to the bidders and auctioneers for merchandise. The prices increase progressively. If a bidder decides to take a price from $w_1, w_2, \ldots, w_k$, he/she sends his/her ID_j value; otherwise he/she sends 0. Then each of the bidders sends k polynomials to each auctioneer. The auctioneers then do the secure multiparty computation for addition and figure out the sum of the ID_j values for the final price. After that, three cases are likely to take place:

1. If there is only one bidder willing to pay the price, he/she is the winner, and the auction comes to an end. Nobody gets to know

the winner's real identity except the seller. In this case, the requirement of anonymity is ensured.

2. If more than one bidder is willing to pay the price, the result is the total of the bidders' identities. It means that there is a tie. These bidders will know that someone else has offered the same price too.
3. If nobody is willing to bid the price, the result is 0. It means none of the prices posted by the seller is attractive enough for any of the bidders. In this case, no information is revealed.

First, all bidders turn to the seller to register. The seller assigns public identities to the bidders for this competition and publishes them to the auctioneers. The bidders' identities then go under symmetric-key encryption with the seller's key. Therefore, the identities are protected to ensure the anonymity of the bidders. For example, the j-th bidder's public identity can be defined as follows.

$$ID_j = b_j,\ b_j > \sum_{i=1}^{j-1} b_i, \quad \text{for } 2 \leq j \leq n\,.$$

The seller maintains a secret table as follows that can help to derive the identities of all the bidders.

Table 1

Encrypted identities of all the bidders

Code name (ID_j)	Encrypted identity
b_1	$E_{d_s}(I_1)$
b_2	$E_{d_s}(I_2)$
.	.
b_j	$E_{d_s}(I_j)$
.	.
b_n	$E_{d_s}(I_n)$

On the last round auction, t auctioneers can compute the unique winner's public identity ID_j by means of the *Lagrange scheme* [16] and then sent it to the seller.

When the seller obtains the winner's public ID_j, b_j, he/she can figure out the identity of the winner by looking into the secret table and then checking out $E_{d_s}(I_j)$. Here I_j is the j-th identity, and $E_{d_s}(\cdot)$ is an encryption function with the seller's key d_s.

Our protocol is shown in detail as follows. First, the initialization step requires that all the bidders come to the seller to register and get the code names. The bidders are then qualified to bid in the auction. In the polling step, the seller posts k prices for the goods to the bidders arid auctioneers. Next, in the bidding step, all the bidders bid their own prices for the goods. In the opening step, the system knows who the winner is in this auction. And in declaring step, the seller is informed of the winner's ID.

Initialization: All the bidders first register at the seller. The seller generates ID_j for all the bidders and publishes them to the auctioneers for this competition. ID_j can be defined as $ID_j = b_j$, where $b_j > \sum_{i=1}^{j-1} b_i$, for $2 \leq j \leq n$.

Polling: The seller S posts k prices $(w_1, w_2, \ldots, w_k)$ for the goods to the bidders arid auctioneers. And the auctioneers publish an integer r and one-way hash function g to all the bidders.

Bidding: Each bidder ID_j only chooses one price w_l from the k prices $(w_1, w_2, \ldots, w_k)$. The j-th bidder randomly picks k polynomials from $f_{jl}(x) = s_l + a_{1l}x + a_{2l}x^2 + \ldots + a_{(t-i)l}x^{t-1} \bmod p$, where $l \in 1, 2, \ldots, k$ and $j \in 1, 2, \ldots, n$. Then, he/she sends them to the m auctioneers, where p is a large prime and $a_1, a_2, \ldots, a_{t-1}$ are integers ranging in $[1, p-1]$. The free variable, s_l, is established as follows:

$$\begin{cases} s_l = g^r(ID_j) & : j\text{-th bidder willing to bid the price } w_l \,; \\ s_l = 0 & : \text{otherwise,} \end{cases}$$

where $g^r(\cdot)$ denotes that the one-way hash function g is to be computed r times.

Remark. The bidder applies hash function g to a free variable, and the reason for that is to prevent anyone from disguising a legal bidder to bid. He/she makes the bid by computing using one-way function g upon the free variable r times. The auctioneers declare $r = r - 1$ when there is a tie, and, in this case, the auction moves to the round.

Opening: The i-th auctioneer can collect $f_{jl}(\alpha_i)$ from every bidder for each price, where α_i is i's identity, and compute $F_l(\alpha_i) = f_{1l}(\alpha_i) + f_{2l}(\alpha_i) + \ldots + f_{nl}(\alpha_i)$ for each price and then publish the result to the seller and the other auctioneers. When getting t or more than t polynomials, namely $F_l(\alpha_i), \ldots, F_l(\alpha_t), \ldots, F_l(\alpha_m)$, each auctioneer can obtain the free variable s_l by means of the Lagrange scheme to solve the simultaneous equations.

Therefore, the sum of the identities of bidders T for each price can be obtained. Checking from the highest price w_k down, we can find the first non-zero figure from the sum of identities. The winning price is the first non-zero figure from the sum of identities. The auctioneers get to know the identities because it is a *Super Increasing sequence*. They can use the *Algorithm* as follows [11, 14]:

for $i = n$ down to 1 do if
  if $T \geq g^r(b_i)$ then
    $T = T - g^r(b_i)$
    $x_i = 1$
  else
    $x_i = 0$
if $\sum_{i=1}^{n} x_i g^r(b_i) = T$ then
  $X = (x_1, x_2, \ldots, x_n)$ is the solution
else
  there is no solution

If $x_i = 1$, that means the i-th bidder is a winner in this auction. If more than one x_i is equal to 1, that means there is a tie, arid only the bidders that satisfy $x_i = 1$ can re-participate in the next round.

Declaring: Lastly, we can find the winner according to the following scenarios:

- If the sum of identities turns out to be only one, it represents the bidder ID_j is the winner. Then the auctioneer informs the seller of the result. The seller can decrypt the winner's identity I_j via $E_{d_s}(I_j)$ from his/her secret maintaining table.
- If the sum of identities turns out to be more than one, then there is a tie in this auction. The auctioneers should find the winners out, and declare which of the bidders are allowed to enter the next auction round on the bulletin board. The seller resets the k prices, $w'_1, w'_2, \ldots, w'_k$, where $w'_1 > w_k$.

If no non-zero figures can be found out of the free variable, it means that nobody has made a bid upon the prices from $w_1, w_2, \ldots, w_k$. The seller must reset those k prices, $w'_1, w'_2, \ldots, w'_k$, where $w'_k < w_k$ and republish them for the next auction round.

3. A simple example

Initialization: Assume that there are three bidders in this auction: Bidder 1 (I_1), Bidder 2 (I_2), and Bidder 3 (I_3). The seller gives them three public identities $ID_j = b_j$, where $j = 1, 2, 3$. Then the seller publishes them to the auctioneers and maintains a secret table as Table 2.

Figure 2
Encrypted identities of all the bidders

ID_j	Encrypted identity
b_1	$E_{d_s}(I_1)$
b_2	$E_{d_s}(I_2)$
b_3	$E_{d_s}(I_3)$

Assume that there are five auctioneers, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, and α_5, respectively.

Polling: The seller posts 5 bidding prices for the goods, $\{1, 2, 3, 4, 5\}$, to the bidders and auctioneers. Then, the auctioneers publish an integer r and a one-way hash function g.

Bidding: Suppose Bidder 1 is willing to bid price 3, Bidder 2 is willing to bid price 3, and Bidder 3 is willing to bid price 2. According to Shamir's threshold scheme $(3, 5)$, in this example, only when three auctioneers work together can the winner's identity ID_j be obtained by using the Lagrange scheme. Our scheme works as follows:

- Bidder 1: Randomly picks 5 polynomials of degree 2 as

$$\begin{aligned}
f_{11}(x) &= g^r(b_1) + a_{11}x + a_{11}x^2 \bmod p,\\
f_{12}(x) &= g^r(b_1) + a_{12}x + a_{12}x^2 \bmod p,\\
f_{13}(x) &= g^r(b_1) + a_{13}x + a_{13}x^2 \bmod p,\\
f_{14}(x) &= 0 + a_{14}x + a_{14}x^2 \bmod p,\\
f_{15}(x) &= 0 + a_{15}x + a_{15}x^2 \bmod p,
\end{aligned}$$

and sends them to all auctioneers i, $i = 1, 2, \ldots, 5$.

- Bidder 2: Randomly picks 5 polynomials of degree 2 as

$$\begin{aligned}
f_{21}(x) &= g^r(b_2) + a_{21}x + a_{21}x^2 \bmod p, \\
f_{22}(x) &= g^r(b_2) + a_{22}x + a_{22}x^2 \bmod p, \\
f_{23}(x) &= g^r(b_2) + a_{23}x + a_{23}x^2 \bmod p, \\
f_{24}(x) &= 0 + a_{24}x + a_{24}x^2 \bmod p, \\
f_{25}(x) &= 0 + a_{25}x + a_{25}x^2 \bmod p,
\end{aligned}$$

and sends them to all auctioneers i, $i = 1, 2, \ldots, 5$.

- Bidder 3: Randomly picks 5 polynomials of degree 2 as

$$\begin{aligned}
f_{31}(x) &= g^r(b_3) + a_{31}x + a_{31}x^2 \bmod p, \\
f_{32}(x) &= g^r(b_3) + a_{32}x + a_{32}x^2 \bmod p, \\
f_{33}(x) &= g^r(b_3) + a_{33}x + a_{33}x^2 \bmod p, \\
f_{34}(x) &= 0 + a_{34}x + a_{34}x^2 \bmod p, \\
f_{35}(x) &= 0 + a_{35}x + a_{35}x^2 \bmod p,
\end{aligned}$$

and sends them to all auctioneers i, $i = 1, 2, \ldots, 5$.

Opening: The i-th auctioneer can collect $f_{jl}(\alpha_i)$ from every bidder for each price, and compute $F_l(\alpha_i)$ for each price as follows:

$$\begin{array}{ccc}
\textit{Auctioneer } 1 & \textit{Auctioneer } 2 & \textit{Auctioneer } 3 \\
F_1(\alpha_1) & F_1(\alpha_2) & F_1(\alpha_3) \\
\vdots & \vdots & \vdots \\
F_5(\alpha_1) & F_5(\alpha_2) & F_5(\alpha_3)
\end{array}$$

And then the auctioneer can use Lagrange scheme to recover the free variable s_l:

$$\begin{aligned}
F_5(0) &= F_5(\alpha_1) + F_5(\alpha_2) + F_5(\alpha_3) = 0 + 0 + 0 = 0 \\
F_4(0) &= F_4(\alpha_1) + F_4(\alpha_2) + F_4(\alpha_3) = 0 + 0 + 0 = 0 \\
F_3(0) &= F_3(\alpha_1) + F_3(\alpha_2) + F_3(\alpha_3) = g^r(b_1) + g^r(b_2) + 0 = T\,.
\end{aligned}$$

Checking from the highest price w_5 down, we can find the first non-zero figure at price 3 from the sum of identities, by using the above *Algorithm* for solving a *Super Increasing* subset problem [11, 14].

As the result, we know ID_1 and ID_2 tie in this auction.

Declaring: The auction ends up a tie with two winners ID_1 and ID_2. Declare the next auction round for only ID_1 and ID_2 is declared so as to find the final winner.

4. Analysis

We give performance analysis and crypt analysis in this section.

Performance analysis

We use Knapsack theory to efficiently make clear the identities of the bidders who bid the same highest price. In the initiation step, all the bidders must register at the seller. The seller assigns public identities composed of $b_j > \sum_{i=1}^{n} b_i$. In the opening step, t or more than t auctioneers can compute the sum of the winners' public identities by means of the *Lagrange* scheme and solve it by the algorithm. The algorithm can exactly figure out the winners' identities.

Assume that we have n bidders and v out of these n bidders win the first round in this auction. If a tie happens in [9, 13], then the seller will have to ask all these n bidders to join the next round. Such a procedure can drag on and on and become exhausting before the winner finally comes out if he/she can.

In this paper, we have proposed a scheme more efficient than those in [9, 13]. In our scheme, if there is a tie, only the v winners of this round can participate in the next auction. Because we can exactly recognize the identities of the winners of the tie, we can reduce re-bidding times and come up with the final winner a lot more quickly.

Cryptanalysis

The bids of those who lose in the auction will not be unveiled. In the mean time, all of the bidders are kept anonymous. Throughout the auction, the bidders are seen as no more than public identities. The seller is the only one who gets to know the identity of the final winner by checking the secret table and then decrypting the encrypted identity by his/her symmetric-key.

Our scheme is based on Shamir's (t, n) threshold secret sharing method [16]. The security is guaranteed except that t or more than t auctioneers could collaborate and divulge bids, which is riot likely to happen. Besides, the bids of the bidders who lose the auction will not be revealed.

5. Discussion and conclusion

As our scheme has demonstrated, it is efficient to find out the identity of the winner by a secret table. The security of the table is maintained by the seller with a symmetric-key cryptosystem. So, we suggest that 512-bit strings be used in the Super Increasing sequence as the bidders' ID_j and b_j so as to reduce the probability of other bidders disguising the owner of ID_j to bid.

This paper focuses on solving the problem of multiple winners in a tie. The problem has been mentioned in Kikuchi's *et al.*'s paper [9], and their solution is to simply allow all the bidders to join in the next round, as if starting the auction all over again. To deal with the problem more constructively and more efficiently, we offer a new scheme that can identify the identities of the winners of the tie, allowing only the tie winners to participate in the competition in the next round. This way, the final winner can come out with much more ease.

References

[1] M. Ben-Or, S.Goldwasser and A. Wigderson, Completeness theorems for non-cryptographic fault-tolerant distributed computation, in *Proceedings of the 30th Annual ACM Symposium on the Theory of Computing*, pp. 1–10, Texas, May 1998.

[2] E. F. Brickell and A. M. Odlyzko, Cryptanalysis: A survey of recent results, in *Preliminary version in Proceedings of the IEEE*, Vol. 76, pp. 578–593, New Jersey, USA, May 1988.

[3] Y. F. Chang and C. C. Chang, Enhanced anonymous auction protocols with freewheeling bids, in *20th International Conference on Advanced Information Networking and Applications*, Vol. 1, pp. 1–6, April 18–20, 2006.

[4] W. Changjie, C. Xiaofeng and W. Yumin, An agent-based multi rounds online auction protocol with sealed bids, in *17th International Conference on Advanced Information Networking and Applications*, pp. 194–197, March 27–29, 2003.

[5] B. Chor and R.L. Rivest, A knapsack-type public key cryptosystem based on arithmetic in finite fields, *IEEE Transactions on Information Theory*, Vol. 34 (5), pp. 901–909, 1988.

[6] M.K. Franklin and M.K. Reiter, The design and implementation of a secure auction service, *IEEE Transactions on Software Engineering*, Vol. 22 (3), pp. 302–312, 1996.

[7] M.-S. Hwang, I.-C. Lin and L.-H. Li, A simple micro-payment scheme, *Journal of Systems and Software*, Vol. 55 (3), pp. 221–229, 2001.

[8] M.-S. Hwang, E. J.-L. Lu and I.-C. Lin, Adding times-tamps to the secure electronic auction protocol, *Data & Knowledge Engineering*, Vol. 40 (2), pp. 155–162, 2002.

[9] H. Kikuchi, M. Hakavy and D. Tygar, Multi-round anonymous auction protocols, *IEICE Transactions on Information and Systems*, Vol. E82-D (4), pp. 769–777, 1999.

[10] M. Kudo, Secure electronic sealed-bid auction protocol with public key cryptography, *IEICE Transactions on Fundamentals*, Vol. E81-A (1), pp. 20–27, 1998.

[11] C. S. Laih, J. Y. Lee, L. Harn and Y. K. Su, Linearly shift knapsack public key cryptosystem, *IEEE Journal on Selected Areas in Communications*, Vol. 7 (4), pp. 534–539, 1989.

[12] I. C. Lin, M. S. Hwang and C. C. Chang, Security enhancement for the anonymous secure e-voting over a network, *Computer Standards and Interfaces*, Vol. 25 (2), pp. 131–139, 2003.

[13] S. Liu, C. Wang and Y. Wang, A secure multi-round electronic auction scheme, in *Proceedings of the EUROCOMM'2000*, pp. 330–334, Germany, May 2000.

[14] A. J. Menezes, P. C. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[15] T. Rabin and M. Ben-Or, Verifiable secret sharing and multiparty protocols with honest majority, in *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pp. 73–85, Washington, May 1989.

[16] A. Shamir, How to share a secret?, *Communications of the ACM*, Vol. 22 (11), pp. 612–613, 1979.

[17] F. Zhang, Q. Li and Y. Wang, A new secure electronic auction scheme, in *Proceedings of the EUROCOMM 2000*, pp. 54–56, Germany, May 2000.

[18] Q. Xiao and L. Ping, A general secure electronic auction protocol, in *IEEE International Conference on Systems, Man and Cybernetics*, pp. 398–402, October 10-13, 2004.

Received September, 2006