Tsinghua Science and Technology

Volume 22 | Issue 2 Article 1

2017

Privacy-Preserving Strategyproof Auction Mechanisms for Resource Allocation

Yu-E Sun
School of Urban Rail Transportation, Soochow University, Suzhou 215006, China.

He Huang
School of Computer Science and Technology, Soochow University, Suzhou 215006, China.

Xiang-Yang Li
School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China.

Yang Du
School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China.

Miaomiao Tian
School of Computer Science and Technology, Anhui University, Hefei 230031, China.

See next page for additional authors

Privacy-Preserving Strategyproof Auction Mechanisms for Resource Allocation

Authors

Yu-E Sun, He Huang, Xiang-Yang Li, Yang Du, Miaomiao Tian, Hongli Xu, and Mingjun Xiao

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 01/09 pp119–134
Volume 22, Number 2, April 2017

Privacy-Preserving Strategyproof Auction Mechanisms for Resource Allocation

Yu-E Sun, He Huang*, Xiang-Yang Li, Yang Du, Miaomiao Tian, Hongli Xu, and Mingjun Xiao

Abstract: In recent years, auction theory has been extensively studied and many state-of-the-art solutions have been proposed aiming at allocating scarce resources. However, 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. Besides the privacy-preserving issue, the performance guarantee of social efficiency maximization is also crucial for auction mechanism design. In this paper, we study the auction mechanisms that consider the above two aspects. We discuss two multi-unit auction models: the identical multiple-items auction and the distinct multiple-items auction. Since the problem of determining a multi-unit auction mechanism that can maximize its social efficiency is NP-hard, we design a series of nearly optimal multi-unit auction mechanisms for the proposed models. We prove that the proposed auction mechanisms are strategyproof. Moreover, we also prove that the privacy of bid value from each bidder can be preserved in the auction mechanisms. To the best of our knowledge, this is the first work on the strategyproof multi-unit auction mechanisms that simultaneously consider privacy preservation and social efficiency maximization. The extensive simulations show that the proposed mechanisms have low computation and communication overheads.

Key words: approximation mechanism; multi-unit auction; privacy preserving; social efficiency; strategyproof

1 Introduction

Resource allocation is one of the most important issues in many areas. Typical examples include the virtual machine resource allocation in cloud computing, spectrum resource allocation in wireless communications, and so on. Since an auction is a fair and efficient resource allocation in the real world, it has also been introduced into the networking area, especially for scarce resource allocations. By far, many auction mechanisms have been designed for different resource allocation problems, such as the computing resources in the cloud[1], spectrum licenses[2–4], cellular networks[5], and CRNs[6].

Strategyproofness (a.k.a., *truthfulness*) is regarded as one of the key objectives in the auction mechanism design, which means that the optimal strategy for bidders is to bid their *true valuations* of the items for sale. Most of the auction mechanisms are designed to charge each winner a minimum bid value, by which she can win the auction, to ensure the strategyproofness of the bidders[7]. 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 it to maximize his profits. For

• Yu-E Sun is with School of Urban Rail Transportation, Soochow University, Suzhou 215006, China.
• He Huang is with School of Computer Science and Technology, Soochow University, Suzhou 215006, China. E-mail: huangh@suda.edu.cn.
• Xiang-Yang Li, Yang Du, Hongli Xu, and Mingjun Xiao are with School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China.
• Yu'e Sun, He Huang, Yang Du, Hongli Xu, and Mingjun Xiao are also with Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou 215123, China.
• Miaomiao Tian is with School of Computer Science and Technology, Anhui University, Hefei 230031, China.
∗ To whom correspondence should be addressed.
Manuscript received: 2016-08-25; revised: 2017-02-08: accepted: 2017-02-13

instance, suppose you value some items at \$100, and submit the true valuation to the auctioneer in a sealed-bid auction. Actually, the minimum bid value that you will win in the auction is \$50. However, the auctioneer is willing to charge you \$99 to maximize the profits, instead of charging you \$50 for strategyproofness. In this situation, will you still submit your true valuation to the auctioneer?

To address the above problem, the bid values should be hidden throughout 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 to privacy preservation. For instance, in Refs. [8, 9], the authors designed mechanisms to protect the bid value in the first-price and the second-price sealed-bid auctions. Huang et al.[10] proposed a strategyproof and bid privacy-preserving auction mechanism for spectrum allocation. Pan et al.[11, 12] gave a secure combinatorial spectrum auction by using homomorphic encryption to deal with the untrustworthy auctioneer. However, none of these privacy-preserving auction mechanisms provided any performance guarantee on *social efficiency*, i.e., the total bid value of winners, which is a standard and critical auction metric[13, 14].

In this paper, we focus on the privacy-preserving and strategyproof auction mechanism design for resource allocation, which can simultaneously maximize the social efficiency. We observe that most of the existing auction mechanisms fail to consider the multiple-items trading. Nevertheless, bidders in practical applications may often express their preferences for a specified number of items or some specified bundles of items, instead of an individual item. This kind of auction is called as the *multi-unit auction*. There are two types of multi-unit auctions, in which the items to be sold are *identical* or *distinct*. In this paper, we will propose two auction mechanisms to manage the identical case and the distinct case, respectively. For the identical case, the demand of each bidder is a fixed number of items, which is inseparable. For example, if a cloud computing job requires 35 time slices, the bidder must auction off at least 35 time slices. It is meaningless to win an auction with less than 35 time slices. The auction of distinct items is also known as a *combinatorial auction*. In a combinatorial auction, all bidders can bid for bundles of items rather than individual items[15]. For instance, if a user wants to run a cloud application by using 130 CPUs and 8 GB of storage from 8AM to 10AM, the user will only be interested in the entire bundle of resources for meeting the demand. In addition, the bid value and the required items of each bidder are private and sensitive information of auctions, since the auctioneer might raise the price in future auctions to maximize the profit after learning these information. Hence, we need to protect the privacy of these sensitive information throughout the whole auction. Meanwhile, we also need to let the auctioneer know each winner's demand so that the auction can be completed.

Designing a multi-unit auction mechanism with the maximum social efficiency is an NP-hard problem[16]. Many efficient approximation algorithms have been proposed for both the Identical items Auction model (IA model) and Combinatorial Auctions model (CA model). For example, there is a Polynomial Time Approximation Scheme (PTAS), which is suitable for the IA auction model, as well as an approximation algorithm with an approximation factor of $\sqrt{h}$ that has been proved to be a tight one for the CA. Our work is not to design approximation algorithms to improve the performance of the existing studies, but to construct the mechanisms with privacy preservation, 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 while guaranteeing high performance is very challenging. To tackle this problem, we introduce an agent into our auction model, which is a *semi-trusted* third-party and 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 an allocation decision and computing the payment of the winners. Such a design ensures the privacy protection without affecting the correctness of the auctions. Moreover, the extra costs incurred by this design are negligible. The whole auction mechanisms still have low computation and communication overheads.

Although there exists a PTAS for the IA model, it is a very challenging work to design a privacy-

preserving version of PTAS. We propose a privacy-preserving bid mechanism with an approximation factor of 2. For the combinatorial auction, we provide a privacy-preserving version of the auction mechanism proposed in Ref. [17], which has an approximation factor of $\sqrt{h}$. We prove that our new method for CA can protect both the bid values of all bidders and the items that 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 a social efficiency performance guarantee.

The rest of the paper is organized as follows: Section 2 introduces some necessary preliminaries. Section 3 designs an approximately optimal social efficiency and privacy-preserving strategyproof auction mechanism for identical items. In Section 4, we further introduce a combinatorial auction with privacy-preserving. Section 5 evaluates the performance of our approach. Section 6 discusses the related literature and Section 7 concludes the paper.

2 Model, Problem, and Preliminaries

In this section, we first briefly introduce the auction system model. Then, we illustrate the necessary economic property of an auction mechanism and state our auction design targets in Section 2.2. In Section 2.3, we review the cryptographic tools used in this paper.

2.1 Auction model

In recent years, auctions have been deemed as a preeminent means to allocate resources in many areas. Many resource allocation problems can directly be seen as (resource) auction problems. In general, our auction design is not limited to a concrete resource allocation problem. Here we directly present the auction model, which can manage many resource allocation problems. Consider a sealed-bid auction, as shown in Fig. 1, in which there exists an auctioneer, a set of bidders, and an agent. At the beginning of the auction, all the 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 the bidders, but will not collude with the auctioneer.

We study two auction models in this paper: IA model and CA model. In the IA model, we assume that there exists a set of identical items denoted as $\mathcal{I} = \{I_1, I_2, ..., I_h\}$, and m bidders denoted by $\mathcal{B} = \{1, 2, ..., m\}$ 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 items. 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 in both 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.

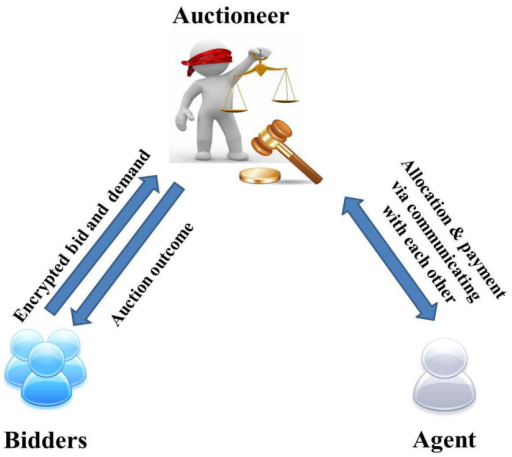


Fig. 1 Secure auction model.

2.2 Auction goals

The goals of our auction mechanism are two-fold: (1) the proposed auction mechanism should preserve some economic properties, such as strategyproof and social efficiency maximization; and (2) the auction mechanism should preserve the privacy of bidders. The detailed description follows.

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, and p_i are the bid value, true valuation, and the payment of bidder i for all the items he wants to buy, respectively. Then, the utility of bidder i is defined as

$$u_i = \begin{cases} v_i - p_i, & \text{if bidder } i \text{ wins the auction;} \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

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 proven 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 to satisfy 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. Nor do they know which items each loser wants to get.

2.3 Paillier's homomorphic encryption cryptosystem

We use a 1024-bit length Paillier's homomorphic encryption system in this paper, which satisfies the following homomorphic operations:

$$E(\mathsf{msg}_1)E(\mathsf{msg}_2) = E(\mathsf{msg}_1 + \mathsf{msg}_2),$$
$$E(\mathsf{msg}_1)^{\mathsf{msg}_2} = E(\mathsf{msg}_1\mathsf{msg}_2),$$

where $E(\mathsf{msg}_i)$ is the ciphertext of message msg_i.

To facilitate reading, we summarize some symbols that are used in this paper in Table 1.

Table 1 Some symbols used in this paper.

Symbol	Meaning
$\mathcal{I}, \mathcal{B}$	The set of items and bidders in the auction
h, m	The number of items and bidders in the auction
N_i, c_i	The number / combination of items bidder i wants to buy
v_i, b_i, p_i	The true valuation, bid value, and payment of bidder i for all the items he wants to buy
u_i	The utility of bidder i
EK,DK	The encrypt key and decrypt key of the agent
$E(\mathsf{msg})$	The ciphertext of message msg
i'	The bidder with rank i in the sorted bid set
π_1, π_2	The permutation for the ID of bidders and items
$X_i, x_{i,j}$	The demand vector of bidder i, where $x_{i,j} = 1$ if bidder i wants to buy item I_j; otherwise $x_{i,j} = 0$

2.4 Application scenario illustration

In this subsection, we illustrate two typical application scenarios for the IA model and the CA model, respectively.

For the IA model, we consider the virtual machine resource allocation in cloud computing. In an infrastructure-as-a-service cloud, the computation resources (e.g., CPU, RAM, disk) have been packed into some virtual machines. Cloud users can request some virtual machines to run their computational tasks. For example, Amazon EC2 can provide seven categories and 23 types of virtual machines. When EC2 users want to request some virtual machines of the same type, the corresponding virtual machine allocation problem will fall into the IA model, and can be solved by our proposed auction mechanism. Most existing studies focus on the storage and computational privacy in cloud computing. Only a few studies consider the bid privacy in the process of the resource allocation of cloud computing. None of them likes our solution considers strategyproofness, privacy, and the performance guarantee simultaneously.

For the CA model, we consider a spectrum auction scenario where the spectrum channels are heterogeneous, due to the different frequencies, bandwidths, and licensed areas. All the spectrum channels in the market are viewed as items in the CA model. The new spectrum demanders are viewed as the bidders. Each bidder i needs a combination of spectrum channels, which is c_i in the CA model. Then, the spectrum auction problem in this setting is exactly a concrete CA problem. Spectrum auctions have been widely studied in recent years, but only a few studies consider the privacy-preserving issue in their work. To the best of our knowledge, our work is the first to provide a strategyproof and privacy-preserving solution for the combinatorial spectrum auction problem.

3 Identical Items Auction Mechanism Design with Privacy Preservation (IAMP)

In this section, we propose an IAMP design, 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, the agent publishes EK as a public key, and keeps DK private. We assume that the parameter n is 1024-bit length in this work. Each bidder i encrypts the 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 decide on the winner aiming to maximize the social efficiency. However, the social efficiency maximization problem can be reduced to the Knapsack Problem, which is a well-known NP-hard problem. To address this NP-hard problem, a PTAS has been proposed in Ref. [18], which is also suitable for our model. Unfortunately, there is a large computation and comparison overload in this PTAS, since it is based on dynamic programming. It is very difficult to design a bid privacy preservation version based on this PTAS. Therefore, we build our privacy-preserving method based on another approximation algorithm, which can approximate the optimal allocation within a factor of 2.

The main idea of the approximation method we used is depicted as follows:

(1) We first sort the per-unit bid values of bidders in non-increasing order:

$$\frac{b_{\sigma(1)}}{N_{\sigma(1)}} \geqslant ... \geqslant \frac{b_{\sigma(i)}}{N_{\sigma(i)}} \geqslant ... \geqslant \frac{b_{\sigma(m)}}{N_{\sigma(m)}} \tag{2}$$

where $\sigma(i)$ is the i-th bidder in the sorted bid set.

(2) Then, we find the critical bidder $\sigma(k)$, which satisfies

$$\sum_{i=1}^{k-1} N_{\sigma(i)} \leqslant h \leqslant \sum_{i=1}^{k} N_{\sigma(i)} \tag{3}$$

where h is the number of items in the market.

(3) If $\sum_{i=1}^{k-1} b_{\sigma(i)} \geqslant b_{\sigma(k)}$, then the top $k-1$ bidders in the sorted bid set win the auction; otherwise, bidder $\sigma(k)$ wins.

Lemma 1 The proposed algorithm can approximate $1/2$ of the optimal algorithm.

Proof Suppose $\mathcal{O}$ is the set of bidders in the optimal solution, and $w(\mathcal{O}) = \sum_{i\in\mathcal{O}} b_i$. Obviously,

$$w(\mathcal{O}) \leqslant \sum_{i=1}^{k} b_{\sigma(i)} \tag{4}$$

Then, we can easily obtain

$$\frac{1}{2}w(\mathcal{O}) \leqslant \frac{1}{2}\sum_{i=1}^{k} b_{\sigma(i)} \leqslant \max(\sum_{i=1}^{k-1} b_{\sigma(i)}, b_{\sigma(k)}) \tag{5}$$

This completes our proof. ■

The details of our allocation mechanism with privacy preservation is depicted in Algorithm 1. First, we sort the per-unit bid values of bidders to decide the winners. To address the issue of privacy-preserving, bidders first encrypt their bids using the encryption key 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 selected based on the consideration of the correctness of the 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 $\delta_1 \frac{b_i}{N_i} + \delta_2$ into non-increasing order without accessing any true bid values of the bidders. Furthermore, the

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.
$$\frac{b_{\sigma(1)}}{N_{\sigma(1)}} \geqslant ... \geqslant \frac{b_{\sigma(m)}}{N_{\sigma(m)}}.$$
Obviously, $\frac{b_i}{N_i} \geqslant \frac{b_j}{N_j}$ if $\delta_1 \frac{b_i}{N_i} + \delta_2 \geqslant \delta_1 \frac{b_j}{N_j} + \delta_2$.
4: The agent finds the critical bidder $\sigma(k)$ by computing:
$$\sum_{i=1}^{k-1} N_{\sigma(i)} \leqslant h \leqslant \sum_{i=1}^{k} N_{\sigma(i)}.$$
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 $\sum_{i=1}^{k-1} b_{\sigma(i)} \geqslant b_{\sigma(k)}$; otherwise, the agent 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.

auctioneer also maps the true ID of the 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 the bidders either. Then, we need to find the bidders with the top $k-1$ per-unit bids and the bidder with the k-th per-unit bid. The agent can do this easily with the sorted per-unit bids. Next, the agent sends the permutated ID of the bidders with the top k per-unit bids to the auctioneer. Then, the auctioneer computes the encrypted bid sum of the bidders with the 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 judge which one is bigger and further decides the winning bidders.

Next, we will show that our allocation mechanism for the IA model is bid-monotone.

Lemma 2 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 In our allocation mechanism, we set the bidder $\sigma(k)$ to win the auction, or the bidders with the top $k-1$ per-unit bids to win the auction. In the case of bidder $\sigma(k)$ winning the auction, we can easily get $b_{\sigma(k)} \geqslant \sum_{i=1}^{k-1} b_{\sigma(i)}$. When bidder $\sigma(k)$ increases his bid from $b_{\sigma(k)}$ to $b'_{\sigma(k)} > b_{\sigma(k)}$, obviously, both $b'_{\sigma(k)} \geqslant \sum_{i=1}^{k-1} b_{\sigma(i)}$ and $b'_{\sigma(k)} \geqslant \max(b_{\sigma(i)} | i < k)$ hold. Thus, bidder $\sigma(k)$ will always win no matter whether $\frac{b'_{\sigma(k)}}{N_{\sigma(k)}}$ is the k-th highest per-unit bid or not.

In the case of the bidders with the top $k-1$ per-unit bids winning the auction, the bidders who are in the bidder set with the top $k-1$ per-unit bids remain unchanged when any of the $k-1$ bidders increase their bid. Suppose bidder $\sigma(j)$ increases his bid to $b'_{\sigma(j)}$, we can easily get that $\sum_{i=1}^{j-1} b_{\sigma(i)} + b'_{\sigma(j)} + \sum_{i=j+1}^{k-1} b_{\sigma(i)}$ is still larger than $b_{\sigma(k)}$. Thus, the bidders with the top $k-1$ bids will also win the auction.

This completes our proof. ■

3.3 Payment calculation mechanism

It has been proven 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 the winners with privacy preservation.

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

$$\sum_{i=1}^{f-1} N_{\sigma(i)} \leqslant h \leqslant \sum_{i=1}^{f} N_{\sigma(i)} \tag{6}$$

Obviously, the critical value of each winner $\sigma(i)$ is less than the L_i^*-th bid value, and larger than the U_i^*-th bid value. To find the critical value of each winner, we first compute their critical intervals. As shown in Algorithm 2, we use a 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 $\sigma(i)$ equal to the per-unit bid of the M-th bidder in the sorted list, and then compare the bid sum of the 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 achieved 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 the auctioneer can further obtain 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 $\sigma(i)$ won or not, by decrypting and comparing the values $\sum_{j=1}^{k-1} b_{\sigma(j)^*}$ and $b_{\sigma(k)^*}$. Then, the agent can obtain the new boundary for the binary search, until the critical interval of bidder $\sigma(i)$ is found.

After obtaining the critical interval of each winner, we compute their critical values. For the case that winner $\sigma(i)$ is the new k-th bidder, and the 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

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

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

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

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

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

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

$$E(\delta_{M,2}N_{\sigma(M)})E(b_{\sigma(k)^*})^{N_{\sigma(M)}\delta_{M,1}}.$$

4: The agent decrypts the received ciphertexts and checks if bidder $\sigma(i)$ win or not by bidding $\frac{b_{\sigma(M)}N_{\sigma(i)}}{N_{\sigma(M)}}$, then executes the following operation.

5: **if** $\sigma(i)$ wins by bidding $\frac{b_{\sigma(M)}N_{\sigma(i)}}{N_{\sigma(M)}}$ **then**

6: The agent sets $L = M$, and $M = \lfloor (U + L)/2 \rfloor$;

7: **else**

8: The agent sets $U = M$, and $M = \lfloor (U + L)/2 \rfloor$;

9: **end if**

10: Repeat Steps $2 - 8$ 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 $\sigma(i)$.

the critical value $p_{\sigma(i)}$ of winner $\sigma(i)$ as follows:

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

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

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

Assume that $s_1 = \sum_{j=1}^{k-1} b_{\sigma(j)^*}$, $s_2 = b_{\sigma(U_i^*)}N_{\sigma(i)}$, and $s_3 = b_{\sigma(k)^*} + b_{\sigma(i)}$. 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 their respective critical value, thus we can also obtain Algorithm 1.

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 following and sends the results to the agent.

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

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

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 following, and sends the results to the agent.

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

$$E(\delta_6 N_{\sigma(U_i^*)} + \delta_5(s_2 + s_1 N_{\sigma(U_i^*)}) =$$

$$E(\delta_6 N_{\sigma(U_i^*)})(E(b_{\sigma(U_i^*)})E(\prod\nolimits_{j=0}^{k-1} E(b_{\sigma(j)^*})))^{\delta_5 N_{\sigma(i)}},$$

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

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: **end if**

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

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

Theorem 1 The auction mechanism we proposed is strategyproof.

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

3.4 Security analysis

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

Theorem 2 Our auction mechanism for identical-items guarantees bid privacy.

Proof In our auction mechanism for identical items, the auctioneer can only obtain the encrypted bids of the bidders and the payments of the winners. Without the decryption key, the auctioneer cannot derive any other information from these encrypted bids. The

auctioneer knows the payments of the winners but cannot construct the equations among them since the auctioneer does not know exactly which variables are involved in these equations, i.e., the auctioneer cannot determine which value is larger than the other in the payment equations. Thus, the bid values of the bidders can be well preserved from the auctioneer.

The agent holds the decryption key but has no direct access to the encrypted bids. According to our auction mechanism, the agent will receive many encrypted bids or bid sums which are masked by random numbers. Assume that the number of bids or bid sums received by the agent is n. With these bids or bid sums, the agent can build n functions that contain no less than $n + 2$ bids, bid sums, or random numbers. Since the number of variables is larger than the number of functions, the agent cannot decrypt any true bid values of the bidders. Furthermore, the payment of each winner is also considered. Note that the IDs of the bidders are permutated by the auctioneer. Thus, the agent cannot map the payment equation to each winner with the auction results, indicating that the true bid values of the bidders are blind for the agent.

In conclusion, the bids of the bidders are blind to both the auctioneer and the agent. That is, our auction mechanism for identical-items guarantees bid privacy. ■

4 Combinatorial Auction Mechanism Design with Privacy Preservation (CAMP)

In this section, we propose a CAMP design, which also achieves strategyproofness and maximizes social efficiency. Compared with IAMP, CAMP not only protects the true bid values of the bidders, but also preserves the demands of the losers.

4.1 Bidding

Like the bidding process in IAMP, the agent first generates encryption and decryption keys of Paillier's cryptosystem, and publishes the EK. Then, each bidder encrypts $b_i/\sqrt{|c_i|}$ using the EK of the agent and sends the results to the auctioneer. However, all the bidders not only want to protect their own bids in our CA model, but also want to hide the items that they want to buy if they lose in the auction. Thus, each bidder will also encrypt the targeted set of items. Let $\boldsymbol{X}_i = \{x_{i,1}, x_{i,2}, ..., x_{i,h}\}$ be the demand vector of bidder i, where $x_{i,j} = 1$ if $I_j \in c_i$, otherwise $x_{i,j} = 0$. For each $x_{i,j}$, bidder i generates a random integer r and encrypts $x_{i,j}$ using the EK of the agent. Finally, bidder i sends $(E(b_i/\sqrt{|c_i|}), E(X_i))$ to the auctioneer, where $E(X_i) = \{E(x_{i,1}), E(x_{i,2}), ..., E(x_{i,h})\}$.

Table 2 shows an example of the demand and encrypted demand of the bidders when $h = 5$.

4.2 Allocation mechanism

After receiving the encrypted bids and demands from the bidders, the auctioneer selects a set of bidders as winners if the social efficiency is maximized. It has been proven in Ref. [17] that the social efficiency maximization problem in the combinatorial auction is NP-hard, and the upper bound of approximation ratios of the polynomial time algorithms is $\sqrt{h}$.

Dong et al. proposed an auction mechanism with a greedy allocation mechanism in Ref. [17], which can approximate the optimal one within a factor of $\sqrt{h}$. We briefly describe this mechanism below:

- First, a normalized bid $\dfrac{b_i}{\sqrt{|c_i|}}$ for each bid b_i is calculated, and then the bidders are sorted according to the non-increasing order of the normalized bids.
- Next, 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 has been granted were it not for the presence of i. Then, bidder i pays zero if his bid is denied or $l(i)$ does not exist; otherwise, he pays $\sqrt{|c_i|} \cdot n_{l(i)}$, where $n_{l(i)}$ is the normalized bid of bidder $l(i)$.

Following the CA mechanism stated above, only two operations rely on the true bid values of the bidders: sorting the bidders according to their normalized bids and computing the payment for each winner i using the normalized bid of $l(i)$. Thus, we can similarly perform the same steps in IAMP to protect the bid privacy of the bidders. However, the agent needs to know the demand vectors of all the bidders to check if they overlap with each other in the combinatorial auction. Therefore, the most challenging issue of designing privacy-

Table 2 The demand and encrypted demand of bidders.

Bidder	Demand	Encrypted demand
1	$\{1, 0, 1, 0, 0\}$	$\{E(1), E(0), E(1), E(0), E(0)\}$
2	$\{0, 1, 0, 0, 1\}$	$\{E(0), E(1), E(0), E(0), E(1)\}$
...	...	...
m	$\{1, 1, 0, 1, 0\}$	$\{E(1), E(1), E(0), E(1), E(0)\}$

preserving CA mechanism is to protect the demand of the losers. To manage this challenge, we encrypt the demand vector of the bidders. More specifically, we confuse the ID of the bidders and the ID of the 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 sends the demand vectors to the agent. With the confused information and decryption key, the agent can also obtain the overlapping information of the bidders, but can barely map them to the true demands of the losers. Furthermore, the auctioneer is only provided the encrypted demand vectors and the auction result but has no idea about the demands of each loser. Then, the demands privacy of the losers is protected. The detail of our allocation mechanism with privacy preservation is shown in Algorithm 4.

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, the normalized bid is larger than the normalized bid of $l(i)$. Thus, $n_{l(i)} \cdot \sqrt{|c_i|}$ is the critical value of winner i if $l(i)$ exists. Otherwise, the critical value of winner i is zero. Our payment calculation mechanism is shown in Algorithm 5.

4.4 Security analysis

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

Proof Since the demand vectors of the bidders are encrypted and the auctioneer does not have the decryption key, the auctioneer cannot retrieve anything from the encrypted vectors. Moreover, the agent only sends the demand vectors of the winners to the auctioneer. Thus, the auctioneer has no means to access the true demands of the losers. For the agent, he can decrypt the demand vector of any bidder but cannot determine the exact demand of each loser i since the real relationships between items and the IDs of the bidders are permutated by permutation functions, which are only possessed by the auctioneer. Therefore, we can conclude that our CA mechanism protects the demands of the losers. ■

Theorem 4 Our CA mechanism guarantees bid privacy.

Proof Without loss of generality, let us consider the bid b_i of bidder i. The auctioneer can obtain the encrypted bid $E(b_i)$ and $p_i = b_{l(i)}\sqrt{|c_i|}/\sqrt{|c_{l(i)}|}$ for each winner i. Since b_i has been encrypted, the auctioneer cannot retrieve any information from $E(b_i)$. Moreover, the auctioneer does not know which items each loser bids for and has no idea which bidder is $l(i)$ of winner i. Thus, the auctioneer cannot find the bid value of any bidder from each p_i.

Although the agent possesses the decryption key, he cannot directly access the encrypted bids as the encrypted bids are masked by the auctioneer using random numbers, before they are sent to the agent. With

Algorithm 4 Allocation mechanism for combinatorial auction

1: The auctioneer randomly picks two integers $\delta_1 \in \mathbb{Z}_{2^{1012}}$, $\delta_2 \in \mathbb{Z}_{2^{1022}}$, executes the following homomorphic operation, and then 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 the private key, and reorders them in the descending order:

$$\delta_1 \frac{b_{\sigma(1)}}{\sqrt{|c_{\sigma(1)}|}} + \delta_2, ..., \delta_1 \frac{b_{\sigma(m)}}{\sqrt{|c_{\sigma(m)}|}} + \delta_2,$$

where

$$\frac{b_{\sigma(1)}}{\sqrt{|c_{\sigma(1)}|}} \geqslant ... \geqslant \frac{b_{\sigma(m)}}{\sqrt{|c_{\sigma(m)}|}}.$$

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** $j \leqslant h$ and $\sigma(i) \in W$ **do**
8: **if** $x_{\sigma(i),j} = 1$ and $\sum_{k=1}^{i-1} x_{\sigma(k),j} \geqslant 1$ **then**
9: Set $W = W \setminus \{\sigma(i)\}$
10: **end if**
11: Set $j = j + 1$
12: **end while**
13: **end for**
14: The agent sends the set W of winners to the auctioneer.

Algorithm 5 Payment calculation for combinatorial auction

1: For each winner $i \in W$, the agent finds $l(i)$ and 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:

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

the masked bids, the agent can build m functions with m encrypted bids and two random numbers. Since the number of variables is greater than the number of functions, the agent cannot decrypt any true bid values of the bidders. The payment p_i of each winner i is available to the agent. However, the IDs and the demand vectors of the bidders are disrupted by the auctioneer. Thus, the agent does not know $l(i)$ either. That is, the agent still cannot determine the bid value of any bidder using the p_i's.

In conclusion, our CA mechanism guarantees bid privacy. ■

5 Simulation Results

In this section, we present our evaluation results and the performance analysis of our auction mechanisms, including the auction performance and the cost of computation and communication.

5.1 Auction performance

We first introduce two major metrics to evaluate the performance of the auction mechanism, namely social efficiency ratio and revenue ratio.

- *Social efficiency ratio*: the social efficiency ratio is defined as the ratio between the social efficiency of our approximation mechanism and the optimal mechanism.
- *Revenue ratio*: the revenue for an auction is the total payment received from all winners, that is, the ratio between the revenue of our approximation mechanism and the optimal mechanism. However, it is challenging to obtain the optimal revenue. Thus, we use the optimal social efficiency instead of the optimal revenue in our simulation, which is an upper bound of the optimal revenue.

In our simulation, we assume the bid values of the bidders are randomly distributed in the range $[0, 10\,000]$, and the number of items that each bidder wants to buy is randomly distributed in the range $[1, N_{\max}]$, where $N_{\max}$ is the maximum number of items that each bidder can bid. In each set of evaluations, we vary one factor among the bidder number, items number, and $N_{\max}$, while fixing the other two factors. In our CA0 model, we first randomly generate a number N_i from $[1, N_{\max}]$ for each bidder i, and then randomly choose N_i items from the item set $\mathcal{I}$ as bidder i's demand c_i.

Since one of the important goals of the auction design is to maximize the social efficiency, we first evaluate the social efficiency ratio of our approximation algorithms. As shown in Fig. 2, the social efficiency ratio increases with the number of bidders in both the IAMP and CAMP mechanisms. Theoretically, both the weights of the optimal solution and that of our approximation solution should increase with the bidder number and the number of items. However, we find an interesting result: the social efficiency ratio decreases with the increasing number of the items in CAMP. One possible reason is that, when the number of items increase,

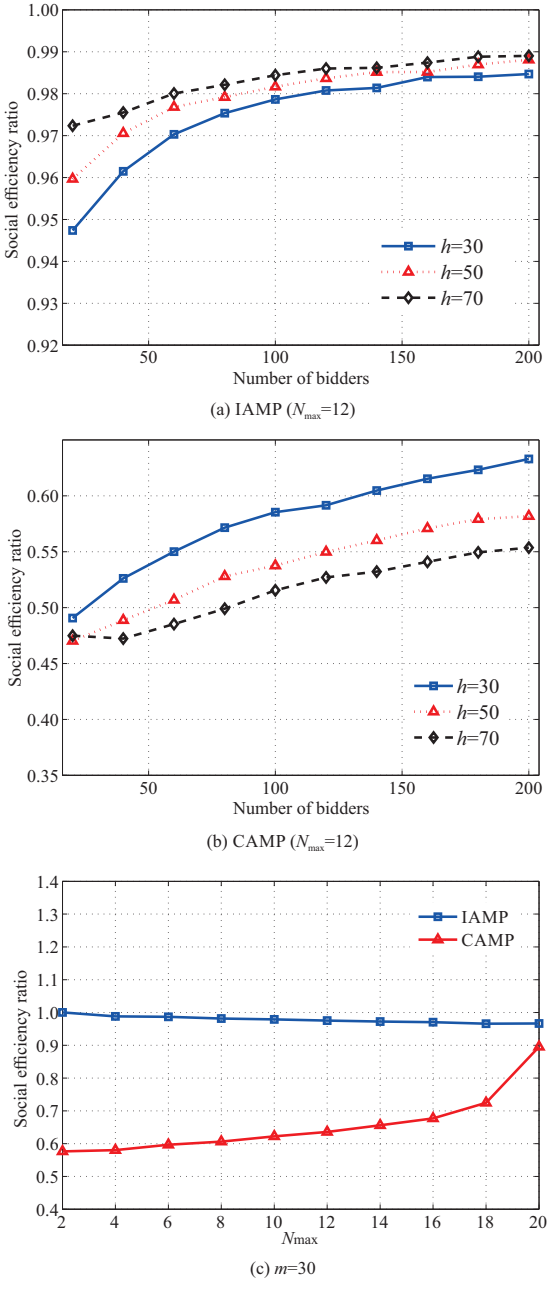


Fig. 2 Social efficiency ratio of the proposed approximation algorithms.

the optimal social efficiency increases faster than the approximation solution in CAMP, but increases slower than the approximation solution in other cases. We fix the number of bidders and items, and increase the maximum number of items that each bidder wants to buy, as shown in Fig. 2c. Due to the demands of the bidders being inseparable, the social efficiency ratio curve of the IA model declines with increasing $N_{\max}$ in Fig. 2c. However, in the CA model, more items are sold to bidders with high bid values and the social efficiency ratio increases with increasing $N_{\max}$. Besides, we can also learn from Fig. 2 that our approximation algorithms perform much better than the theoretical values, especially for the IA model.

In addition, we also compare the social efficiency of CAMP with a greedy mechanism. This greedy mechanism first sorts the bids of the bidders in descending order, and then scans the bidders one-by-one to decide which bidder wins the auction, as we did in CAMP. The simulation result is shown in Fig. 3. Obviously, CAMP has better performance than the greedy mechanism. This is mainly because the proposed CAMP sorts the bidders according to their normalized bids, while the greedy mechanism sorts the bidders according to their bids. Thus, the unit bid value of the winners in CAMP is larger than that in the greedy mechanism, which can lead to greater social efficiency.

The revenue ratios of our approximation algorithms are described in Fig. 4. Since we charge each winner their respective critical value in our auction mechanisms, then theoretically, the total payment for winners should increase when the competitive rate increases. Conversely, the competitive rate is affected by the bidder number, item number, and $N_{\max}$. Basically, our evaluation results corroborate the theoretical analysis. However, due to the similar reason as that provided for the social efficiency ratio, the performance of the revenue ratio decreases with the increasing number of items in CAMP, while performing opposite in IAMP.

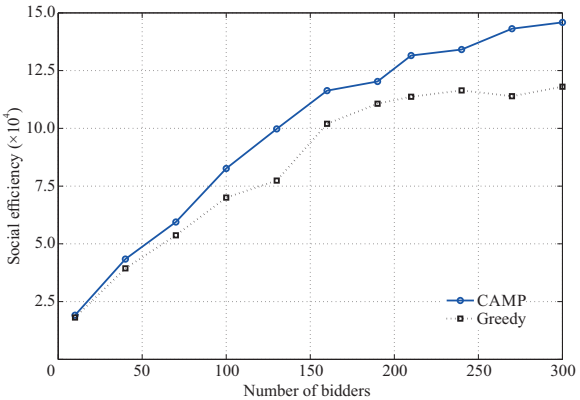


Fig. 3 Social efficiency of the CAMP and the comparison greedy algorithm ($N_{\max}$= 12).

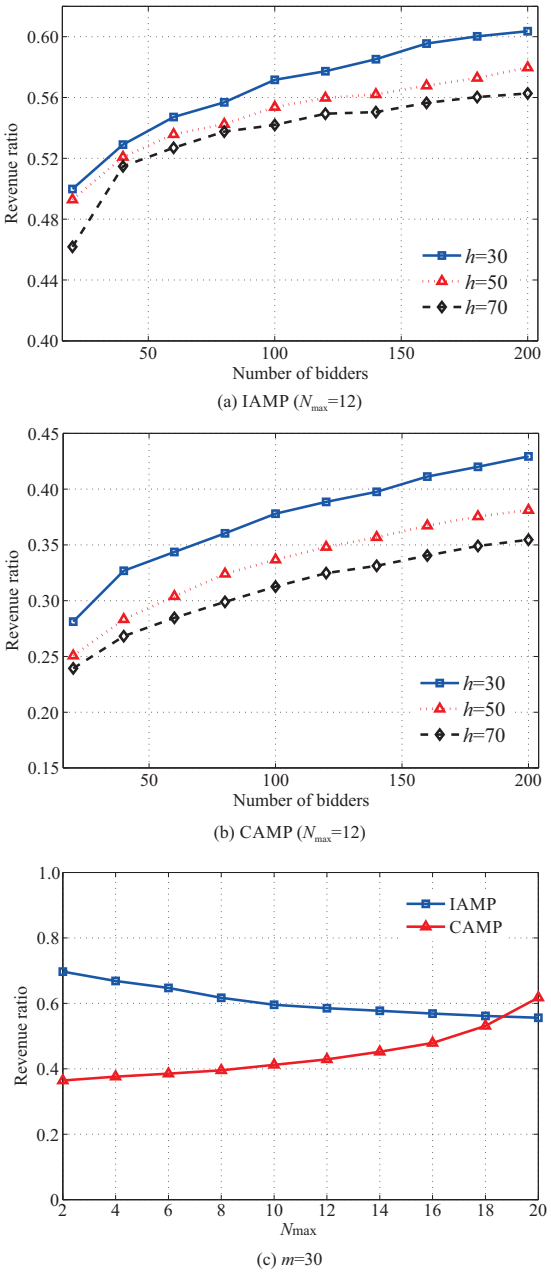


Fig. 4 Revenue ratio of the proposed approximation algorithms.

5.2 Computation and communication overhead

We evaluate the computation and communication overhead of our approximation algorithms. Since computation overhead is dominated by the auctioneer and the agent in both auction models, we do not

consider the bidders' computation overhead. As shown in Fig. 5, the auctioneer spends more time in the IA model than in the CA model. This is because the auctioneer spends most of his time computing the payments from the winners. However, we can easily find them in the CA model.

The run-time of each bidder is roughly 30 ms in the IA model. However, bidders need to encrypt their bids and demands in the CA 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 greater in IAMP.

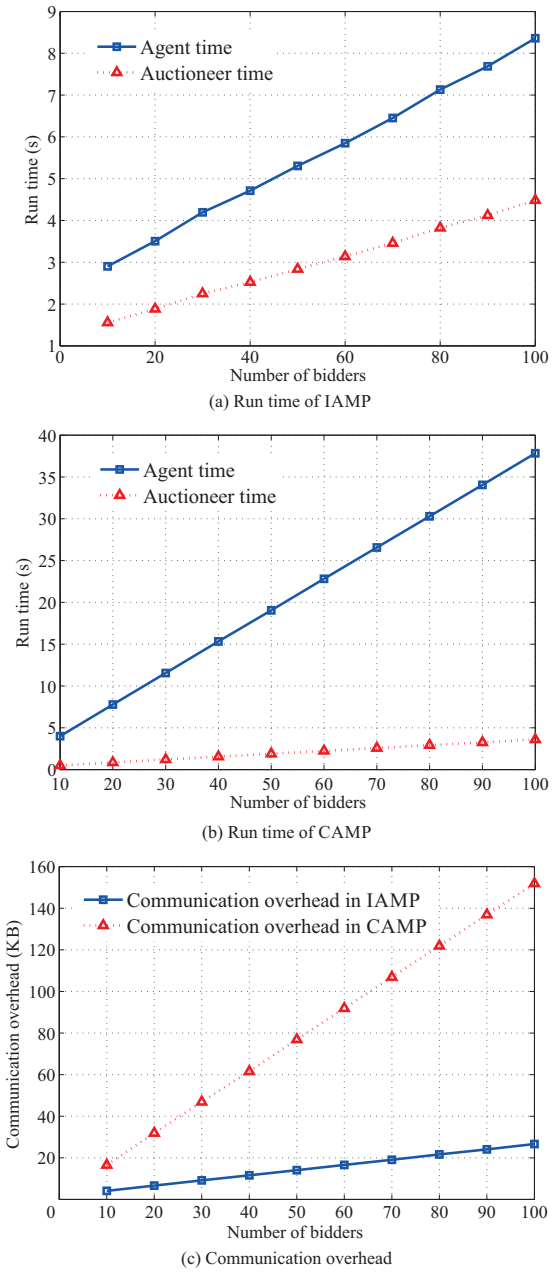


Fig. 5 Computation and communication overhead when $h = 5$.

In the evaluation, we set n to be of 1024-bit length. Figure 5c shows the communication overhead of our auction mechanisms with privacy preservation. It is found that the communication overhead of CAMP is much higher than that of IAMP. The main reason is that bidders encrypt only their bids in the IA, but encrypt both their bids and demands in the CA.

5.3 Comparison with prior state-of-art work

To show superiority of the proposed mechanisms, we compare the performance of our work with prior work in Ref. [19], and further prove that our mechanisms perform better than the mechanisms in Ref. [19].

First, we consider the performance of social efficiency. The IA model studied in this work is similar to the auction model stated in Ref. [19]. However, the optimal allocation problem studied in Ref. [19] can be solved in polynomial time, which is easier than ours. The CA models studied in our work and Ref. [19] are identical. It has been proven that the optimal allocation problem of the CA model is NP-hard. However, Ref. [19] proposed a privacy-preserving mechanism for the optimal allocation, but not for the approximation allocation. Thus, the proposed mechanism of Ref. [19] for the CA model cannot be solved in polynomial time either. Moreover, in the auction mechanism design, there are two procedures to be addressed. The first is the allocation mechanism design and the second is payment calculation. The work of Ref. [19] concentrates on the privacy-preserving allocation mechanism design, so the payment calculation is not mentioned.

Then, we compare the performance of privacy preservation. We proved that our mechanisms can protect the bid privacy of bidders if the auctioneer does not collude with the agent. There are three parties in Ref. [19], namely the weight publisher, the evaluator, and the mask publisher. The proposed mechanism can protect the bid privacy of the bidders when no more than t_w evaluators and t_m mask publishers collude with each other. Note that the number of evaluators is no less than the possible maximal bid value, i.e., there are at least 1000 evaluators if the maximal bid is 1000. There is only one auctioneer and one agent in our mechanisms; thus, the privacy preservation of our mechanisms is easier to achieve than the mechanisms proposed in Ref. [19].

For the performance of communication overhead, the communication overhead of our mechanisms is $O(m)$ for the IA model and $O(mh)$ for the CA model, where m is the number of bidders and h is the number of goods. The communication overhead of the mechanisms proposed in Ref. [19] is $O(e\times(l+(t_m+1)\times(\log e+l+n\log e)))$, where $l=mh$, e is the number of evaluators, t_m+1 is the number of mask publishers, and each bidder will submit the fraction of bid to n evaluators. Clearly, the communication overhead of our mechanism is lower than the mechanisms proposed in Ref. [19].

6 Literature Review

Many solutions have been proposed in previous literature to address the scarcity problem of the limited resources, such as radio spectrum, emissions permits, and airport landing slots. The auction has been shown to be one of the most effective methods among all the solutions. However, most studies on auctions (e.g., Refs. [3, 4, 20–22]) only allow bidders to bid a single item in one round of the auction. There are only a few researchers who have considered the case that each bidder can bid for multiple items. Huang et al.[23] proposed an auction mechanism, in which all participants could exchange multi-unit items. Wurman et al.[24] designed an auction mechanism which transforms the buyers' multi-unit items demand to a single-unit transaction. Babaioff and Walsh[25] studied a budget-balanced and strategy-proof double auction mechanism, where each buyer desires for a bundle of items. Chu and Shen[26] proposed an asymptotically efficient strategyproof auction mechanism, namely BC-LP, which achieved bundling of commodities transactions for buyers. Combinatorial auction[15, 27] allowing bidders to bid for packages of items has been widely studied in various research fields recently, such as cloud computing, spectrum auction, etc. The authors in Ref. [28] introduced combinatorial auction-based allocation mechanisms for the virtual machine allocation problem of cloud computing. Dong et al.[17] applied a combinatorial spectrum auction model with time-frequency flexibility in cognitive radio networks. However, none of these auction mechanisms provided any guarantee on privacy preservation.

Several sealed-bid auction mechanisms with privacy preservation have been proposed in previous studies. For instance, Refs. [8, 9] are works about the first-price or second-price auction mechanism design, which protect the bid values of bidders. In Refs. [10, 29–34], a second central party, called an "auction issuer", "auction authority", or "agent" in addition to the auctioneer, was introduced to the auction. These works model this second central party as a trusted or semi-trusted party, which communicates with the auctioneer to make the winner decision and to compute the payment from winners while protecting the privacy of the bidders. Brandt and Sandholm[35–38] focused on the design of unconditional full privacy auction protocols, which relies neither on a trusted third-party, nor on any computational intractability assumptions. Although these protocols are fully privacy-preserving, the computational and communication complexities are relatively high. Brandt and Sandholm[39] also designed secure mechanisms for three common types of multi-unit auctions: uniform-price, discriminatory, and the generalized Vickrey auctions. In Ref. [12], a secure combinatorial spectrum auction was designed using homomorphic encryption to deal with the untrustworthy auctioneer. In Ref. [19], several secure combinatorial auction mechanisms were proposed with dynamic programming via polynomial secret sharing. Unfortunately, the optimal allocation problem in most practical auctions is NP-hard, especially in multi-unit auctions. None of the existing solutions with privacy preservation have provided any performance guarantee, such as maximizing the social efficiency. In this work, we tackle this problem to design strategyproof and privacy-preserving auction mechanisms that maximize social efficiency.

7 Conclusion

In this paper, we proposed the first strategyproof and privacy-preserving multi-unit auction mechanisms that maximize social efficiency. We study two cases for multi-unit auctions, 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 each case, which have the approximation factors of 2 and $\sqrt{h}$, respectively. Furthermore, we also computed the critical payment with privacy preservation for each winner, and theoretically proved the properties of our auction mechanisms, such as strategyproofness, privacy preservation, and approximation factor. Additionally,

although the privacy-preserving design has incurred some computation and communication overheads, the auction mechanisms are still efficient. Our evaluation results demonstrated that our protocols not only achieve good social efficiency, but also perform well in computation and communication aspects.

Hence, we believe that this is the first study of multi-unit auction mechanisms with performance guarantee and privacy preservation; however, there are several interesting questions left for future work. The first is to study the case when the bidder's demands are separable, and their per unit bids are related to the number of identical items they win in the auction. The second is to design strategyproof and privacy preserving auction mechanisms when bidders can bid on multi-combinatorial items, but only want to buy one of the items in the combinatorial auction.

Acknowledgment

This paper was supported by the National Natural Science Foundation of China (Nos. 61572342 and 61672369), the Natural Science Foundation of Jiangsu Province (Nos. BK20151240 and BK20161258), China Postdoctoral Science Foundation (Nos. 2015M580470 and 2016M591920). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the funding agencies (NSFC).

References

[1] W. Y. Lin, G. Y. Lin, and H. Y. Wei, Dynamic auction mechanism for cloud resource allocation, in *Proc. 10th IEEE/ACM CCGrid*, Melbourne, Australia, 2010, pp. 591–592.

[2] A. Gopinathan, Z. Li, and C. Wu, Strategyproof auctions for balancing social welfare and fairness in secondary spectrum markets, in *Proc. 31st IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 2813–2821.

[3] H. Huang, Y. Sun, X. Y. Li, Z. Chen, W. Yang, and H. Xu, Near-optimal truthful spectrum auction mechanisms with spatial and temporal reuse in wireless networks, in *Proc. 14th ACM MobiHoc*, Bangalore, India, 2013, pp. 237–240.

[4] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, ebay in the sky: Strategy-proof wireless spectrum auctions, in *Proc. 14th ACM Mobicom*, San Francisco, CA, USA, 2008, pp. 2–13.

[5] W. Dong, S. Rallapalli, R. Jana, L. Qiu, K. Ramakrishnan, L. Razoumov, Y. Zhang, and T. W. Cho, Ideal: Incentivized dynamic cellular offloading via auctions, in *Proc. 32nd IEEE INFOCOM*, Turin, Italy, 2013, pp. 755–763.

[6] X. Wang, Z. Li, P. Xu, Y. Xu, X. Gao, and H. H. Chen, Spectrum sharing in cognitive radio networksan auction-based approach, *IEEE Trans. on Sys., Man, and Cybernetics, Part B: Cybernetics*, vol. 40, no. 3, pp. 587–596, 2010.

[7] V. Krishna, *Auction Theory*. Academic Press, 2009.

[8] Y. F. Chung, K. H. Huang, H. H. Lee, F. Lai, and T. S. Chen, Bidder-anonymous english auction scheme with privacy and public verifiability, *Journal of Systems and Software*, vol. 81, no. 1, pp. 113–119, 2008.

[9] H. Kikuchi, (M+1)st-price auction protocol, *Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 85, no. 3, pp. 676–683, 2002.

[10] Q. Huang, Y. Tao, and F. Wu, SPRING: A strategy-proof and privacy preserving spectrum auction mechanism, in *Proc. 32nd IEEE INFOCOM*, Turin, Italy, 2013, pp. 2219–2227.

[11] M. Pan, X. Zhu, and Y. Fang, Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer, *Wireless Networks*, vol. 18, no. 2, pp. 113–128, 2012.

[12] M. Pan, H. Li, P. Li, and Y. Fang, Dealing with the untrustworthy auctioneer in combinatorial spectrum auctions, in *Proc. GLOBECOM 2011*, Houston, TX, USA, 2011, pp. 1–5.

[13] S. Dobzinski, N. Nisan, and M. Schapira, Approximation algorithms for combinatorial auctions with complement-free bidders, in *Proc. 37th ACM STOC*, Baltimore, MD, USA, 2005, pp. 610-618.

[14] D. Lehmann, L. I. Oćallaghan, and Y. Shoham, Truth revelation in approximately efficient combinatorial auctions, *Journal of the ACM* , vol. 49, no. 5, pp. 577–602, 2002.

[15] P. Cramton, Y. Shoham, and R. Steinberg, *Combinatorial Auctions*. MIT Press, 2006.

[16] M. H. Rothkopf, A. Pekeč, and R. M. Harstad, Computationally manageable combinational auctions, *Management Science*, vol. 44, no. 8, pp. 1131–1147, 1998.

[17] M. Dong, G. Sun, X. Wang, and Q. Zhang, Combinatorial auction with time-frequency flexibility in cognitive radio networks, in *Proc. 31st IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 2282–2290.

[18] K. Lai and M. X. Goemans, The knapsack problem and fully polynomial time approximation schemes (FPTAS), *Retrieved November*, vol. 3, pp. 2012, 2006.

[19] K. Suzuki and M. Yokoo, Secure combinatorial auctions by dynamic programming with polynomial secret sharing, in *Proc. 7th Financial Cryptography*, Le Gosier, Guadeloupe, 2003, pp. 44–56.

[20] P. Xu and X. Y. Li, Online market driven spectrum scheduling and auction, in *Proc. the CoRoNet workshop of 15th ACM MobiCom*, Beijing, China, 2009, pp. 49–54.

[21] S. G. Wang, P. Xu, X. H. Xu, S. J. Tang, X. Y. Li, and X. Liu, TODA: Truthful online double auction for spectrum allocation in wireless networks, in *Proc. IEEE Dyspan 2010*, Singapore, 2010, pp. 1–10.

[22] P. Xu, S. G. Wang, and X. Y. Li, SALSA: Strategyproof online spectrum admissions for wireless networks, *IEEE*

Trans. on Computers, vol. 59, no. 12, pp. 1691–1702, 2010.

[23] P. Huang, A. Scheller-Wolf, and K. Sycara, Design of a multi–unit double auction e-market, *Computational Intelligence*, vol. 18, no. 4, pp. 596–617, 2002.

[24] P. R. Wurman, W. E. Walsh, and M. P. Wellman, Flexible double auctions for electronic commerce: Theory and implementation, *Decision Support Systems*, vol. 24, no. 1, pp. 17–27, 1998.

[25] M. Babaioff and W. E. Walsh, Incentive-compatible, budget-balanced, yet highly efficient auctions for supply chain formation, *Decision Support Systems*, vol. 39, no. 1, pp. 123–149, 2005.

[26] L. Y. Chu and Z. J. M. Shen, Truthful double auction mechanisms, *Operations Research*, vol. 56, no. 1, pp. 102-120, 2008.

[27] A. Mu'Alem and N. Nisan, Truthful approximation mechanisms for restricted combinatorial auctions, *Games and Economic Behavior*, vol. 64, no. 2, pp. 612–631, 2008.

[28] S. Zaman and D. Grosu, Combinatorial auction-based allocation of virtual machine instances in clouds, *Journal of Parallel and Distributed Computing*, vol. 73, no. 4, pp. 495–508, 2013.

[29] M. Abe and K. Suzuki, M+1-st price auction using homomorphic encryption, in *Proc. 5th Public Key Cryptography*, Paris, France, 2002, pp. 115–124.

[30] O. Baudron and J. Stern, Non-interactive private auctions, in *Proc. 6th Financial Cryptography*, Southampton, Bermuda, 2002, pp. 364–377.

[31] C. Cachin, Efficient private bidding and auctions with an oblivious third party, in *Proc. 6th ACM CCS*, Singapore, 1999, pp. 120–127.

[32] M. Naor, B. Pinkas, and R. Sumner, Privacy preserving auctions and mechanism design, in *Proc. 1st ACM EC*, Denver, CO, USA, 1999, pp. 129–139.

[33] A. Juels and M. Szydlo, A two-server, sealed-bid auction protocol, in *Proc. 7th Financial Cryptography*, Le Gosier, Guadeloupe, 2003, pp. 72–86.

[34] H. Lipmaa, N. Asokan, and V. Niemi, Secure vickrey auctions without threshold trust, in *Proc. 7th Financial Cryptography*, Le Gosier, Guadeloupe, 2003, pp. 87–101.

[35] F. Brandt, Secure and private auctions without auctioneers, Technical Report FKI-245-02, Institut für Informatik, Technische Universität München, 2002.

[36] F. Brandt, Fully private auctions in a constant number of rounds, in *Proc. 7th Financial Cryptography*, Le Gosier, Guadeloupe, 2003, pp. 223–238.

[37] F. Brandt, How to obtain full privacy in auctions, *International Journal of Information Security*, vol. 5, no. 4, pp. 201–216, 2006.

[38] F. Brandt and T. Sandholm, On the existence of unconditionally privacy-preserving auction protocols, *ACM TISSEC*, vol. 11, no. 2, p. 6, 2008.

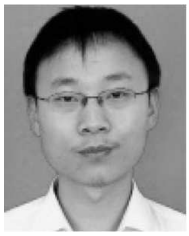
[39] F. Brandt and T. Sandholm, Efficient privacy-preserving protocols for multi-unit auctions, in *Proc. Financial Cryptography and Data Security*, Roseau, Dominica, 2005, pp. 298–312.

Yu-E Sun is an associate professor of Urban Rail Transportation Department, Soochow University, China. She received the PhD degree from Chinese Academy of Science in 2011. Her current research interests are span privacy preserving in spectrum auction, wireless sensor networks, algorithm design and analysis for wireless networks, and network security. She is a member of ACM.

He Huang is an associate professor in the School of Computer Science and Technology at Soochow University, China. He received the PhD degree from University of Science and Technology of China in 2011. His current research interests include spectrum auction, privacy preserving in auction, wireless sensor networks, and algorithmic game theory. He is a member of IEEE computer society, and a member of ACM.

Xiang-Yang Li received the bachelor degree from Tsinghua University, China, in 1995, and the MS and PhD degrees from University of Illinois at Urbana-Champaign in 2000 and 2001, respectively. He was a professor with the Illinois Institute of Technology. He is currently a professor and an executive dean of the School of Computer Science and Technology with the University of Science and Technology of China. He has authored a monograph entitled *Wireless Ad Hoc and Sensor Networks: Theory and Applications* and co-edited several books, including *Encyclopedia of Algorithms*. His research interests include wireless networking, mobile computing, security and privacy, cyber physical systems, and algorithms. He is a recipient of the China NSF Outstanding Overseas Young Researcher (B). He was an IEEE Fellow (2015) and an ACM Distinguished Scientist (2015). He holds the EMC-Endowed Visiting Chair Professorship at Tsinghua University from 2014 to 2016. He has received the six best paper awards, and one best demo award. He is an editor of several journals and has served many international conferences in various capacities.

Miaomiao Tian received the PhD degree in computer science from University of Science and Technology of China in 2014. After that he was a postdoc at University of Science and Technology of China for two years. Currently, he is an associate professor in the School of Computer Science and Technology, Anhui University, China. His research interests include cryptography and information security.



Hongli Xu received the PhD degree in computer science from the University of Science and Technology of China in 2007. Currently, he is an associate research fellow in the School of Computer Science and Technology at the University of Science and Technology of China. His main research interests include cooperative communication, vehicular ad hoc network, and software defined networks. He is a member of the IEEE.

Yang Du is a postgraduate student in Department of Computer Science and Technology from the University of Science and Technology of China. He received the BE degree from Soochow University in 2015. His current research interests include privacy preserving in auction, data mining, and truth discovery.

Mingjun Xiao is an associate professor in the School of Computer Science and Technology at the University of Science and Technology of China (USTC). He received the PhD degree from USTC in 2004. In 2012, he was a visiting scholar at Temple University, under the supervision of Dr. Jie Wu. He has served as a reviewer for many journal papers. His main research interests include delay tolerant networks and mobile social networks