Privacy-Preserving Strategyproof Auction Mechanisms for Resource Allocation in Wireless Communications

Yu-E Sun[1,3], He Huang[2,3(✉)], Xiang-Yang Li[3], Yang Du[3], Miaomiao Tian[3], Hongli Xu[3], and Mingjun Xiao[3]

[1] School of Urban Rail Transportation, Soochow University, Suzhou, China
[2] School of Computer Science and Technology, Soochow University, Suzhou, China
huangh@suda.edu.cn
[3] School of Computer Science and Technology,
University of Science and Technology of China, Hefei, China

Abstract. In recent years, auction theory has been extensively studied and many state-of-art solutions have been proposed aiming at allocating scarce resources (*e.g.* spectrum resources in wireless communications). Unfortunately, most of these studies assume that the auctioneer is always trustworthy in the sealed-bid auctions, which is not always true in a more realistic scenario. On the other hand, performance guarantee, such as social efficiency maximization, is also crucial for auction mechanism design. Therefore, the goal of this work is to design a series of strategyproof and privacy preserving auction mechanisms that maximize the social efficiency. To make the designed auction model more general, we allow the bidders to express their preferences about multiple items, which is often regarded as the *multi-unit auction*. As computing an optimal allocation in multi-unit auction is NP-hard, we design a set of near optimal allocation mechanisms with privacy preserving separately for: (1) The auction aims at identical multi-items trading; and (2) The auction aims at distinct multi-items trading, which is also known as combinatorial auction. To the best of our knowledge, we are the first to design strategyproof multi-unit auction mechanisms with privacy preserving, which maximize the social efficiency at the same time. The evaluation results corroborate our theoretical analysis, and show that our proposed methods achieve low computation and communication complexity.

Keywords: Approximation mechanism · Multi-unit auction · Privacy preserving · Social efficiency · Strategyproof

1 Introduction

Auction serves as a preeminent way to allocate resources to multiple bidders, especially for the scarce resources in wireless communications (such as *the computing resources in cloud* [14], *spectrum licenses* [7,8,21], *cellular networks* [6],

Y. Wang et al. (Eds.): BigCom 2016, LNCS 9784, pp. 13–26, 2016.
DOI: 10.1007/978-3-319-42553-5_2

CRNs [19,20], and *etc.*) due to its fairness and efficiency [1,11]. Strategyproofness (*a.k.a truthfulness*) is regarded as one of the key objectives in the auction mechanism design, which means that the optimal strategies for bidders is to bid their *true valuations* of the items for sale. Most of the auction mechanisms are designed to charge each winner the minimum bid value, by which he can win the auction, to ensure the strategyproofness of bidders. Unfortunately, the auctioneer may not always be trustworthy. Once the true valuation of each bidder is revealed to an untrustworthy auctioneer, he may take advantage of this to maximize his own profits.

To solve the above challenge, the bid values should be hidden in the whole procedure of the auction. Thus, protecting the privacy of bids should be regarded as an attractive objective in the design of auction mechanisms. In recent years, some researchers have dedicated their efforts in the auction mechanism design with privacy preserving. For instance, in [2,10], the authors design some mechanisms to protect the bid value in the first price and the second price sealed-bid auctions. Huang *et al.* [9] propose a strategyproof and bid privacy preserving auction mechanism for spectrum allocation. Pan *et al.* [15,16] also give a secure combinatorial spectrum auction by using homomorphic encryption to deal with the untrustworthy auctioneer. However, none of these auction mechanisms with privacy preserving provides any performance guarantee on *social efficiency*, *i.e.* the total bid value of winners, which is a standard and critical auction metric [4,13].

In this paper, we focus on the privacy preserving and strategyproof auction mechanism design for resource allocation, which can maximize the social efficiency at the same time. Observe that most of the existing auction mechanisms fail to take the multiple items trading into consideration. Nevertheless, bidders may often express their preferences for a specified number of items or some specified bundles of items, instead of individual item. This kind of auction is called by the *multi-unit auction*. There are two cases in multi-unit auction: the items sold in the market are *identical* or *distinct*. In this work, we will propose two auction mechanisms to deal with the identical condition and the distinct condition. In our design for identical items, the demand of each bidder is a fixed number of items, which is inseparable. The auction for distinct items is also known as *combinatorial auction*. In a combinatorial auction, all the bidders can bid for bundles of items rather than individual items [3]. Thus, the combinatorial auctions enable bidders to express their preferences in a more meaningful way. In both auction models, the bid values of bidders are private information. Except that, which items that each bidder wants to buy is also a sensitive information in the combinatorial auction. This is because if the auctioneer knows that how many bidders are interested in each item, he may raise the price in future auctions to maximize his own profit. Besides, the auctioneer needs to know each winner's demand to finish the auction. Therefore, except for protecting the bid values of bidders in both auction models, we also need to protect the *combination items* that each loser wants to buy in the combinatorial auction.

The multi-unit auction mechanism design with consideration of social efficiency maximization issue is NP-hard [17]. Many efficient approximation algorithms have been proposed for both the Identical items Auction model (*i.e.* IA model) and Combinatorial Auctions model (*i.e.* CA model). For example, there are a polynomial time approximation scheme (PTAS), which is suitable for the IA auction model, and an approximation algorithm with an approximation factor of $\sqrt{h}$ that has been proved tight for the combinatorial auctions. Thus, our work in this paper is not to design approximation algorithms that improve the performance of the existing studies, but is to design mechanisms with privacy preserving, based on these existing approximation mechanisms.

However, the computation burden which relies on the bid values of bidders is too heavy in the existing approximation algorithms with good performance guarantee. Thus, the task of designing privacy preserving auction mechanisms with performance guarantee is highly challenging. To tackle this, we introduce an agent into our auction model, who is a *semi-trusted* third party, and he can help the auctioneer to decide the winners and compute their charges. In our design, the auctioneer generates a public key and a secret key of Paillier's homomorphic cryptosystem. Bidders encrypt their bids by using the public key. Then, the agent performs homomorphic computation on the ciphertexts, adds random numbers, and sends the results to the auctioneer for making allocation decision and computing payment of winners. By this design, the privacy is protected without affecting the correctness of the auctions.

Although there exists a PTAS for the IA model, it is considered as a very challenging work to design a privacy preserving version of PTAS. To this end, we propose a privacy preserving bid mechanism with an approximation factor of 2. For the combinatorial auction, we give a privacy preserving version of the auction mechanism proposed in [5], which has an approximation factor of $\sqrt{h}$. We prove that our new method for combinatorial auction can protect both the bid value of all bidders and the items each loser wants to buy. To the best of our knowledge, the auction mechanisms presented in this paper are the first strategyproof and privacy preserving multi-unit auction mechanisms with social efficiency performance guarantee.

2 Preliminaries

2.1 Auction Model

We consider a sealed-bid auction, in which there exist an auctioneer, a set of bidders, and an agent. At the beginning of the auction, all bidders first encrypt their bids by using the public key generated from the agent, and then submit their encrypted bids to the auctioneer. Next, the auctioneer allocates the items to the bidders, and decides the charges for the winners after communicating with the agent. We assume that the agent is a *semi-trusted* third party, who is curious about the bid values of bidders, but will not collude with the auctioneer.

We study two auction models in this paper: the Identical items Auction model (*e.g.* IA model) and the distinct items auction model (*a.k.a* Combinatorial

Auction model, CA model). In the IA model, we assume that there exist a set of identical items denoted as $\mathcal{I} = \{I_1, I_2, \ldots, I_h\}$, and m bidders denoted by $\mathcal{B} = \{1, 2, \ldots, m\}$ in the market. Each bidder i is only interested in a fixed number of items, denoted by N_i, and is willing to pay *no more than* v_i for all of them. In the CA model, the items in the market are distinct, and each bidder $i \in \mathcal{B}$ wants to buy the items in a specified subset $c_i \subseteq \mathcal{I}$. Note that both in the IA model and the CA model, the demand of each bidder is inseparable, which means that bidder i will get all the items that he wants to buy if he wins.

2.2 Auction Goals

Our primary goal is to design a strategyproof auction mechanism which can maximize the social efficiency. We define the *social efficiency* of an auction as the total bid values of the winning bidders. Suppose b_i, v_i, p_i, are the bid value, true valuation, and the payment of bidder i for all the items he want to buy, respectively. Then, the utility of bidder i is defined as

$$u_i = \begin{cases} v_i - p_i & \text{if bidder } i \text{ wins the auction} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

Strategyproofness is often regarded as one of the most crucial properties of auction mechanisms. We say an auction is strategyproof if bidding truthfully is the *dominant strategy* for each bidder. Therefore, we need to prove that for each bidder i, u_i is maximized when $b_i = v_i$ to ensure the strategyproofness of bidders. It has been proved by Myerson that an auction is strategyproof if and only if the following two conditions hold:

- **Bid-monotone Constraint:** The items allocation mechanism is bid-monotone, which means that, when bidder i wins the auction by bidding b_i, he will always win by bidding $b_i' > b_i$.
- **Critical Value Constraint:** The charge from a winner i is his critical value, *i.e.*, the minimum bid that he will win the auction.

Following this direction, we design the strategyproof auction mechanisms satisfying the above-mentioned characteristics.

The privacy goals of our auction mechanisms are as follows:

- In the IA model, we protect the bid values of bidders, which means that all bids from bidders are blind to both the auctioneer and the agent.
- In the CA model, neither the auctioneer nor the agent knows the true bid values of bidders, as well as which items that each loser wants to get.

3 IAMP: Identical Items Auction Mechanism Design with Privacy Preservation

In this section, we design a strategyproof mechanism IAMP for Identical items Auction model (IA model), which achieves an approximately optimal social efficiency and supports privacy preservation. Our auction mechanism mainly consists of three steps: bidding, allocation and payment calculation.

3.1 Bidding

Before running the auction, the agent first generates an encryption key EK and a decryption key DK of Paillier's cryptosystem. Then, he publishes EK as a public key, and keeps DK in private. We assume that the parameter n is of 1024-bit length in this work. Each bidder i encrypts his bid b_i to $E(b_i)$, and sends $(E(b_i), N_i)$ to the auctioneer, where N_i is the number of items that he wants to buy.

3.2 Allocation Mechanism

After receiving the encrypted bids from the bidders, the auctioneer needs to make the winner decision aiming at maximizing the social efficiency. We can prove that the social efficiency maximization problem can be reduced to the Knapsack problem, which is a well known NP-hard problem.

To address this NP hardness, a Polynomial Time Approximation Scheme (PTAS) was proposed in [12] for knapsack problem, which is also suitable for our model. Besides, it has been proven that this PTAS is bid-monotone, which implies that there exists a strategyproof auction mechanism. Unfortunately, it is really a hard work to design a bid privacy preservation version based on this mechanism. There is a large computation and comparison overload in this PTAS based on dynamic programming. Therefore, we build our privacy preserving method on the top of another approximation algorithm which can approximate the optimal allocation within a factor of 2.

Next, we will show the detail of our allocation mechanism with privacy preserving. Following the approximation algorithm above, we need to sort the per-unit bid values of bidders to decide the winners. To solve this with privacy preserving, bidders first encrypt their bids by using the Encryption Key (EK) of the agent, and submit the encrypted bids to the auctioneer. Then, the auctioneer masks them by using two random values $\delta_1 \in \mathbb{Z}_{2^{\gamma_1}}$ and $\delta_2 \in \mathbb{Z}_{2^{\gamma_2}}$ as $\delta_1 b_i + \delta_2 N_i$. Note that the range $[1, 2^{\gamma_1}]$ and $[1, 2^{\gamma_2}]$ for δ_1 and δ_2 should be chosen based on the consideration of the correctness of modular operations: $\delta_1 b_i + \delta_2 N_i$ should be smaller than the modulo used in Paillier's system. Since the agent has the decryption key, he can compute and sort $\delta_1 \frac{b_i}{N_i} + \delta_2$ in the non-increasing order without access any true bid values of bidders.

Furthermore, the auctioneer also maps the true ID of bidders by using a permutation before sending $\{E(\delta_1 b_i + \delta_2 N_i), N_i\}_{i \in \mathcal{B}}$ to the agent. Thus, the agent cannot map the masked bids $\{\delta_1 b_i + \delta_2 N_i\}_{i \in \mathcal{B}}$ to bidders either. With the sorted per-unit bids, the agent can find the bidders with top $k-1$ per-unit bids and the bidder with k-th per-unit bid. After the agent sends the permutated ID of bidders with top k per-unit bids to the auctioneer, the auctioneer can compute the encrypted bid sum of bidders with top $k-1$ per-unit bids. Since the agent has the decryption key, the auctioneer then randomly chooses two integers δ_3 and δ_4 to hide the true value of $E(\sum_{i=1}^{k-1} b_{\sigma(i)})$ and $E(b_{\sigma(k)})$, and communicates with the agent to decide the winning bidders. The detail of our allocation mechanism with privacy preserving is depicted in Algorithm 1.

Algorithm 1. Allocation mechanism for identical items model

1: The auctioneer randomly picks two integers $\delta_1 \in \mathbb{Z}_{2^{1012}}$, $\delta_2 \in \mathbb{Z}_{2^{1022}}$, and executes the homomorphic operation:

$$E(\delta_1 b_i + \delta_2 N_i) = E(b_i)^{\delta_1} E(\delta_2 N_i).$$

2: Then, the auctioneer maps the ID of bidders by using permutation $\pi : \mathbb{Z}_m \to \mathbb{Z}_m$, and sends $\{E(\delta_1 b_i + \delta_2 N_i), N_i, \pi(i)\}_{i \in \mathcal{B}}$ to the agent.

3: The agent decrypts $E(\delta_1 b_i + \delta_2 N_i)$ by using his private key $DK = (\lambda, \mu)$, then computes $\delta_1 \frac{b_i}{N_i} + \delta_2$ and sorts b_i/N_i in non-increasing order.

4: The agent finds the critical bidder $\sigma(k)$ by computing:

$$\sum_{i=1}^{k-1} N_{\sigma(i)} \leq h \leq \sum_{i=1}^{k} N_{\sigma(i)}.$$

5: To decide the winners, the agent sends $(\{\sigma(i)\}_{i<k}, \sigma(k))$ to the auctioneer, where $\{\sigma(i)\}_{i<k}$ is out of order.

6: The auctioneer randomly picks two integers $\delta_3 \in \mathbb{Z}_{2^{1012}}$, $\delta_4 \in \mathbb{Z}_{2^{1022}}$, computes the following and sends the result back to the agent.

$$E(\delta_3 \sum_{i=1}^{k-1} b_{\sigma(i)} + \delta_4) = (\prod_{i=1}^{k-1} E(b_{\sigma(i)}))^{\delta_3} E(\delta_4)$$
$$E(\delta_3 b_{\sigma(k)} + \delta_4) = E(b_{\sigma(k)})^{\delta_3} E(\delta_4)$$

7: After receiving the ciphertexts, the agent decrypts them , and sends $\{\sigma(i)\}_{i<k}$ to the auctioneer if $\sum_{i=1}^{k-1} b_{\sigma(i)} \geq b_{\sigma(k)}$; otherwise, he sends $\sigma(k)$ to the auctioneer.

8: The auctioneer chooses the bidders that the agent sends to him as winners, and sets other bidders as losers.

Then, we will show that our allocation mechanism for identical items auction model is bid monotone.

Lemma 1. *The proposed allocation mechanism is bid-monotone, which means that if bidder $\sigma(i)$ wins by bidding $b_{\sigma(i)}$, he will always win by bidding $b'_{\sigma(i)} > b_{\sigma(i)}$.*

Proof. Due to page limits, the proof is referred to [18].

3.3 Payment Calculation Mechanism

It has been proved that an auction is strategyproof if and only if its winner determination mechanism is bid monotone and it always charges each winner its critical value. We have proved that our allocation mechanism is bid-monotone, which indicates that there exists a critical value for each winner. Hence, the objective of this step is to compute the critical values of winners with privacy preserving.

Since our allocation mechanism is bid monotone, there must exist some intervals denoted by $[L_i, U_i]$, which satisfies that bidder $\sigma(i)$ wins the auction as long as his per-unit bid value is larger than the L_i-th per-unit bid value in the sorted bid list and always loses if his per-unit bid value is less than the U_i-th per-unit bid value. We say $[L_i^*, U_i^*]$ is the critical interval of winner $\sigma(i)$ if $L_i^* = U_i^* - 1$. It is not hard to get that i is the lower bound of L_i^*, and f is the upper bound of U_i^* which satisfies:

$$\sum_{i=1}^{f-1} N_{\sigma(i)} \leq h \leq \sum_{i=1}^{f} N_{\sigma(i)} \tag{2}$$

Obviously, the critical value of each winner $\sigma(i)$ is less than the L_i^*-th bid value, while larger than the U_i^*-th bid value. In order to find the critical value of each winner, we first compute their critical intervals. As shown in Algorithm 2, we use binary search to compute the critical interval for each winner $\sigma(i)$. In each round of the binary search, we set the per-unit bid of bidder $\sigma(i)$ being equal to the per-unit bid of the M-th bidder in the sorted list, and then compare the bid sum of new top $k-1$ bids and the k-th bid, to check whether $\sigma(i)$ with the new bid value will win or not. This can be done since the auctioneer can compute the encrypted value $E(b_{\sigma(M)}N_{\sigma(i)})$, which is equal to $E(b_{\sigma(i)}N_{\sigma(M)})$, and further, the auctioneer can get the encrypted values of $E(\sum_{j=1}^{k-1} b_{\sigma(j)^*}N_{\sigma(M)})$ and $E(b_{\sigma(k)^*}N_{\sigma(M)})$ through homomorphic operations. With these encrypted values, the agent can check whether bidder $\sigma(i)$ win or not, by decrypting and comparing the values $\sum_{j=1}^{k-1} b_{\sigma(j)^*}$ and $b_{\sigma(k)^*}$. Then, the agent can get the new boundary of binary search, until he finds the critical interval of bidder $\sigma(i)$.

After getting the critical interval of each winner, we compute the critical values for them. For the case that winner $\sigma(i)$ is the new k-th bidder, and his per-unit bid value is smaller than the L_i^*-th, but larger than the U_i^*-th per-unit bid value in the sorted list, we compute the critical value $p_{\sigma(i)}$ of winner $\sigma(i)$ as follow:

$$p_{\sigma(i)} = \max(\sum\nolimits_{j=1}^{k-1} b_{\sigma(j)^*}, \frac{b_{\sigma(U_i^*)}N_{\sigma(i)}}{N_{\sigma(U_i^*)}})$$

In the other case, the critical value of winner $\sigma(i)$ is

$$p_{i'} = \max(b_{\sigma(k)^*} + b_{\sigma(i)} - \sum\nolimits_{j=1}^{k-1} b_{\sigma(j)^*}, \frac{b_{\sigma(U_i^*)}N_{\sigma(i)}}{N_{\sigma(U_i^*)}})$$

Assume that $s_1 = \sum_{j=1}^{k-1} b_{\sigma(j)^*}$, and $s_2 = b_{\sigma(U_i^*)}N_{\sigma(i)}$, $s_3 = b_{\sigma(k)^*} + b_{\sigma(i)}$. The details of our payment calculation mechanism with privacy preservation are described in Algorithm 3.

We have proved that our allocation mechanism is bid monotone, and we charge each winner its critical value, thus we can also get that:

Theorem 1. *The auction mechanism we proposed is strategyproof.*

Since the goal of this work is to design strategyproof auction mechanism with privacy preserving, we will show that the proposed IAMP protects the true bid values of bidders in the next subsection.

Algorithm 2. Compute the critical interval for winner $\sigma(i)$

1: The agent first computes the interval of the binary search $[i, f]$, and sets $L = i$, $U = f$ at the beginning. Then, he sets $M = \lfloor (U + L)/2 \rfloor$.
2: The agent sends the IDs $(\{\sigma(j)^*\}_{j<k}, \sigma(M), \sigma(k)^*)$ to the auctioneer, where $\{\sigma(j)^*\}_{j<k}$ is out of order, $\sigma(j)^*)$ and $\sigma(k)^*)$ are the new bidders with the j-th and k-th per-unit bid value when $\sigma(i)$ bids $\frac{b_{\sigma(M)}N_{\sigma(i)}}{N_{\sigma(M)}}$, respectively.
3: The auctioneer first sets the bid of bidder $\sigma(i)$ in this round of binary search by setting $E(b_{\sigma(i)}N_{\sigma(M)})$ as:

$$E(b_{\sigma(i)}N_{\sigma(M)}) = E(b_{\sigma(M)})^{N_{\sigma(i)}}.$$

4: Then, he randomly chooses two integers $\delta_{M,1} \in \mathbb{Z}_{2^{1012}}$, $\delta_{M,2} \in \mathbb{Z}_{2^{1022}}$, computes the follows and sends the results back to the agent.

$$E(\delta_{M,2}N_{\sigma(M)} + \delta_{M,1}\sum_{j=0}^{k-1} b_{\sigma(j)^*}N_{\sigma(M)}) = E(\delta_{M,2}N_{\sigma(M)})E(b_{\sigma(k)^*})^{N_{\sigma(M)}\delta_{M,1}}$$

5: The agent decrypts the ciphertexts he received and checks bidder $\sigma(i)$ win or not by bidding $\frac{b_{\sigma(M)}N_{\sigma(i)}}{N_{\sigma(M)}}$, then he executes the following operation.
6: **if** $\sigma(i)$ wins by bidding $\frac{b_{\sigma(M)}N_{\sigma(i)}}{N_{\sigma(M)}}$ **then**
7: The agent sets $L = M$, and $M = \lfloor (U + L)/2 \rfloor$;
8: **else**
9: The agent sets $U = M$, and $M = \lfloor (U + L)/2 \rfloor$;
10: Repeat step $2 \sim 8$ until $U = L + 1$.
11: The agent sets $U_i^* = U$, and $L_i^* = L$, then $[L_i^*, U_i^*]$ is the critical interval of winner $\sigma(i)$.

3.4 Security Analysis

The most important target of our auction mechanism is to protect the bid values of bidders. There are two central parties in our mechanism, including the auctioneer and the agent. In the following, we will show that the bid values of bidders are blind for both the auctioneer and the agent.

Theorem 2. *Our auction mechanism for identical items guarantees the bid privacy preserving.*

Proof. Due to page limits, the proof is referred to [18].

Algorithm 3. Payment calculation for winner $\sigma(i)$

1: **if** $\sigma(i) = \sigma(k)^*$ **then**

2: The auctioneer randomly chooses two integers $\delta_5 \in \mathbb{Z}_{2^{1012}}$, $\delta_6 \in \mathbb{Z}_{2^{1022}}$, computes the follows and sends the results to the agent.

$$E(\delta_6 + \delta_5 s_1) = E(\delta_6)(\prod_{j=0}^{k-1} E(b_{\sigma(j)^*}))^{\delta_5}$$

$$E(\delta_6 N_{\sigma(U_i^*)} + \delta_5 s_2) = E(\delta_6 N_{\sigma(U_i^*)}) E(b_{\sigma(U_i^*)})^{\delta_5 N_{\sigma(i)}}$$

3: The agent computes and sends $p'_{\sigma(i)}$ to the auctioneer, where

$$p'_{\sigma(i)} = \max(\delta_6 + \delta_5 s_1, \delta_6 + \delta_5 s_2 / N_{\sigma(U_i^*)}).$$

4: **else**

5: The auctioneer randomly chooses two integers $\delta_5 \in \mathbb{Z}_{2^{1012}}$, $\delta_6, \delta_7 \in \mathbb{Z}_{2^{1022}}$, computes the follows and sends the results to the agent.

$$E(\delta_6 + \delta_5 s_3) = E(\delta_6)(E(b_{\sigma(k)^*}) E(b_{\sigma(i)}))^{\delta_5}$$

$$\begin{aligned} &E(\delta_6 N_{\sigma(U_i^*)} + \delta_5 (s_2 + s_1 N_{\sigma(U_i^*)}) \\ &= E(\delta_6 N_{\sigma(U_i^*)}) (E(b_{\sigma(U_i^*)}) E(\prod_{j=0}^{k-1} E(b_{\sigma(j)^*})))^{\delta_5 N_{\sigma(i)}} \end{aligned}$$

$$E(\delta_7 + \delta_5 s_1) = E(\delta_7) E(\prod_{j=0}^{k-1} E(b_{\sigma(j)^*}))^{\delta_5}$$

6: After receiving the ciphertext, the agent computes $p'_{\sigma(i)}$ and sends it to the auctioneer, where

$$p'_{\sigma(i)} = \max(\delta_6 - \delta_7 + \delta_5 (s_3 - s_1), \delta_6 - \delta_7 + \delta_5 s_2 / N_{\sigma(U_i^*)}).$$

7: The auctioneer sets the payment of winner i' is $p_{i'}$, where

$$p_{i'} = (p'_{i'} - \delta_6 + \delta_7)/\delta_5.$$

4 CAMP: Combinatorial Auction Mechanism Design with Privacy Preservation

4.1 Bidding

Similar to the bidding process in IAMP, the agent first generates encryption and decryption keys of Paillier's cryptosystem, and publishes his encryption key. Then, each bidder encrypts $b_i/\sqrt{|c_i|}$ by using the encryption key of the agent and sends the results to the auctioneer. However, every bidder not only wants to protect his bid in our combinatorial auction model (CA model), but

also wants to hide the items that he wants to buy if he loses in the auction. Thus, each bidder will also encrypt the set of items that he wants to buy. Let $X_i = \{x_{i,1}, x_{i,2}, \ldots, x_{i,h}\}$ be the demand vector of bidder i, where $x_{i,j} = 1$ if $I_j \in c_i$, $x_{i,j} = 0$ otherwise. For each $x_{i,j} \in X_i$, bidder i generates a random integer r and encrypts $x_{i,j}$ by using the encryption key of the agent. Finally, bidder i sends $(E(b_i/\sqrt{|c_i|}), E(X_i))$ to the auctioneer, where $E(X_i) = \{E(x_{i,1}), E(x_{i,2}), \ldots, E(x_{i,h})\}$.

4.2 Allocation Mechanism

After receiving the encrypted bids and demands from the bidders, the auctioneer chooses a set of bidders as winners if the social efficiency is maximized. It has been proven in [5] that the social efficiency maximization problem in the combinatorial auction is NP hard, and the upper bound of approximation ratios of polynomial time algorithms is $\sqrt{h}$.

Dong *et al.* propose an auction mechanism with a greedy allocation mechanism in [5], which can approximate the optimal one within a factor of $\sqrt{h}$. We will briefly describe it below:

- First, a normalized bid $\frac{b_i}{\sqrt{|c_i|}}$ for each bid b_i is calculated, and then the bidders are sorted according to the non-increasing order of the normalized bids.
- Finally, the greedy allocation mechanism examines every bidder in the sorted list sequentially, and grants the bidder only if his demand does not overlap with all the demands of the previously granted bidders.
- Assume $l(i)$ is the first bidder following i in the sorted list that has been denied but have been granted were it not for the presence of i. Then, the bidder i pays zero if his bid is denied or $l(i)$ does not exist; otherwise, he pays $\sqrt{|c_i|} * n_{l(i)}$, where $n_{l(i)}$ is the normalized bid of bidder $l(i)$.

Following the combinatorial auction mechanism stated above, only two operations rely on the true bid values of bidders: sorting the bidders according to their normalized bids and computing the payment for each winner i by using the normalized bid of $l(i)$. Thus, we can use the similar way as what we did in IAMP to protect the bid privacy of bidders. However, the agent needs to know the demand vectors of all the bidders to check if they are overlapping with each other in combinatorial auction. Therefore, the most challenging issue of designing privacy preserving combinatorial auction mechanism is to protect the demand of losers. To deal with this challenge, we encrypt the demand vector of bidders. More specifically, we confuse the ID of bidders and the ID of items by separately using permutations $\pi_1 : \mathbb{Z}_m \to \mathbb{Z}_m$ and $\pi_2 : \mathbb{Z}_h \to \mathbb{Z}_h$, before the auctioneer send the demand vectors to the agent. With the confused information and decryption key, the agent can also get the overlapping information of bidders, but can hardly map them to the true demands of losers. On the other hand, the auctioneer only gets the encrypted demand vectors and the auction result, he has no idea with the demand of each loser either. Then, the demand privacy of losers are protected. The detail of our allocation mechanism with privacy preserving is shown in Algorithm 4.

Algorithm 4. Allocation mechanism for combinatorial auction

1: The auctioneer randomly picks two integers $\delta_1 \in \mathbb{Z}_{2^{1012}}$, $\delta_2 \in \mathbb{Z}_{2^{1022}}$, and executes the following homomorphic operation, then he sends $\{\pi_1(i), E(\delta_1 \frac{b_i}{\sqrt{|c_i|}} + \delta_2), \{E(x_{i,j}), \pi_2(j)\}_{I_j \in \mathcal{I}}\}_{i \in \mathcal{B}}$ to the agent.

$$E(\delta_1 \frac{b_i}{\sqrt{|c_i|}} + \delta_2) = E(\frac{b_i}{\sqrt{|c_i|}})^{\delta_1} E(\delta_2)$$

2: The agent decrypts the set of bids $\{E(\delta_1 \frac{b_i}{\sqrt{|c_i|}} + \delta_2)\}_{i \in \mathcal{B}}$ by using his private key, and reorder them in descending order.
3: The agent decrypts the demand of bidders, and computes the winners as follows:
4: Set $W = \mathcal{B}$
5: **for** $i = 1$ to m **do**
6: Set $j = 1$
7: **while** $j \leq h$ and $\sigma(i) \in W$ **do**
8: **if** $x_{\sigma(i),j} = 1$ and $\sum_{k=1}^{i-1} x_{\sigma(k),j} \geq 1$ **then**
9: Set $W = W \setminus \{\sigma(i)\}$
10: Set $j = j + 1$
11: The agent sends the set W of winners to the auctioneer.

4.3 Payment Calculation Mechanism

Recall that an auction is strategyproof if and only if it is bid-monotone and always charges each winner its critical value. For each winner i in the greedy allocation mechanism, his normalized bid is larger than the normalized bid of $l(i)$. Thus, $n_{l(i)} * \sqrt{|c_i|}$ is the critical value of winner i if $l(i)$ exist. Otherwise, the critical value of winner i is zero. Our payment calculation mechanism is shown in Algorithm 5.

Algorithm 5. Payment calculation for combinatorial auction

1: For each winner $i \in W$, the agent first finds $l(i)$ and then computes p_i' as follows:

$$p_i' = \begin{cases} \delta_1 \frac{b_{l(i)}}{\sqrt{|c_{l(i)}|}} + \delta_2 & \text{if } l(i) \text{ exist} \\ 0 & \text{otherwise} \end{cases}$$

2: The agent sends the set $\{p_i', X_i, \pi(i)\}_{i \in W}$ to the auctioneer.
3: The auctioneer computes the payment for each winner as follows:

$$p_i = \max(\sqrt{|c_i|}(p_i' - \delta_2)/\delta_1, 0).$$

Theorem 3. *Our combinatorial auction mechanism protects the demand c_i of each loser i.*

Proof. Due to page limits, the proof is referred to [18].

Theorem 4. *Our combinatorial auction mechanism guarantees the bid privacy preserving.*

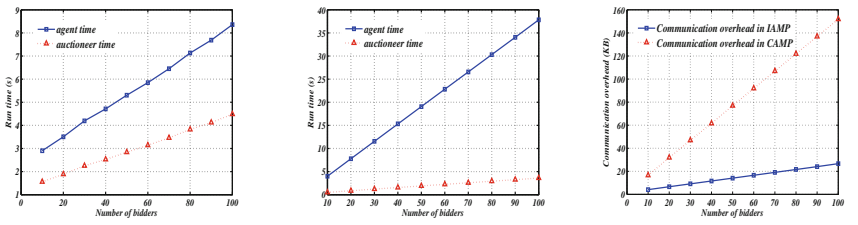
Proof. Due to page limits, the proof is referred to [18].

5 Simulation Results

We evaluate the computation and communication overhead of our approximation algorithms with privacy preserving. Since computation overhead is dominated by the auctioneer and the agent in both auction models, we do not plot the bidders' computation overhead. As shown in Fig. 1, the auctioneer spends more time in the identical auction model than in the combinatorial auction model. This is because auctioneer spends most of his time in computing the payment of winners. However, we can easily find them in the combinatorial auction model.

The run time of each bidder is roughly 30 ms in the identical auction model. However, bidders need to encrypt their bids and demand in the combinatorial auction model. Thus, the run time of the agent or a bidder is related to the number of items in the combinatorial auction. Our simulation results show that the run time of each bidder is roughly 180 ms in CAMP when $h = 5$, and the run time of the agent is much more than that in IAMP.

In the evaluation, we set n to be of 1024-bit length. Figure 1c shows the communication overhead of our auction mechanisms with privacy preserving. We find that the communication overhead of CAMP is much higher than that of IAMP. The main reason is that bidders only encrypt their bids in the identical auction, but encrypt both their bids and demands in the combinatorial auction.



(a) Run time of IAMP (b) Run time of CAMP (c) Communication cost

Fig. 1. Computation and communication overhead when $h = 5$

6 Conclusion

In this paper, we proposed the first strategyproof and privacy preserving multi-unit auction mechanisms that maximize the social efficiency. We study two cases for multi-unit auction, where the items in the market are identical and distinct.

Under these two cases, the optimal item allocation problem is NP hard to solve. Thus, we designed secure and near optimal allocation mechanisms for them, which have the approximation factors of 2 and $\sqrt{h}$, respectively. Further, we also computed the critical payment with privacy preserving for each winner, and theoretically proved the properties of our auction mechanisms, such as strategyproofness, privacy preserving and approximation factor. Our evaluation results demonstrated that our protocols not only achieve good social efficiency, but also perform well at computation and communication.

Acknowledgements. This work is partially supported by National Natural Science Foundation of China (NSFC) under Grant No. 61572342, No. 61303206, Natural Science Foundation of Jiangsu Province under Grant No. BK20151240, China Postdoctoral Science Foundation under Grant No. 2015M580470. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of author(s) and do not necessarily reflect the views of the funding agencies (NSFC).

References

1. Chen, D., Yin, S., Zhang, Q., Liu, M., Li, S.: Mining spectrum usage data: a large-scale spectrum measurement study. In: ACM Mobicom 2009, pp. 13–24 (2009)
2. Chung, Y.F., Huang, K.H., Lee, H.H., Lai, F., Chen, T.S.: Bidder-anonymous English auction scheme with privacy and public verifiability. J. Syst. Softw. **81**(1), 113–119 (2008)
3. Cramton, P., Shoham, Y., Steinberg, R.: Combinatorial Auctions, vol. 475. MIT Press, Cambridge (2006)
4. Dobzinski, S., Nisan, N., Schapira, M.: Approximation algorithms for combinatorial auctions with complement-free bidders. In: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing (STOC), pp. 610–618 (2005)
5. Dong, M., Sun, G., Wang, X., Zhang, Q.: Combinatorial auction with time-frequency flexibility in cognitive radio networks. In: IEEE INFOCOM 2012, pp. 2282–2290 (2012)
6. Dong, W., Rallapalli, S., Jana, R., Qiu, L., Ramakrishnan, K., Razoumov, L., Zhang, Y., Cho, T.W.: iDEAL: incentivized dynamic cellular offloading via auctions. IEEE/ACM Trans. Netw. (TON) **22**(4), 1271–1284 (2014)
7. Gopinathan, A., Li, Z.: Strategyproof auctions for balancing social welfare and fairness in secondary spectrum markets. In: IEEE INFOCOM 2011, pp. 3020–3028 (2011)
8. Huang, H., Sun, Y.-E., Li, X.-Y., Chen, Z., Yang, W., Xu, H.: Near-optimal truthful spectrum auction mechanisms with spatial and temporal reuse in wireless networks. In: ACM MobiHoc 2013, pp. 237–240 (2013)
9. Huang, Q., Tao, Y., Wu, F.: Spring: a strategy-proof and privacy preserving spectrum auction mechanism. In: IEEE INFOCOM 2013, pp. 827–835 (2013)
10. Kikuchi, H.: (M+1)st-price auction protocol. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **85**(3), 676–683 (2002)
11. Krishna, V.: Auction Theory. Academic Press, San Diego (2009)
12. Lai, K., Goemans, M.X.: The knapsack problem, fully polynomial time approximation schemes (FPTAS) (2006). Accessed 3 Nov 2012

13. Lehmann, D., Oćallaghan, L., Shoham, Y.: Truth revelation in approximately efficient combinatorial auctions. J. ACM (JACM) **49**(5), 577–602 (2002)
14. Lin, W.-Y., Lin, G.-Y., Wei, H.-Y.: Dynamic auction mechanism for cloud resource allocation. In: 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid), pp. 591–592 (2010)
15. Pan, M., Li, H., Li, P., Fang, Y.: Dealing with the untrustworthy auctioneer in combinatorial spectrum auctions. In: IEEE GLOBECOM 2011, pp. 1–5 (2011)
16. Pan, M., Zhu, X., Fang, Y.: Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer. Wirel. Netw. **18**(2), 113–128 (2012)
17. Rothkopf, M.H., Pekeč, A., Harstad, R.M.: Computationally manageable combinational auctions. Manag. Sci. **44**(8), 1131–1147 (1998)
18. Sun, Y.-E., Huang, H., Li, X.-Y., et al.: Privacy-preserving strategyproof auction mechanisms for resource allocation in wireless communications. Technical report, Soochow University, June 2016. http://home.ustc.edu.cn/~huang83/bigcom.pdf
19. Wang, X., Huang, L., Xu, H., Huang, H.: Truthful auction for resource allocation in cooperative cognitive radio networks. In: IEEE ICCCN 2015, pp. 1–8 (2015)
20. Wang, X., Li, Z., Xu, P., Xu, Y., Gao, X., Chen, H.-H.: Spectrum sharing in cognitive radio networks an auction-based approach. IEEE Trans. Syst. Man Cybern. Part B Cybern. **40**(3), 587–596 (2010)
21. Zhou, X., Gandhi, S., Suri, S., Zheng, H.: eBay in the Sky: strategy-proof wireless spectrum auctions. In: ACM Mobicom 2008, pp. 2–13 (2008)

http://www.springer.com/978-3-319-42552-8

Big Data Computing and Communications
Second International Conference, BigCom 2016,
Shenyang, China, July 29-31, 2016. Proceedings
Wang, Y.; Yu, G.; Zhang, Y.; Han, Z.; Wang, G. (Eds.)
2016, XVI, 466 p. 201 illus., Softcover
ISBN: 978-3-319-42552-8